A Behavioral Economics Perspective on the Formation and Effects of Privacy Risk Perceptions in the Context of Privacy-Invasive Information Systems

TECHNISCHE UNIVERSITÄT DARMSTADT

Vom Fachbereich Rechts- und Wirtschaftswissenschaften
der Technischen Universität Darmstadt

genehmigte

Dissertation

von

Hendrik Brakemeier, M.Sc.
geboren in Bern (Schweiz)

zur Erlangung des akademischen Grades
Doctor rerum politicarum (Dr. rer. pol.)

Erstgutachter: Prof. Dr. Peter Buxmann
Zweitgutachter: Prof. Dr. Alexander Benlian
Darmstadt 2018

Brakemeier, Hendrik: A Behavioral Economics Perspective on the Formation and Effects of Privacy Risk Perceptions in the Context of Privacy-Invasive Information Systems

Darmstadt, Technische Universität Darmstadt

Dissertation veröffentlicht auf TUprints im Jahr 2018
Tag der mündlichen Prüfung: 06.03.2018

Declaration of Authorship

I hereby declare that the submitted thesis is my own work. All quotes, whether word by word or in my own words, have been marked as such.

The thesis has not been published anywhere else nor presented to any other examination board.

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher weder einer anderen Prüfungsbehörde vorgelegt noch veröffentlicht.

Hendrik Brakemeier

Darmstadt, 16. Januar 2018

Abstract

In recent years, more and more information systems are proliferating that gather, process and analyze data about the environment they are deployed in. This data oftentimes refers to individuals using these systems or being located in their surroundings, in which case it is referred to as *personal information*. Once such personal information is gathered by an information system, it is usually out of a users' control how and for which purpose this information is processed or stored. Users are well aware that this loss of control about their personal information can be associated with negative long-term effects due to exploitation and misuse of the information they provided. This makes using information systems that gather this kind of information a double-edged sword. One can either use such systems and realize their utility but thereby threaten ones' own privacy, or one can keep ones' privacy intact but forego the benefits provided by the information system. The decision whether to adopt this type of information system therefore represents a tradeoff between benefits and risks.

The vast majority of information systems privacy research to date assumed that this tradeoff is dominated by deliberate analyses and rational considerations, which lead to fully informed privacy-related attitudes and behaviors. However, models based on these assumptions often fail to accurately predict real-life behaviors and lead to confounding empirical observations. This thesis therefore investigates, in how far the risk associated with disclosing personal information to privacy-invasive information systems influences user behavior against the background of more complex models of human decision-making. The results of these investigations have been published in three scientific publications, of which this cumulative doctoral thesis is comprised. These publications are based on three large-scale empirical studies employing experimental approaches and being underpinned by qualitative as well as quantitative pre-studies. The studies are guided by and focus on different stages of the process of perceiving, evaluating and mentally processing privacy risk perceptions in considerations whether to disclose personal information and ultimately use privacy-invasive information systems.

The first study addresses different conceptualizations of privacy-related behaviors, which are oftentimes used interchangeably in privacy research, despite it has never been investigated

whether they are indeed equivalent: Intentions to disclose personal information to an information system and intentions to use an information system (and thereby disclose information). By transferring the multiple-selves-problem to information systems privacy research, theoretical arguments are developed and empirical evidence is provided that those two intentions are (1) conceptually different and (2) formed in different cognitive processes. A vignette-based factorial survey with 143 participants is used to show, that while risk perceptions have more impact on disclosure intentions than on usage intentions, the opposite holds for the hedonic benefits provided by the information system. These have more impact on usage intentions than on disclosure intentions.

The second study moves one step further by addressing systematically different mental processing of perceived risks and benefits of information disclosure when considering only one dependent variable. In particular, the assumption that the perceived benefits and risks of information disclosure possess additive utility and are therefore weighted against each other by evaluating a simple utility function like "*Utility = Benefit – Cost"* is investigated. Based on regulatory focus theory and an experimental pre-study with 59 participants, theoretical arguments are developed, that (1) the perception of high privacy risks evokes a state of heightened vigilance named *prevention-focus* and (2) this heightened vigilance in turn changes the weighting of the perceived benefits and risks in the deliberation whether to disclose personal information. Results from a second survey-based study with 208 participants then provide empirical evidence, that perceptions of high risks of information disclosure in fact evoke a prevention focus in individuals. This prevention focus in turn increases the negative effect of the perceived risks and reduces the positive effect of the perceived benefits of information disclosure on an individuals' intention to disclose personal information.

Instead of investigating the processing of risk perceptions, the third study presented in this thesis focuses on the formation of such perceptions. The focus is therefore on the process of selecting, organizing and interpreting objective cues or properties of information systems when forming perceptions about how much privacy risk is associated with using the system. Based on an experimental survey study among 233 participants the findings show, that individuals in fact have difficulties evaluating privacy risks. In particular, (1) the formation of privacy risk perceptions is dependent on external reference information and (2) when such external reference information is available, individuals are enabled to form more confident risk judgments, which in turn have a stronger impact on an individual's privacy-related

behavior. These findings suggest a reconceptualization of privacy risks as not only being characterized by an extremity (how much risk is perceived) but also the dimension of confidence in ones' own risk perception.

Overall, the research findings of the three studies presented in this thesis show, that widely accepted assumptions underlying information systems privacy research are severely over-simplified. The results therefore contribute significantly to an improved understanding of the mental processes and mechanisms leading to the acceptance of privacy-invasive information systems.

Zusammenfassung

In den letzten Jahren ist eine immer stärkere Verbreitung von Informationssystemen, die Daten aus ihrer Umwelt erfassen, verarbeiten und analysieren, beobachtbar. Diese Daten beziehen sich dabei häufig auch auf Menschen, die diese Systeme nutzen oder sich in deren Umfeld bewegen. In diesem Fall spricht man von *persönlichen Informationen*. Sobald solche persönlichen Informationen von einem Informationssystem erfasst wurden, verlieren dessen Nutzer in der Regel jegliche Kontrolle darüber, wie und für welche Zwecke diese Informationen gespeichert oder verarbeitet werden. Die Nutzer sind sich dabei durchaus bewusst, dass dieser Kontrollverlust über ihre persönlichen Informationen langfristig negative Konsequenzen für sie haben kann. Gründe hierfür sind beispielsweise die Verwendung der persönlichen Informationen entgegen dem ursprünglichen Zweck, Verlust oder Weitergabe der Informationen an Unberechtigte oder anderweitiger Missbrauch. Die Nutzung solcher Informationssysteme geht daher sowohl mit positiven als auch negativen Konsequenzen einher. Entweder das System wird genutzt, wobei man von dem vom System gestifteten Nutzen profitiert, aber gleichzeitig seine Privatsphäre gefährdet, oder man schützt seine Privatsphäre, aber verzichtet damit auch auf den Nutzen, den das Informationssystem bietet. Die Entscheidung, solch ein System zu nutzen, stellt folglich eine Abwägung zwischen Nutzen und Risiko dar.

Der überwiegende Anteil der Forschung zum Thema *Privatsphäre* in der Disziplin der Wirtschaftsinformatik nimmt bis heute an, dass diese Abwägung auf wohl durchdachten Bewertungen und rationalen Überlegungen fußt. Forschungsmodelle, die auf dieser Annahme aufbauen, können tatsächliches Verhalten von Menschen in Bezug auf ihre Privatsphäre jedoch häufig nicht erklären und führen in verschiedenen Kontexten zu unterschiedlichen Ergebnissen. In dieser Arbeit wird daher untersucht, inwiefern das mit der Preisgabe persönlicher Informationen an ein Informationssystem verbundene Risiko das Nutzerverhalten vor dem Hintergrund komplexerer Modelle menschlichen Entscheidungsverhaltens beeinflusst. Die Forschungsergebnisse wurden in drei wissenschaftlichen Publikationen veröffentlicht, die Teil dieser kumulativen Doktorarbeit sind. Diese Veröffentlichungen basieren auf drei großzahligen empirischen Studien, welche

durch quantitative und qualitative Vorstudien gestützt werden. Die Studien beziehen sich auf unterschiedliche Stufen des Prozesses der Wahrnehmung, Bewertung und mentalen Verarbeitung von Wahrnehmungen eines Privatsphärerisikos bei der Entscheidung, persönliche Informationen preiszugeben beziehungsweise privatsphäreinvasive Informationssysteme zu nutzen.

Die erste Studie untersucht verschiedene Konzeptualisierungen von privatsphärerelevantem Verhalten, die in der aktuellen Forschungslandschaft synonym verwendet werden, obwohl nie untersucht wurde, ob diese Konzeptualisierungen tatsächlich äquivalent zu verwenden sind: Die Absicht, persönliche Informationen an ein Informationssystem preiszugeben und die Absicht, ein privatsphäreinvasives Informationssystem zu nutzen (und dabei persönliche Informationen an dieses preiszugeben). Durch die Übertragung des sogenannten *multiple-selves-problems* in die Privatsphäreforschung werden theoretische Argumente dafür entwickelt, dass die beiden genannten Verhaltensabsichten (1) konzeptuell unterschiedlich und (2) die Ergebnisse verschiedener kognitiver Prozesse sind. Auf Basis einer multifaktoriellen Vignettenstudie mit 143 Teilnehmern wird gezeigt, dass während Risikowahrnehmungen einen größeren Einfluss auf die Informationspreisgabeabsicht als auf die Nutzungsabsicht haben, das Gegenteil für die von einem Informationssystem gestifteten hedonistischen Nutzenaspekte gilt. Diese haben mehr Einfluss auf die Nutzungsabsicht als auf die Absicht zur Informationspreisgabe.

Während die erste Studie Unterschiede des Einflusses von Risiko- und Nutzenwahrnehmungen auf unterschiedliche abhängige Variablen untersucht, geht die zweite Studie einen Schritt weiter und betrachtet systematisch unterschiedliche mentale Verarbeitungsmechanismen von Risiko- und Nutzenwahrnehmungen bei Betrachtung nur einer abhängigen Variablen. Dabei wird die in der Forschung gängige Annahme untersucht, dass Nutzen- und Risikoaspekte sich durch additive Nutzwerte auszeichnen und die Abwägung dieser damit als eine Nutzenfunktion der Form "*Utility = Benefit – Cost"* dargestellt werden kann. Auf Grundlage der *regulatory focus theory* und einer experimentellen Vorstudie mit 59 Teilnehmern werden Argumente dafür hergeleitet, dass (1) die Wahrnehmung hoher Privatsphärerisiken zu einer erhöhten Wachsamkeit führt, die als *prevention-focus* bezeichnet wird und (2) diese erhöhte Wachsamkeit wiederum die Gewichtung von Nutzen- und Risikowahrnehmungen in der Entscheidung über die Preisgabe persönlicher Informationen beeinflusst. Eine zweite Fragebogenstudie mit 208 Teilnehmern liefert empirische Evidenz, dass die Wahrnehmung hoher Privatsphärerisiken tatsächlich

einen *prevention-focus* hervorruft. Dieser führt dazu, dass der negative Einfluss der wahrgenommenen Privatsphärerisiken verstärkt und der positive Einfluss der Nutzenwahrnehmung auf die Informationspreisgabeabsicht abgeschwächt wird.

Die dritte Studie, die im Rahmen dieser Arbeit dargestellt wird, legt den Fokus nicht auf die mentale Verarbeitung von Privatsphärerisiken, sondern auf deren Entstehung. Dabei wird der Prozess des Auswählens, Organisierens und Interpretierens von objektiv beobachtbaren Eigenschaften eines Informationssystems bei der Beurteilung des von diesem System ausgehenden Privatsphärerisikos genauer beleuchtet. Im Rahmen einer Umfragestudie mit experimentellem Studiendesign unter 233 Teilnehmer wird gezeigt, dass es Menschen tatsächlich häufig schwerfällt, Privatsphärerisiken zu bewerten. Dabei wird inbesondere gezeigt, dass (1) die Bildung von Risikowahrnehmungen durch extern verfügbare Referenzinformationen beeinflusst wird und (2) wenn solche externen Referenzinformationen verfügbar sind, das Vertrauen in die eigene Risikoeinschätzung erhöht ist und diese wiederum einen größeren Einfluss auf das privatsphärerelevante Verhalten aufweist. Auf Basis dieser Ergebnisse wird eine zweidimensionale Rekonzeptualisierung von wahrgenommenen Privatsphärerisiken vorgeschlagen, die sich offenbar nicht nur durch einen Risikograd (d.h. die Höhe der wahrgenommenen Privatsphärerisiken), sondern auch die Dimension der Zuversicht in die eigene Risikoeinschätzung auszeichnen.

Übergreifend zeigen die in der Arbeit vorgestellten Ergebnisse, dass in der Privatsphäreforschung weit verbreitete Annahmen den mentalen Prozess der Wahrnehmung und Verarbeitung von Privatsphärerisiken zu stark vereinfachen. Die Arbeit trägt damit erheblich zu einem besseren Verständnis der mentalen Prozesse und Mechanismen bei, die zur Akzeptanz von privatsphäreinvasiver Informationstechnologie führen.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AIS	Association for Information Systems
AISeL	AIS electronic Library
App	Application
AVE	Average Variance Extracted
CFI	Comparative Fit Index
CR	Composite Reliability
Cr. α	Cronbach's Alpha
EVA	Evaluability
H	Hypothesis
HED	Hedonic Attitude
INT	Intention
IS	Information System(s)
IT	Information Technology
JE	Joint Evaluation Mode
LBS	Location-Based Service
LISREL	Linear Structural Relations (Software)
NNFI	Nonnormed Fit Index
OSN	Online Social Network
PLS	Partial Least Squares
RMSEA	Root Mean Square Error of Approximation
RQ	Research Question
RSK	Perceived Risk of Information Disclosure
SD	Standard Deviation
SE	Single Evaluation Mode
SEM	Structural Equation Modeling
SPSS	Statistical Package for the Social Sciences (Software)
SRMR	Standardized Root Mean Square Residual
TAM	Technology Acceptance Model
TPB	Theory of Planned Behavior

TRA	Theory of Reasoned Action
UTIL/UTL	Utilitarian Attitude
VIS	Visual Appeal

1 Introduction

In recent years, more and more information systems are proliferating that gather, process and analyze data about the environment they are deployed in. With the proliferation of smartphones (Statista 2017a), sensor-equipped watches and smart home appliances (Statista 2017b), the amount of information that is being stored by information systems increases every day. Simultaneously, trends like personalization (Chellappa and Sin 2005), real-time and ubiquitous computing (Lyytinen and Yoo 2002) foster the idea that information systems are not only used as productivity tools in working environments but are intertwined into peoples' everyday life. This has led to an increasing amount of personal information being actively inputted into but also passively registered by information systems. Prominent examples are Facebook *"Likes"* (Rosendaal 2010) reflecting personal preferences, social media ties denoting one's social environment or even the contents of computer-mediated communications. But also, financial information is stored in smartphone applications or health-related data is collected by wearable sensors like fitness wristbands (Angst and Agarwal 2009; Fernández-Alemán et al. 2013). Another upcoming trend that has to be considered here is Smart Home appliances like Amazon's Echo or Google Home, which record and process every word spoken in their surroundings (Ferdinand and Jetzke 2017; Turk 2016).

Once such information is gathered by an information system, it is usually out of a users' control how and for which purpose this information is processed or stored (Acquisti 2004; Acquisti et al. 2015). It could be transferred to servers of the provider of the information system via the internet or analyzed to create profiles, for example, for targeted marketing activities. Furthermore, information could be intentionally sold to third parties or fall into the hands of malicious actors like hackers if not stored properly by application providers. Users are well aware that disclosing personal information while using privacy-invasive information systems may be associated with potential negative long-term effects due to this loss of control. This makes using this kind of information system a double-edged sword. One can either use such information systems and realize their utility but thereby threaten one's own

privacy, or one can keep privacy intact but forego the benefits provided by such information systems.

The proliferation of this kind of information systems leads to a rich discourse about how individuals deal with these conflicting goals during decisions whether to disclose personal information. Since the 1970s research investigated how people react to situations in which they have to decide whether to disclose personal information in return for a certain benefit (Smith et al. 2011) from various perspectives like the legal sciences, policy research, psychology and also information systems research. Different macro-models have been proposed as synthesis of literature based on this research, but, as Dinev et al. (2015, p. 639) note in a recent research commentary published in one of the information systems research community's leading journals – *Information Systems Research* – these macro-models all rely on a "… covert assumption: responses to external stimuli result in deliberate analyses, which lead to fully informed privacy-related attitudes and behaviors." However, the principles reflected by these macro-models regularly fail to predict and explain actual user behavior. It rather seems that individuals "…engage in privacy-related behaviors spontaneously, often in circumstances […] where little deliberation takes place" (Dinev et al. 2015, p. 640). Therefore, the current models discussed in literature seem to only provide an incomplete picture of privacy-related decision-making of individuals in the area of information systems privacy research. This thesis is therefore concerned with the question of in how far the risk associated with disclosing personal information to privacy-invasive information systems influences user behavior from a behavioral economics perspective.

This approach to information systems privacy research can contribute to extant research as well as inform practitioners dealing with privacy-management from a provider perspective. The following two sections describe in more detail why the results presented in this thesis are relevant to researchers (section 1.1) as well as practitioners (section 1.2).

1.1 Scientific Relevance

Research on information privacy addresses the developments described above from a scientific perspective. As noted above, scholars began in the early 1970s to investigate how users react to situations involving the disclosure of personal information (Smith et al. 2011). Over the years, more and more factors influencing this tradeoff have been identified and integrated into theories, ultimately leading to a somewhat disconnected research landscape and coexistence of different theoretical approaches. Albeit researchers investigated lots of

different concepts, some overarching factors emerge in a multitude of studies and therefore seem to be the main drivers of information disclosure behavior. Among these are, for example, the general attitude of a person towards privacy, oftentimes denoted as a person's general degree of privacy concern, one's beliefs about the party information are disclosed to, which usually refers to trust, the benefits one can realize by disclosing private information and the potential negative consequences of doing so in a certain situation, referred to as the perceived risks of information disclosure. The macro-models based on extant literature mentioned above provide an overall picture of the relationships determining people's disclosure behavior (Bélanger and Crossler 2011; Smith et al. 2011; Yuan 2011). Albeit not being equivalent, these macro-models all share one common characteristic that is widely spread in information systems research based on economic theory: "human beings are capable of always making rational decisions" (Ariely 2009, p. 80) and therefore engage in "effortful, deliberate information processing when forming privacy-related perceptions" (Dinev et al. 2015, p. 640). In particular, situation-specific privacy-related decision making is described as a rational tradeoff between the positive and negative consequences of information disclosure – usually operationalized as a tradeoff between the perceived benefits of information disclosure and the perceived risk of information disclosure and termed *privacy calculus* (Laufer and Wolfe 1977; Li 2012).

However, this rational tradeoff has been found to fail at explaining real-life behaviors. It much more seems that privacy-related decisions are very context specific (Dinev et al. 2015), suggesting that people make privacy-related decisions spontaneously, guided by momentary feelings, short-sighted desires and emotions instead of thoughtful deliberations. Such decisions are oftentimes influenced by perceptual biases, false assumptions, cognitive shortcuts, and incomplete information. The mechanisms underlying such biased privacy-related decision making based on incomplete information and other heuristics have rarely been considered in extant research (Dinev et al. 2015). However, focusing on deliberate considerations and rational tradeoffs has led to ambiguities and obscurities in privacy research. For example, while some studies find the behavioral intention to disclose personal information to be mainly determined by privacy risks (Kehr et al. 2015; Keith et al. 2013), others report the perceived benefits of information disclosure to be the primary antecedent (Li et al. 2014; Shibchurn and Yan 2015). Some studies even find no effect of privacy risks on privacy-related behavior at all (Krasnova et al. 2012). Others find that even when asking the same person, privacy-related decisions are inconsistent across time (Norberg et al. 2007). These different results in terms of intentions or behavior based on the same input parameters

cannot be explained by purely rational and deliberate cognitive processes. Therefore, it seems fruitful to incorporate a psychological perspective into information systems privacy research to gain a deeper understanding of which cognitive processes inform privacy-related behaviors and thereby unveil factors that help to explain the inconsistent empirical findings across contexts.

The consideration of human behavior in economic contexts against the background of psychological biases and irrational behavior is referred to as *behavioral economics*. Investigating privacy-related behaviors from this viewpoint might therefore help to explain the inconsistencies mentioned above and provide new perspectives for information systems privacy research.

1.2 Practical Relevance

Apart from these scientific considerations, the topic of how privacy-related attributes of information systems influence user behavior is also relevant from the perspective of practitioners. Users nowadays expect that information systems become more and more intertwined with their environment and provide real-time and context-relevant information. To provide this kind of functionalities, providers are forced to gather various kinds of context-relevant information. Apart from being essential to provide certain functionalities, data also has an economic value for providers, that can be monetized (e.g., Chen et al. 2012; Lycett 2013; Woerner and Wixom 2015). Thus, personal information can be a valuable asset for application providers. For these two reasons, providers of information systems are usually interested in collecting, processing and ultimately monetizing as much information as possible. However, collecting too much information from users also bears the potential for negative consequences. The more information is collected, the fewer users will an information system attract because they are concerned regarding their privacy (e.g., Dinev and Hart 2006; Krasnova et al. 2010). As a consequence, the population to extract information from becomes smaller the more information is collected. Practitioners are therefore also confronted with conflicting goals in the context of the privacy-friendliness of their application: They can either collect more information from each individual user and thereby increase the monetization potential of each user but thereby also scare-off users or they can try to be more privacy-friendly and as a consequence have the potential to attract a greater number of users with lower monetization potential (Buxmann 2015). Finding the right balance between the conflicting goals of maximizing monetization potential per user and maximizing the number of total users is nowadays oftentimes done by gut-feeling or trial and error approaches

(Buxmann 2015). Gaining a richer understanding of how users perceive privacy-relevant attributes of information systems and form usage intentions based on these offers providers a more thorough basis for privacy management decisions and is therefore valuable when trying to optimize applications in terms of privacy.

Furthermore, providers are usually constrained by limited resources in terms of human resources, money and time. Thus, they have to carefully prioritize into which features of their applications they invest these resources. Against the background of privacy calculus theory, there are two possible ways of increasing the dissemination of a privacy-invasive information system: increasing the benefit it provides or reducing the privacy risks it evokes (Li 2012). However, extant privacy research is ambiguous about whether and when increasing benefits or reducing evoked privacy risks has more effect on the adoption of privacy-invasive information systems (e.g., Krasnova et al. 2012). Thus, extant research fails at providing clear guidance for application providers when putting effort into the development of new features to improve functionality or investing in privacy-relevant techniques reducing evoked privacy risks serves company goals better.

Lastly, extending knowledge in this area can help providers of privacy-friendly information systems to make their privacy-friendliness a competitive advantage (Foroohar 2017; Hoffman 2014). Privacy-friendliness can only be transformed into a competitive advantage if people in fact react to privacy-friendly product attributes and value those in their adoption decision. If privacy-relevant product attributes remain unconsidered, there is no advantage for providers to be privacy-friendly and therefore the privacy-friendliness may not be suitable to create a relative advantage compared to less privacy-friendly providers.

The studies presented in this thesis can inform these kinds of decisions practitioners face by stopping them from “operating on the premise that people make logical decisions” (Ariely 2009, p. 78) and investigate in more detail under which circumstances privacy-relevant attributes of privacy-invasive information systems in fact influence adoption behavior and when they do not. Thus, they allow providers to deduce more detailed, reliable and valid conclusions about how much data should be collected from users and in which situations investing in privacy-friendliness or putting effort into increased functionality is more expedient.

Before turning to the research projects described in this thesis in more detail, the overall theoretical background for the studies is laid out in the following chapter. First, the topic of privacy-invasive information systems is outlined to define the applicability of the results

presented in this thesis. In section 2.2, the current theoretical perspectives on privacy-related decision-making are outlined and perspectives are provided, in how far incorporating a behavioral economics perspective can extend these theoretical approaches. Afterwards, in chapters 3 to 5, three studies are presented all extending the classical rational view of privacy-related decision-making in different aspects.

2 Research Context and Positioning of the Thesis

In this section, the overarching foundation for the studies forming this thesis is laid out. First, the scope of the thesis is demarcated by providing definitions for fundamental terms used in this thesis and the type of IT artifact the research findings presented in this thesis can be applied to. Afterwards, the theoretical groundwork for the research presented in this thesis is introduced and a description of how the studies presented in chapters 3 to 5 can be integrated into existing research is provided.

2.1 Definition of the Scope of the Thesis

The research projects forming this thesis are all concerned with how individuals make decisions about whether it is acceptable to have personal information gathered and processed by information systems under different circumstances. To clarify the scope and clearly delineate the applicability of research findings presented in later sections, the following sections are concerned with what is meant by *personal information*, the concept of *privacy* and what type of information systems this thesis addresses against this background. We begin by defining what is meant by *personal information*.

2.1.1 Personal Information

The term *personal information* terminologically refers to a special type of information. Thus, to clarify the term, this section first shortly addresses what is meant by information in general and then discusses in more detail what characterizes the subset of information that is referred to as being *personal information*.

The term *information* is used in different ways, all being more or less useful in different fields. A reasonable and useful perspective for this thesis that is also widely used in information systems research is the "Standard Definition of Information" (Floridi 2005, p. 352). This definition refers to information as being "data plus meaning" (Checkland and Scholes 1999, p. 303), which in turn requires three conditions to be met: (1) information consists of data, (2) the data are well-formed and (3) this well-formed data is meaningful (Floridi 2005). The definition of data, in turn, is disputed, however, working out a clear

definition is out of the scope of this thesis. In the context of information systems, data usually refers to bits and bytes and therefore ultimately to a sequence of ones and zeros. The second condition of being well-formed is met if the data are clustered in a way, that complies with the rules of some given system, code or language (Floridi 2015). This is also referred to as being *syntactically* correct. Concerning bits and bytes, these should be arranged in a way in which they encode, for example, characters, words or images. Lastly, these well-formed data should have some kind of meaning attached to them. In other words, it must follow the *semantics* of some given system, code or language, which makes the text or images formed by the data meaningful for the recipient (Davis and Olson 1985).

The adjective *personal* further specifies a condition that has to be met by meaningful data to be considered being *personal information* and therefore the type of information relevant to this thesis. In their well-respected literature review on privacy research, Smith et al. (2011, p. 990) use a relatively generic definition by noting that personal information refers to „information about individuals and groups". More specific definitions of the term, that allow a clearer delineation of what personal information is and what it is not, have been developed in the legal sciences. The European Commission uses the following definition in the context of the European Data Protection Directive:

> *"Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address" (European Commission 2012).*

This definition of personal information is also adopted for this thesis, thus personal information is defined as well-formed data, that is meaningful and related to an individual. Please note that this definition is in line with the one provided by Smith et al. (2011), which explicitly mentions information about groups. As groups are a collection of at least two individuals, information relating to a group is also related to at least two individuals. Now that the term personal information has been delineated, the term *information privacy* will be discussed.

2.1.2 Information Privacy

In the previous section, the concept of personal information has been defined. Keeping such personal information to ourselves and not having them openly available to the public is inherently important to human beings and referred to as *privacy*. The concept of privacy is

socially important, because it "… provides the cover under which most human wrongdoing takes place, and then it protects the guilty from taking responsibility for their transgressions once committed" (Schoeman 1984, p. 1). As a consequence, "privacy may be seen as a culturally conditioned sensitivity that makes people more vulnerable than they would otherwise be to selective disclosures and to the sense of comparative inferiority and abject shame – a sense engendered by ignorance about the inner lives of others" (Schoeman 1984, p. 1).

To discuss the topic of information privacy, agreement about what is meant by the term is crucial. However, privacy has been defined from a variety of perspectives and therefore no unanimous definition exists. First, it has to be noted, that the topic of this thesis is information privacy as opposed to physical privacy. Physical privacy denotes "access to an individual and/or the individual's surroundings and private space" (Smith et al. 2011, p. 990), while information privacy refers to access to personal information (Smith et al. 2011). In the following, the focus will be on information privacy.

The earliest definitions conceptualized privacy as a *right*. For example, Warren and Brandeis (1890, p. 193) define privacy as "the right to be left alone". A definition that is more tailored to personal information and therefore information privacy defines the term as the "right of an individual to determine what information about himself (or herself) may be communicated to others" (Schoeman 1984, p. 2).

Others conceptualize privacy as a *state* and define it as a state of "limited access to information about [a person], limited access to the intimacies of his life, or limited access to his thoughts […]" (Schoeman 1984, p. 3).

A third conceptualization sees privacy as an ability to exert *control*. Against this background, privacy has been defined as "the selective control of access to the self" or "the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (Margulis 1977, p. 10). The conceptualization of privacy as control has come to be the most commonly used conceptualization of privacy in information systems privacy research, "… because it lends itself more readily to the attributes of information privacy" (Smith et al. 2011, p. 995) compared to other conceptualizations. It is particularly suited to describe issues concerning the ability of individuals to control transactions involving their personal information and therefore ultimately covers all conceivable ways of information privacy invasions.

A fourth and somewhat less intuitive definition has been introduced by Davies (1997), who postulates that information privacy can also be seen as "a commodity that can be exchanged for perceived benefits" (Campbell and Carlson 2002, p. 588). This definition was developed based on the conceptualization that more and more firms acquire personal data about their users to monetize it. As a consequence, the discussion about information privacy shifted from being a political and civil rights issue to a consumer-rights issue (Davies 1997). The basic proposition of information privacy being a *commodity* is that consumers can give up parts of their privacy by disclosing personal information to firms in exchange for benefits (Garfinkel et al. 2002).

This definition of privacy as a commodity can be integrated into the control-based definition. People can trade control about their personal information for benefits in situations, in which they feel they are being rewarded for this loss of control adequately. Because of its special suitability and wide adoption in the area of information systems privacy research, as well as its ability to also cover aspects of the definition of privacy as a commodity, the control-based definition of privacy will be employed in the course of this thesis. Against this background, it is now possible to differentiate the type of information system that is addressed in this thesis and therefore represents the boundaries of the applicability of research findings presented in the studies described in chapters 3 to 5.

2.1.3 Privacy-Invasive Information Systems

As is the case with information privacy research in general, this thesis is concerned with the reactions of individuals to *privacy-invasive information systems* (e.g., Dinev et al. 2006; Krasnova et al. 2012; Li et al. 2010; Xu et al. 2009). To enable readers to assess to which information systems the results of this research apply, a clear definition of what characterizes *privacy-invasive information systems* is necessary. Before referring to the special case of *privacy-invasive information systems*, a discussion of the term *information system* is required.

The term *information system* is defined as a system for acquiring, processing, transferring, storing and/or provisioning information (Schwarze 2000) and similarly Ferstl and Sinz (2015) define information systems as a system that processes information, i.e. gathers, transfers, transforms and provides it to its environment. Usually these functions are performed by a combination of hardware and software (a computer), however, this is not a necessary condition. Therefore, some definitions explicitly refer to information systems that involve computers as *computer(-based) information systems* (e.g., Miller and Doyle 1987).

In this thesis, these definitions are adopted and thus, information systems refer to (computer-based) systems, that gather, store and process information. However, this thesis is concerned with a special type of information systems, namely *privacy-invasive information systems*.

Now the question is what makes an information system *privacy-invasive*. As outlined in the previous section, privacy refers to the ability of individuals to control transactions involving their personal information. A privacy-invasion is therefore given, when using an information system leads to a loss of control over one's personal information. For this condition to be met, using the information system firstly has to involve transactions handling personal information. This is given if the information that is processed by the information system is associated with an individual, as was outlined in section 2.1.1. In the context of information systems, this individual is usually the user of such an information system. Once the personal information has been gathered by the information system, this has to be associated with a loss of control about this information for the user. Such a loss of control is also given because the users of information systems usually cannot observe how information is processed by a computer system. As a consequence, the provider of the information system could use the personal information in unforeseen ways by transferring it via networks, analyzing it or sharing it with third parties. Using an information system that processes personal information is therefore regularly associated with such a loss of control about one's personal information (Malhotra et al. 2004) and therefore a privacy-invasion. Taking the definitions of personal information, privacy and information systems together allows a definition the IT artifacts investigated in this thesis and to which our findings are applicable as follows: Privacy-invasive information systems are defined as *computer-based systems, that gather, process and store meaningful data associated with an identifiable individual*.

Now that the object of examination of this thesis has been delineated, the following sections dive more into the mechanisms employed during decisions whether to use such systems in traditional information systems privacy research and then describe how this perspective can be extended by integrating this classical view with behavioral economics.

2.2 Privacy-Related Decision-Making

In the previous sections, it has been described for which type of information system the research presented in this thesis is applicable. In the following, the focus will be on which issues surrounding this type of information system are investigated. Therefore, a brief

overview of the state of research regarding these questions is provided and the theoretical background and motivations of the research projects presented in chapters 3 to 5 are depicted.

In this endeavor, it is first outlined how information systems privacy research has been trying to explain individuals' information disclosure behavior to date in section 2.2.1. Based on this overarching model or set of assumptions, it is outlined in how far these assumptions are fallible because they are oversimplifying the cognitive mechanisms determining information disclosure behavior. It is then described in how far theory is being extended by relaxing these assumptions in section 2.2.2. In the last subsection 2.3, an overall summary of the structure of this thesis is given and it is pointed out, in how far each of the studies presented in this thesis extends extant theory in more detail.

2.2.1 The Neoclassical Approach to Privacy-Related Decision-Making

> *"The fundamental knowledge interest that underlies information system (IS) research is this: how can an IS — as a semiotic and sociotechnical system — be effectively deployed in the human enterprise? […] Effective here means any dimension of improvement in the human condition in which the uses of IT can be evaluated. By human enterprise, we mean any social arrangement that can be served or affected by or can serve the uses of IT, ranging from use by individuals, teams, organizational units, and organizations to use by communities, markets, industries, and societies" (Grover and Lyytinen 2015).*

As this quote from *Management Information Systems Quarterly*, one of the leading journals of information systems research, denotes, explaining the behavior of humans in the context of information system usage has been an elementary part of information systems research for long years. Numerous models, like the theory of reasoned action (TRA) (Ajzen and Fishbein 1969; Ajzen and Fishbein 2000), the theory of planned behavior (TPB) (Ajzen and Fishbein 1980; Fishbein and Ajzen 1975) or the technology acceptance model (TAM) and its extensions (Davis 1989; Davis et al. 1989; Venkatesh and Davis 2000; Venkatesh et al. 2012) all share the goal of explaining the behavior of individuals when interacting with or being confronted with information systems.

The same applies to the area of information systems *privacy* research. In this field of research, the behavior under investigation is usually under which circumstances individuals accept invasions of their privacy by having personal information gathered, processed and stored by privacy-invasive information systems. This topic started to gain interest in the 1970s, when researchers began to express concerns that individuals might not be able to manage their own

personal information because of the proliferation of computer technology at that time (Breckenridge 1970; Laufer and Wolfe 1977; Margulis 1977; Rule 1974). Since then, various theories have been applied to explain and predict this type of behavior. A thorough review of these theories used in information systems privacy research has been published by Li (2012). In this section, a brief overview will be provided.

The first theories in the area of information systems privacy research centered around the concept of privacy concerns. Privacy concerns have been identified as a central concept against the background of agency theory and social contract theory. These theories focus on the relationships between different social or economic actors and in how far one party can observe the behavior and motives of the other. Research argued that the potential of opportunistic behavior when dealing with personal information evokes privacy concerns, which in turn make individuals hesitate to disclose personal information. Empirical studies then provided evidence that privacy concerns are in fact considered by users and can inhibit the disclosure of personal information (e.g., Culnan and Armstrong 1999; Stone et al. 1983). Based on such evidence that privacy concerns are an important factor influencing the decision whether to disclose personal information, the concept was integrated into existing and widely-applied theories used to explain human behavior in information systems research – the theory of reasoned action and the theory of planned behavior (Ajzen 1991; Ajzen and Fishbein 2000; Fishbein and Ajzen 1975). These theories posit that individuals form beliefs about objects and behaviors and base their behavioral intention on a deliberate evaluation of these beliefs.

In the following, the notion of privacy as a commodity (see section 2.1.2) gave rise to the idea of not only considering the negative consequences of information disclosure but conceptualizing privacy-related decision-making as a trade-off also involving positive consequences. This is ultimately reflected by privacy calculus theory, which is deeply rooted in the notion that individuals in an economic context act as rational deciders. Accordingly, the management of personal information was conceptualized as a "calculus of behavior" (Laufer and Wolfe 1977, p. 35) and termed the *privacy calculus theory*. According to privacy calculus theory, an individual's decision whether to disclose personal information is dependent on (1) the *perceived benefits of information disclosure* and (2) the *perceived risks of information disclosure*. These two are weighted against each other and form a *behavioral intention to disclose personal information* (Li 2012; Smith et al. 2011). Thus, research assumed that when deciding whether to disclose personal information or not, people basically evaluate a utility function like the following (e.g., Awad and Krishnan 2006):

Utility = Benefit - Cost

This formula illustrates very well, that privacy calculus theory assumes, that "… consumers perform the risk-benefit analysis in the privacy calculus and decide whether to disclose information based on the net outcomes" (Li 2012, p. 475). If the net outcome utility is positive and therefore disclosing personal information is an overall *gain*, information is disclosed. If the net outcome is negative and disclosing personal information therefore associated with an overall *loss*, personal information is kept private and individuals forego the benefits they could have realized by disclosing their personal information.

This theory in particular exhibits a common assumption in information systems privacy research: human beings make decisions after engaging in effortful, deliberate information processing (Dinev et al. 2015). This was also noted in a recent call for research in *Information Systems Research* (Dinev et al. 2015) which synthesized three comprehensive and well-published literature reviews on information systems privacy research by Bélanger and Crossler (2011), Li (2012), and Smith et al. (2011).

The assumption that human beings make privacy-related decisions based on effortful and deliberate information processing, however, is questionable (Ariely 2009; Kahneman 2003; Simon 1955). If individuals would, in fact, perform purely rational tradeoffs when deciding about information disclosures, decisions would have to be consistent across contexts. However, a handful of studies (e.g., Acquisti 2004; Acquisti and Grossklags 2005a; Acquisti et al. 2012; Li et al. 2011; Li et al. 2008; Tsai et al. 2011) has begun to integrate principles from psychological experiments into information systems privacy research and found severe effects that contradict this assumption (Dinev et al. 2015). Li et al. (2008) for example found that the evaluation of how much risk is associated with the disclosure of personal information is strongly influenced by emotions like fear and joy. Acquisti et al. (2012) were able to provide evidence, that human beings are prone to the herding-effect when deciding about their privacy. They are more willing to disclose personal information if they are told that others also disclosed this information. Also, asking for intrusive information first and less intrusive thereafter leads to more information being disclosed compared to when individuals are asked for the less intrusive information first. Thus, the disclosure of personal information is evaluated differently depending on what has been disclosed before, the behavior of others and even feelings. These findings cannot be reconciled with the assumption that privacy-related decision-making is the result of rational and deliberate information processing.

Thus, with the studies making this thesis, the recent call for more research by Dinev et al. (2015) to move from basic economic theory towards behavioral economics to investigate individuals' reactions to privacy-invasive information systems has been followed.

2.2.2 A Behavioral Economics Perspective on the Privacy Calculus

This thesis contributes to information systems privacy research by moving from seeing privacy-related behavior as the rational tradeoff or deliberate analysis reflected by privacy calculus theory towards a behavioral economics perspective. Behavioral economics is concerned with the synthesis of economic principles with "… procedures and preparations pioneered within the experimental analysis of behavior" (Madden 2000, p. 4). Thus, it tries to increase the realism of the psychological underpinnings of economic analysis" (Camerer and Loewenstein 2011, p. 3) and thereby increase the explanatory power of economic theories (Camerer and Loewenstein 2011). The studies presented in the following chapters are thereby concerned with relaxing the simplifying assumptions made in classical theoretical approaches to privacy-related behaviors (Camerer and Loewenstein 2011).

As privacy calculus is based on basic principles of utility maximization, it is also subject to such simplifying assumptions that might be proven wrong against the background of behavioral economics. Privacy calculus makes three basic assumptions about how an individual makes privacy-related decisions: (1) individuals are able to assess and evaluate the (1.1) perceived privacy risks and (1.2) perceived benefits of information disclosure, (2) these perceptions are weighted against each other to determine the net utility associated with the disclosure of personal information and (3) this net utility determines an individuals' intention to disclose his or her personal information. This is a simplification of the general process in which human beings process sensory input, form perceptions based on this input and ultimately react to these stimuli. This process is termed *perceptual process* in psychology and draws a much richer picture of the process of perception and reaction formation than privacy calculus theory.

According to the *perceptual process*, perceptions are not as easily formed as veridical descriptions of reality as privacy calculus theory assumes. They are rather the result of a complex process which starts when an individual is confronted with a privacy-invasive information system. This information system and its attributes represent a set of stimuli the individual is exposed to. Such stimuli first have to be received by one of the individual's five senses – usually through observation in the context of information systems. However, just

because a stimulus was received does not mean it plays a role in perception formation. It first has to catch the individual's attention to be incorporated in the perception formation process. Only then the stimulus or cue is organized among other stimuli and interpreted by relating it to existing norms and knowledge to make it meaningful. The result of this process is then called a perception (Solomon et al. 2006). Thus, a perception is the result of a three-stage process in which stimuli are selected, organized and interpreted. Such perceptions are in turn evaluated with regard to how to react to them. This evaluation mechanism – the weighting of benefits and risks in the privacy calculus – is again subject to psychological biases and shortcuts that can alter its way of operation (Higgins 1998).

Privacy-related decision-making ultimately is one instance of this complex process and therefore the assumptions underlying the rational view of privacy calculus theory are severely simplified from the actual perceptual process. These simplifications can lead to confounding research results. Three stages where such oversimplifications of psychological mechanisms could interfere with privacy calculus theory can be identified by relating the assumptions made by privacy calculus theory to the perceptual process. As noted above, the first assumption of privacy calculus theory is, that (1) individuals are able to assess and evaluate the (1.1) perceived privacy risks and (1.2) perceived benefits of information disclosure. This assumption abstracts from the perceptual process of selecting, organizing and interpreting stimuli and therefore assumes that a certain stimulus always results in the same perception.

The second assumption privacy calculus theory is based on is that perceptions of risks and benefits are weighted rationally against each other to determine the net utility associated with the disclosure of personal information. This assumption simplifies psychological perceptual processes to the extent, that different weightings of these two antecedents depending on the decision context are neglected. However, it might be possible, that depending on context, people could become more sensitive to privacy risks or benefits provided by an information system when making decisions about whether to disclose personal information to that system. One exemplary factor that might influence the sensitivity to privacy risks mentioned by Dinev et al. (2015) is, for example, the level of cognitive effort during the decision whether to disclose personal information.

Lastly, privacy calculus theory is based on the assumption that the net utility (see the second assumption) determines an individual's intention to disclose his or her personal information. However, information disclosure is not always the primary behavior people have in mind while making privacy-related decisions. Information disclosure is oftentimes merely a

subordinate part of superordinate behaviors. For example, in the information systems context, personal information is usually disclosed while *using* privacy-invasive information systems. Thus, there are different conceptualizations of behavior that all ultimately result in the disclosure of personal information. All these conceptualizations of behavior are treated as being equivalent in extant research (e.g., Malhotra et al. 2004; Sheng et al. 2008; Sledgianowski and Kulviwat 2009; Xu et al. 2009). However, this view might be oversimplified. Depending on whether the focus is on information disclosure itself or information disclosure is only a subordinate aspect of behavior, people might decide differently about their privacy management.

In the following section, it is outlined in how far each of the studies in this thesis addresses the simplifying assumptions of privacy calculus theory described above and which research questions are addressed in particular in the respective papers.

2.3 Thesis Structure and Outline

To address the three simplifications underlying the privacy calculus described in the previous section, several studies were conducted that were published in three papers and together form this cumulative doctoral thesis. The three assumptions are thereby addressed by the three studies in reverse order: from the dependent variable over perceptions onto the mechanism forming these perceptions. This approach was deliberately chosen because identifying the causes of a concept only makes sense if the nature of the concept to be explained has been understood (Hempel 1952). In the following, the motivations for each study will briefly be outlined and the research questions addressed in each study are pointed out. Furthermore, a brief description of the main contributions made by the studies is provided.

The first study (chapter 3) addresses the third assumption of privacy calculus theory, which is that the net utility resulting from benefits and risks of information disclosure determines an individuals' intention to disclose his or her personal information (e.g., Keith et al. 2013; Li et al. 2011; Malhotra et al. 2004; Xu et al. 2009). However, instead of measuring disclosure intentions alone, researchers also often employ the *behavioral intention to use a privacy-invasive information system* as their dependent variable (e.g., Sheng et al. 2008; Sledgianowski and Kulviwat 2009). There are even studies that mix survey items targeted towards usage with items targeted towards disclosure (e.g., Chellappa and Sin 2005; Xu and Teo 2004; Zhou 2011). Thus, it is assumed in privacy research, that decisions concerned with the disclosure of personal information and decisions about using privacy-invasive information

systems incorporating the disclosure of personal information are made coherently. This means that if someone has the intention not to disclose personal information, he or she should also have the intention not to use privacy-invasive information systems that require him or her to do so.

However, the emphasis on the act of information disclosure when people are asked for their *intentions to disclose personal information* may result in a relatively more deliberate answer compared to when they are asked whether they would use a privacy-invasive information system. The reason is, that the conceptualization of behavior as the *intention to use a privacy-invasive information system* puts less emphasis on the act of disclosure itself and may therefore shift the mental process of decision makers towards different aspects. This would be problematic because findings from studies employing one conceptualization would be rendered incomparable with findings found in studies employing the other. This would severely limit the comparability and integratability of results of information privacy studies. The first study, which is presented in chapter 3, therefore addresses the following two research questions:

RQ A.1: Are the behavioral intentions to disclose personal information conceptually different to the behavioral intentions to use a privacy-invasive information system?

RQ A.2: How does the formation of the behavioral intention to disclose personal information differ from the formation of the behavioral intention to use a privacy-invasive information system?

Evidence is provided for the intention to disclose personal information and the intention to use a privacy-invasive information system being the results of different mental processes. In particular, usage intentions seem to reflect what people *want* to do, while the intentions to disclose personal information is more strongly influence by what individuals think they *should* do. As a consequence, the perceived risk of information disclosure is shown to have a stronger impact on an individual's intention to disclose personal information than on ones' intention to use a privacy-invasive information system. The hedonic benefits, in contrast, have a stronger impact on usage than on disclosure intentions.

After clarifying the nature of the two most widely used dependent variables in current information systems privacy research and thereby distinguishing usage and disclosure intentions, the second study focuses in more detail on how individuals process perceptions of benefits and risks of information disclosure when forming an intention to disclose personal

information. In particular, the assumption that the perceived benefits and risks of information disclosure are weighted against each other by evaluating a utility function like

Utility = Benefit - Cost (e.g., Awad and Krishnan 2006)

and behavior depends on whether the result is positive or negative (Li 2012) is investigated.

Based on this utility function, one would expect the benefits and risks to have the same influence on net utility and therefore information disclosure behavior across contexts. However, studies have found results that contradict this expectation. While some studies found the negative effect of the perceived risks of information disclosure to most strongly influence the intention to disclose personal information (Kehr et al. 2015; Keith et al. 2013), others observed that information disclosure intentions are primarily determined by the perceived benefits of information disclosure (e.g. Li et al. 2014; Shibchurn and Yan 2015; Xu et al. 2009). Thus, instead of always evaluating the same utility functions, individuals seem to adapt the weighting of benefits and risks in their utility function depending on the situation.

This variation of weightings can be explained by different mental states called a person's regulatory focus (Higgins 1997), which determines people's sensitivity to negative and positive decision outcomes (Higgins 1998). The regulatory focus is in turn dependent on situational cues, one of which seems to be the risk people are exposed to (Herzenstein et al. 2007; Lee and Aaker 2004) and may therefore change across disclosure contexts. Thus, in the second study presented in chapter 4, the following research questions are addressed:

RQ B.1: Does the regulatory focus determine the weighting of perceived benefits and risks in the decision whether to disclose personal information?

RQ B.2: Is the regulatory focus dependent on the degree of perceived privacy risks in a disclosure situation and does it therefore systematically vary between different disclosure situations?

Based on the results of an experimental survey study it is shown, that when people merely perceive a low level of privacy risks, they, in fact, take a state of incautiousness (named *promotion-focus*) in which behavior is mainly dependent on the perceived benefits of information disclosure. However, if a certain level of privacy-risks is exceeded, people become more vigilant (*prevention-focused*) and base their decision more strongly on the perceived risks of information disclosure.

Chapter 5 then moves from the mechanisms leading from perceptions to behavior towards investigating the mechanism of how risk perceptions are formed at first sight. This means the

study focuses more strongly on the perceptual process of selecting, organizing and interpreting objective cues or properties of information systems when forming perceptions about how much privacy-risk is associated with a certain privacy-invasive information system. Therefore, it addresses the first assumption of privacy calculus theory noted above: individuals are able to evaluate the perceived privacy risks associated with the disclosure of personal information. This assumption has never been empirically validated to date. As mentioned in section 2.2.2, the perceptual process requires individuals to relate information to internal knowledge and values. If an individual lacks sufficient knowledge to relate the stimuli he or she observes to, they can only form vague feelings based on heuristics of how high privacy risks might be (Slovic et al. 2000). However, if provided with external information facilitating evaluation, confidence in one's own risk assessment would increase. Such increased confidence in a perception has been shown to in turn increase the sensitivity to the perception (Lichtenstein and Burton 1988). This is because when external information confirms an individuals' assessment of whether a certain manifestation of a product attribute is good or bad, they regard their own evaluation of this attribute as more valid and therefore place greater emphasis on their perception in their decision-making (Hsee and Zhang 2010). Hence, the impact of a privacy risk perception might depend on how the risk perception was formed.

This potential coupling between the formation and impact of perceived privacy risks has not been considered in information systems privacy research to date. This is problematic because if proven true, measurements of perceived privacy risks and their empirically observed correlations with behavioral consequences would be rendered incomparable across studies due to differences in available reference information. We therefore question that individuals are always able to form confident privacy risk perceptions independent of external reference information. As a consequence, their effect may vary with this amount of reference information available due to differences in confidence in ones' own risk perceptions. Accordingly, the following research questions are evaluated:

RQ C.1: Are users of privacy-invasive information systems able to evaluate the privacy risk associated with the disclosure of a certain amount of personal information independently?

RQ C.2: Do perceived privacy risks influence behavior differently when they are formed in conditions that facilitate evaluation compared to when they are difficult to evaluate?

Based on an experimental survey study among 233 participants evidence is provided, that the presence of reference information significantly increases the effect of the amount of data

gathered by a privacy-invasive application on the perceived risk of information disclosure as well as the effect of the perceived risks of information disclosure on the behavioral intention to use a privacy-invasive information system.

In the following chapters these studies will be presented in the form they were originally published in the order they were addressed above. The only changes that were made concern the figure titles. References to the papers these figures relate to were added to increase the clarity of the list of figures. After these three chapters, the thesis closes with a summarizing depiction of its contributions.

3 Paper A: Distinguishing Usage and Disclosure Intentions in Privacy Research

Title

Distinguishing Usage and Disclosure Intentions in Privacy Research: How Our Two Selves Bring About Differences in the Effects of Benefits and Risks

Authors

Brakemeier, Hendrik, Technische Universität Darmstadt, Germany

Widjaja, Thomas, Universität Passau, Germany

Buxmann, Peter, Technische Universität Darmstadt, Germany

Publication Outlet

Proceedings of the 24th European Conference on Information Systems (ECIS 2016), Istanbul, Turkey

Abstract

Two different conceptualizations of behavioral intentions are oftentimes interchangeably used as dependent variables in privacy research: Intentions to disclose personal information to an information system (IS) and intentions to use an IS (and thereby disclose information). However, the assumption that those two conceptualizations are indeed interchangeable has not been tested yet and, if rebutted, imposes limitations when comparing and integrating results of studies using either of them. By transferring the multiple selves problem to IS privacy research, we develop theoretical arguments and provide empirical evidence that those two intentions are a) conceptually different and b) formed in different cognitive processes. A vignette-based factorial survey with 143 participants is used to show, that while risk perceptions have more impact on disclosure intentions than on usage intentions, the opposite holds for hedonic benefits.

Keywords

disclosure intention, hedonic benefits, multiple selves problem, information privacy, privacy calculus, usage intention, utilitarian benefits

3.1 Introduction

A vast amount of IS privacy literature deals with the question, under which circumstances people are willing to have their personal information gathered and processed by information systems (IS). As disclosure behavior is oftentimes difficult to observe and measure, these studies regularly rely on self-reported behavioral intentions, making them one of the most commonly used dependent variables in privacy research (Smith et al. 2011). However, while some researchers employ the *behavioral intentions to disclose personal information* (e.g., Keith et al. 2013; Li et al. 2011; Malhotra et al. 2004; Xu et al. 2009) others make use of the *behavioral intentions to use a privacy-invasive IS* (e.g., Sheng et al. 2008; Sledgianowski and Kulviwat 2009). Some studies even mix survey items targeted towards usage with items targeted towards disclosure (e.g., Chellappa and Sin 2005; Xu and Teo 2004; Zhou 2011). Furthermore, some studies aiming to build theory to explain usage intentions build upon findings targeting disclosure intentions (Sheng et al. 2008) and vice versa (Zimmer et al. 2010a).

Yet, although addressing the same behavior, using these conceptualizations interchangeably might lead to confounding research results. In particular, the emphasis on the act of information disclosure when people are asked for their *intentions to disclose personal information* may result in a relatively more deliberate answer. The conceptualization of the *intention to use a privacy-invasive IS* in contrast puts less emphasis on the act of disclosure and may therefore evoke different responses. This is problematic, because findings based on one of the conceptualizations may differ from those based on the other, thus imposing limitations when comparing or integrating results of studies using either of them or even (inadvertently) mixing them. Therefore, we address the following two research questions:

RQ1: Are the behavioral intentions to disclose personal information conceptually different to the behavioral intentions to use a privacy-invasive IS?

RQ2: How does the formation of the behavioral intention to disclose personal information differ from the formation of the behavioral intention to use a privacy-invasive IS?

We contribute to the elucidation of the first research question by showing (based on a factor analysis) that the *intention to disclose information* and the *intention to use a privacy-invasive IS* are in fact statistically distinguishable. We further investigate *why* this is the case and develop a theory regarding the formation of those two behavioral intentions: Drawing upon the privacy calculus theory (Li 2012) and the multiple selves problem (Bazerman et al. 1998), we argue, that different cognitive processes underlie the formations of *intentions to disclose*

personal information and *intentions to use a privacy-invasive IS* and they are therefore formed differently. Based on the results of a vignette-based factorial survey among 143 participants, we provide empirical evidence that the perceived risk of information disclosure has a stronger impact on the behavioral intention to disclose information than on the intention to use a privacy-invasive IS. The opposite holds for hedonic benefits provided by the IS, which have more influence on the intention to use the IS than on the intention to disclose information to it.

The remainder of the paper is structured as follows: We first outline the theoretical background for our study by transferring the multiple selves problem to IS privacy research and thereby develop theoretical arguments that the two intentions are formed in different cognitive processes (and are therefore different). Thereafter we describe the methodology employed to investigate the deduced hypotheses followed by the presentation of our findings. RQ1 is investigated with a factor analytical approach, which is followed by the net regression approach proposed by Cohen et al. (2003) to examine RQ2. After the discussion of the results, the paper closes with a depiction of limitations of our study and promising fields for future research.

3.2 Theoretical Background

3.2.1 Conceptual Differences between Privacy-Related Behavioral Intentions

Information systems regularly require their users to have personal information gathered and processed by the system. Thus, one of the prevalent questions in IS-privacy literature is under which circumstances people are willing to accept this invasion of their privacy. As real behavior is oftentimes difficult to observe and measure, privacy research is regularly relying on self-reported behavioral intentions as an indicator of actual disclosure (Smith et al. 2011). However, besides the conceptualization of *behavioral intentions to disclose personal information* and asking people for the extent to which they would reveal their personal information (e.g., Malhotra et al. 2004; Xu et al. 2009; Zimmer et al. 2010b), privacy researchers also utilize *behavioral intentions to use a technology* as outcome of interest, asking people whether they would use a service or a technology (e.g., Sheng et al. 2008; Sledgianowski and Kulviwat 2009). Some publications are even mixing items of these two conceptualizations of behavioral intentions. For example Xu and Teo (2004) measure the "intentions to use a LBS [location-based-service]" by asking for the extent to which people agree to statements like "I would disclose my personal information to use this type of LBS

from the service provider in the next 12 months" but also "I intend to use this type of LBS in the next 12 months" (Xu and Teo 2004, p. 801). Furthermore, some papers investigating the *behavioral intentions to use a privacy-invasive IS* build upon results found for the *behavioral intentions to disclose personal information* in their theory development (e.g., Sheng et al. (2008) investigate the "Intention to Adopt" a personalized ubiquitous-computing-system and build upon Malhotra et al. (2004), who are studying the "Intention to Give Information" in return for a free membership worth 50$) and vice versa (Zimmer et al. 2010a).

The underlying assumption of this tantamount utilization of the two conceptualizations seems to be, that they are conceptually equivalent. A reason why this assumption prevails might be, that in the IS privacy context, information is usually disclosed while using a privacy-invasive IS, which is why the intentions are somewhat interlinked. However, Bazerman et al. (1998) have found that although intentions may be interlinked by referencing the same set of options, individuals often evaluate these options from two different perspectives, "almost as if they are comprised of two competing selves: a *want self* and a *should self*" (Bitterly et al. 2014, p. 2). While the latter can be described by adjectives like rational, cognitive, thoughtful and "cool headed", the former is relatively more emotional, affective, impulsive and "hot headed" (Bazerman et al. 1998). These two selves coexist in individuals even though they differ with regard to their preferences. While the *want self* is attracted by the realization of immediate benefits, the *should self* is more far-sighted and interested in maximizing long term outcomes (Milkman et al. 2008; Milkman et al. 2009; Thaler and Shefrin 1981). For example Schelling (1985) notes that "everybody behaves like two people, one who wants clear lungs and long life and the other who adores tobacco, or the one who wants a lean body and the other who wants dessert […]". Based on these findings, a characterization of when two options differ in their attractiveness for the *want self* and the *should self* can be obtained by comparing the short- and long term utility of the options. Given these two time periods and two options, one option has relatively more *want* and less *should* characteristics when this option is associated with greater utility in the short term but less utility in the long term compared to the *should* option (Milkman et al. 2008).

The decisions people face when they are asked for their behavioral intentions towards a privacy-invasive IS fit this scheme of *want* and *should* options. The option with the higher utility in the short term often is to use an IS and disclose personal information, because it allows to realize utility in the forms of monetary or time savings, pleasure, self-enhancement or social adjustment (Tam et al. 2002). However, by giving up privacy, a person loses the

control over his personal information. According to Acquisti and Grossklags (2003), "That loss of control multiplies, propagates, and persists for an unpredictable span of time. […] For example, a small and apparently innocuous piece of information might become a crucial asset in the right context." Not using the IS and thereby maintaining one's privacy thus "… represents something akin to getting an insurance against future and only uncertain risks" (Acquisti 2004, p. 25). Therefore, in the long term perspective the disclosure of information coming with the usage of a privacy-invasive IS is oftentimes inferior compared to maintaining one's privacy. Thus, non-disclosure is the *should* option compared to using the IS (*want* option).

The two conceptualizations of behavioral intentions as *intentions to disclose personal information* and *intentions to use a privacy-invasive IS* differ with regard to how central the disclosure of information is to the concept. While the former directly and exclusively addresses the act of disclosure itself, the behavioral intention puts more emphasis on the functionalities of the respective technology while moving the awareness away from the act of disclosure and considering it more as subordinate aspect of usage. As a consequence, when an individual is asked for its intention to use a privacy-invasive IS, there is no strong *should* option, because the negative long term effects are not central to the construct and therefore less likely to be applied in judgment (Roese and Sherman 2007). In this case, the *want* self can follow his "own" preferences without being restricted by the *should* self. On the other hand, when one is asked for one's intention to disclose personal information, the focus on the potentially negative consequences in the long term makes it obvious that the decision is between a *should* and a *should-not* option. Research has shown that in cases were individuals are aware of the fact that the decision is a choice between *should* and *should-not,* the decision is affected strongly by the *should* self (Bazerman et al. 1999; Hsee 1996a; Okada 2005). As a consequence, when the intention to disclose personal information and the intention to use a privacy-invasive IS are formed by different selves with different preferences, they also represent different concepts. Our hypothesis regarding RQ 1 therefore is the following.

H1: The intention to disclose personal information and the intention to use a privacy-invasive IS are statistically distinguishable constructs.

3.2.2 Want- and Should-Self in the Privacy Calculus

To further elaborate why the two behavioral intention differ, we consider their formation (RQ2). We therefore integrate differences in the preferences of the want and *should self* into

the privacy calculus theory (Laufer and Wolfe 1977). This theory posits, that when individuals are faced with the decision between giving up and maintaining their privacy, they undertake trade-offs whether a certain loss of privacy is acceptable for the benefits gained in exchange (Laufer and Wolfe 1977). The central constructs of privacy calculus theory are *perceived benefits* and *risks of information disclosure*, which are weighted against each other and result in a *behavioral intention (to disclose personal information* or *to use a privacy-invasive IS* respectively) (Li 2012; Smith et al. 2011). Thus, regarding the formation of usage and disclosure intentions, privacy calculus theory suggests that both are influenced by the same set of antecedents. However, due to the different preference structures of the *want self* and the *should self*, each antecedent can be of a certain importance to the *want self* and of a certain importance (which might be equal, higher or lower) to the *should self*. A lower importance of an antecedent should result in a smaller effect of this antecedent on the decision outcome. The goal of the following section is to discuss the importance of the *perceived risk of information disclosure* and *perceived benefits of information disclosure* (Li 2012; Smith et al. 2011) for the *want self* and the *should self*, and thereby deduce hypotheses about differences between their effects on the *behavioral intention to use a privacy-invasive IS* (formed by the *want self*) and the *behavioral intention to disclose personal information* (formed by the *should* self).

As the importance of each antecedent for *want* and *should self* determines its magnitude of effect on the two behavioral intentions, the question is what type of antecedents are important to the two selves. As noted in the previous section, the *want self* is attracted by the realization of immediate benefits while the *should self* is more far-sighted and interested in maximizing long term outcomes (Milkman et al. 2008; Milkman et al. 2009; Thaler and Shefrin 1981). Thus, if an antecedent determines the degree to which a decision is associated with positive utility in the short term, it is always important to the *want self*. However, from a rational perspective (which is reflected by the *should* self) people are often unsure whether utility that is not of practical character, but comes in the form of enjoyment or other hedonic pleasures, is a legitimate choice criteria. The *should self* therefore tends to hesitate to appreciate attributes determining such hedonic utility and only considers attributes of practical matter (Okada 2005). On the other hand, antecedents representing potentially negative long term consequences that come with the realization of an immediate benefit have been found to be more important to the *should self* than they are to the *want self*, because people frequently feel they *should* make decisions that maximize their long term utility, even when they have to forego short term benefits (Milkman et al. 2008). Against this background we first examine

the importance of the *perceived risk of information disclosure* (H2) for the two selves and then proceed with the *perceived benefits of information disclosure* (H3 and H4).

The *perceived risk of information disclosure* is defined as "[…] the expectation of losses associated with the release of personal information […]" (Xu et al. 2009, p. 149). This refers to the potential of significant losses in the future, may it be due to data leaks or intentional misuse of the data by the provider it was intentionally disclosed to. Thus, the perceived risk of information disclosure determines the extent to which negative long term consequences are anticipated and is therefore more important in the preference structure of the *should self* than it is in that of the *want self*. As a consequence the negative effect of the perceived risk of information disclosure on the behavioral intention to disclose personal information (formed by the *should self*) should be stronger than the negative effect on the intention to use a privacy-invasive IS (formed by the *want self*). This is reflected in the following hypothesis:

H2: The perceived risk of information disclosure has a stronger negative impact on the reported intention to disclose personal information to the provider of a privacy-invasive IS compared to the impact on the reported intention to use the IS. ($\beta_{R\text{-}IU} > \beta_{R\text{-}ID}$)

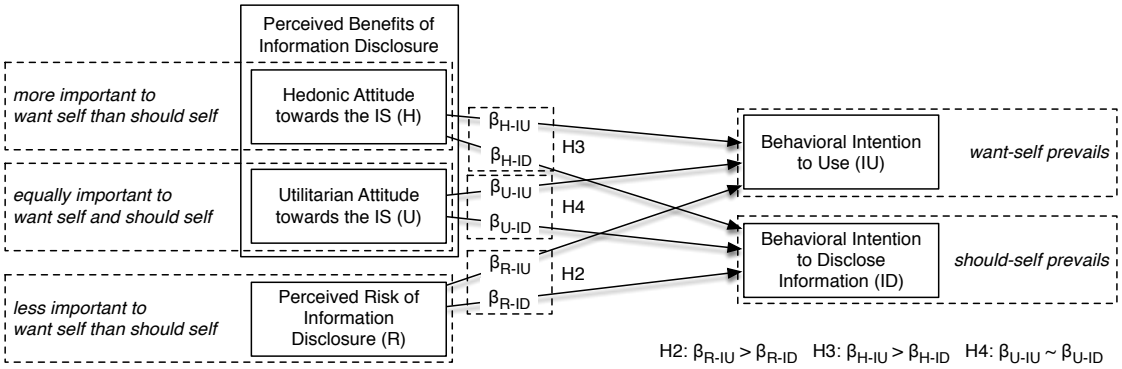

Figure 1: Research Model (Paper A).

To categorize *perceived benefits of information disclosure* and derive the research model depicted in Figure 1, one more distinction has to be made. As noted before, not all utility is equally important to the *want* and *should* self (Chitturi et al. 2007): An antecedent determining the positive utility in the short term is always important to the *want self*, but it is only important to the *should self*, if the underlying utility is of practical character and therefore appears to be rational (Okada 2005). The one-dimensional conceptualization of benefits in the privacy calculus does not distinguish different types of benefits in this regard. Theories from the area of hedonic consumption (Hirschman and Holbrook 1982) are more precise by distinguishing the *utilitarian* and the *hedonic* benefits provided by a product. The

former denotes the capability of a product to fulfil pragmatic goals and accomplish functional tasks (Strahilevitz and Myers 1998). The hedonic quality of a product serves more emotional needs for multisensory experiences and pleasure (Hirschman and Holbrook 1982). We thus extended the basic privacy calculus model by re-conceptualizing the one-dimensional construct of perceived benefits with the hedonic and the utilitarian attitude towards the IS (see Figure 1) to account for the different effects of hedonic and utilitarian benefits (Voss et al. 2003). We use attitudes instead of concrete beliefs about benefits in this study, because a certain benefit, for example a chatting functionality, is likely to contain utilitarian and hedonic aspects (like enabling exchange of information and satisfaction of communication needs) (Alba and Williams 2013). In most privacy studies, however, benefits are assessed by measuring in how far a system provides certain functionalities, for example by asking people for their agreement to statements like "I get to know new people through the OSN [Online Social Network]" (Krasnova et al. 2010). Thus, attitudes allow differentiating the two dimensions of benefits with greater accuracy (Babin et al. 1994; Batra and Ahtola 1991; Ja-Chul et al. 2010).

Although people intrinsically value hedonic benefits and *want* to incorporate them in their decisions (Okada 2005), those hedonic benefits tend to "[…] be more difficult to evaluate and quantify than the practical, functional benefits […]" (Okada 2005, p. 44). As a consequence, the *should* self tends to hesitate to consider the hedonic dimension of benefits due to their subjectivity and irrationality (Okada 2005). This means hedonic product benefits are more relevant to the *want* self compared to the *should* self. Given that the intention to use is evaluated from a *want* perspective while the intention to disclose is based on the preferences of the *should self*, the following hypothesis can be derived:

H3: The hedonic attitude towards an IS has a stronger positive impact on the reported intention to use a privacy-invasive IS compared to the impact on the reported intention to disclose personal information to the provider of the IS. ($\beta_{H\text{-}IU} > \beta_{H\text{-}ID}$)

The problem of lacking justifiability described above does not concern the utilitarian dimension of benefits. These are easier to quantify and thus considering them in a decision is not perceived as being unreasonable or a violation of one's ought's by the *should self* (Okada 2005). As a consequence, utilitarian benefits provided by privacy-invasive IS are not only relevant for the *want self* but also for the *should self*. Thus, the degree to which these are taken into consideration is not affected by whether the *want self* or the *should self* prevails and the following hypothesis ensues.

H4: The utilitarian attitude towards an IS has the same positive impact on the reported intention to use a privacy-invasive IS and the reported intention to disclose personal information to the provider of the IS. ($\beta_{U\text{-}IU} \sim \beta_{U\text{-}ID}$)

3.3 Research Method

We employed a 2 (utilitarian benefit – high/low) x 2 (hedonic benefit – high/low) x 2 (risk – high/low) between-subjects scenario-based factorial survey design (Rossi and Nock 1982) to investigate the relationships of the independent variables with the intention to disclose as well as the intention to use in an adoption decision of a fitness wristband as privacy-invasive IS. The scenario-based factorial survey approach is especially suitable for our research, because contextual variables have been found to have a strong influence on privacy-related decisions (Smith et al. 2011) and scenario-based factorial surveys allow to maintain a high degree of control over the independent and contextual variables and thereby minimize the effects of disturbance variables (Aviram 2012; Finch 1987; Xu and Teo 2004).

A wearable technology was deliberately chosen as context for our study to control for cases in which disclosure of data is to some extent optional and no prerequisite for usage. In such situations the intention to use may exceed the intention to disclose personal information for other reasons than the multiple selves problem. For example, one could plan to provide fake data to a system and thus the intention to provide (real) data to an IS may be lower than the intention to use it. This is not possible in the context of wearable computing, because data is automatically collected by sensors. We targeted participants aged 16 to 24, because wearables were found to be most appealing to this age group (GfK 2013) and contacted them via different sports clubs, university lectures and social media platforms.

3.3.1 Manipulations of Independent Variables

Our study was designed as online survey. The participants were first asked to provide demographic information. Afterwards they were instructed to imagine themselves to be in a situation in which they were confronted with a fitness-wristband possessing different features to manipulate the three independent variables: hedonic benefits, utilitarian benefits and risk. Using such a hypothetical scenario is a common approach in IS privacy research (Hann et al. 2007; Malhotra et al. 2004; Pan and Zinkhan 2006). The features of the wristband in question were varied between participants in such a way that one participant only viewed one of the eight vignettes resulting from the 2 x 2 x 2 factorial design.

Either offering a reduced or an extensive set of practical functions manipulated the utilitarian benefit provided by the wristband. Hedonic benefits were manipulated by means of gamification. Gamification is "[…] the use of game design elements in non-game contexts" (Deterding et al. 2011, p. 10) to "enhanc[e] a service with affordances for gameful experiences in order to support user's overall value creation" (Huotari and Hamari 2012, p. 19). While the wristband low on hedonic benefits did not incorporate gamification, the wristband high on hedonic benefits was gamified. Risk was manipulated via different data handling policies. All textual descriptions are given in Appendix 1.

3.3.2 Measurement of Independent and Dependent Variables

Established scales were used to measure all constructs. The perceived *utilitarian* and *hedonic attitudes towards the wristband* were measured with the scales developed by Voss et al. (2003). The former construct is defined as "[…] the portion of a person's attitude resulting from perceptions of the functional performance of the product […] or its expected performance" (Bruner et al. 2001, p. 187) while the latter relates to "[…] those facets of a product, that relate to the multisensory, fantasy and emotive aspects of one's experience with products" (Hirschman and Holbrook 1982, p. 92). The items for the *perceived risk of information disclosure* were adopted from Xu et al. (2009).

The dependent variables are both behavioral intentions, which are defined as "[…] the degree to which a person has formulated conscious plans to perform or not perform some specified future behavior" (Warshaw and Davis 1985, p. 214). In our case, the specified behaviors are (1) disclosing personal information and (2) using the privacy-invasive IS. The *behavioral intention to disclose personal information* was measured by an established scale asking respondents to specify the extent to which they would reveal their personal information using sematic differentials like unlikely/likely or unwilling/willing (Malhotra et al. 2004; Wakefield 2013; Xu et al. 2009). To measure the *behavioral intention to use the wristband* we employed the scale used by Sheng et al. (2008). An overview of all indicators is given in Appendix 2.

3.4 Data Analysis and Results

We received a total of 207 completely filled out survey responses. Only participants that stated to do sports at least once a week were included in further analyses, because they represent the target group for the wearable presented in the scenarios. People not doing sports on a regular basis might also not be able to assess in how far the given technology is practical and thus have difficulties in estimating the utilitarian attitude towards it. This resulted in 143

responses that entered our analyses. The distribution of survey participants on the groups of the factorial design is shown in. Please note that nonorthogonal data, that is, an unequal number of observations per group, is unproblematic as we employ Cohen's net regression approach (Cohen et al. 2003; Cohen et al. 1990, see section 4.2) to analyze our data (Brown et al. 2011; Overall et al. 1975). There are more male participants in our sample (75.5%) than females (24.5%). The majority (51.0%) were between 20 and 24 years of age and 77% were in the age group of 17-24 years. The youngest participant was 17, the oldest 55 years of age.

risk		high		low	
hedonic benefits		high	low	high	low
utilitarian benefits	high	18	23	14	14
	low	20	18	18	18

Table 1: Distribution of participants on groups of the factorial design (Paper A).

3.4.1 The Factor Structure of Disclosure and Usage Intentions

To test H1, we employed a factor-analytic approach to investigate the correlation structure between the items operationalizing the intention to use and those operationalizing the intention to disclose. This allows to investigate how many statistically distinguishable constructs are represented by our set of usage- and disclosure-related items (Gulliksen 1968; Henson and Roberts 2006). We first performed an exploratory factor analysis to investigate factor loadings. A confirmatory factor analysis was then performed to compare the fits of a single-factor and a two-factor model as described by Bagozzi and Yi (2012).

The Kaiser-Meyer-Olkin test of sampling adequacy (.88) (Kaiser 1970) and Bartlett's test of sphericity ($\chi^2 = 2539.6$, $p < .001$) (Bartlett 1950) indicate that the data is suitable for factor analysis (Dziuban and Shirkey 1974). Principal axis factoring was used as extraction method with the Kaiser criterion (Kaiser 1960) to determine the number of factors to extract (those with eigenvalues > 1). This resulted in two factors, the first with an eigenvalue of 4.7 and explaining 67.3% of the overall variance and the second with an eigenvalue of 1.47 and explaining another 21.06% of the variance. The first factor that was not retained had an eigenvalue of .447. As usage of and disclosure of information to the wristband are interlinked, it is reasonable to expect the emergence two factors that are correlated. We thus used a promax rotation, as it is an oblique rotation method and does not force the factors to be uncorrelated (Gorsuch 1983). The resulting factor pattern matrix is given in Table 2. The correlation between the two factors is .528.

All items targeted towards usage load strongly on the second factor (all > .94) while loadings on the first factor are all below .03. The items targeted towards disclosure on the other hand all load on factor one with loadings > .89 except for ID4 with a loading of .69. The loadings on factor two are .045 and lower. Thus, although using the wristband presented to the participants without disclosing personal information is not possible, the intentions to disclose personal information to its provider and the intention to use it seem to constitute two conceptually different constructs.

A confirmatory factor analysis (Jöreskog 1969) was then employed to compare the fit of a single-factor and a two-factor model (Bagozzi and Yi 2012). Therefore both models were estimated using SPSS Amos 22. Following the recommendations of Bagozzi and Yi (2012) we report the NNFI, CFI, RMSEA and SRMR for both models in Table 3. Values for the NNFI and CFI should exceed 0.95 to indicate good model fit (Hu and Bentler 1999). This is given for the two-factor model. Values for the RMSEA should fall below .1 (MacCallum et al. 1996), which is slightly lower than the .11 obtained for the two-factor model. However, Kenny et al. (2014) have shown that the RMSEA underestimates model fit for models with low degrees of freedom (13 in our case), which is why we deem .11 acceptable. The observed value for the SRMR is well below the threshold of .08 (Hu and Bentler 1999). The single-factor model clearly shows bad fit and violates all criteria for good model fit. Therefore, hypothesis 1 is supported. The intention to disclose personal information and the intention to use a privacy-invasive IS should be considered as two conceptually different constructs.

	Communalities	Factor 1	Factor 2
IU1	.919	.028	***.943***
IU2	.924	.008	***.957***
IU3	.961	-.008	***.984***
ID1	.876	***.943***	-.013
ID2	.893	***.961***	-.031
ID3	.846	***.895***	.045
ID4	.509	***.690***	.042

Table 2: Communalities and factor structure (principal axis factoring and promax rotation, Paper A).

	Criterion for fit	Single-factor model	Two-factor model
NNFI	> .95	.32	.97
CFI	> .95	.55	.98
RMSEA	< .1	.53	.11
SRMR	< .08	.20	.03

Table 3: Results of confirmatory factor analysis for single- and two-factor model (Paper A).

3.4.2 Differences Between the Formations of Disclosure and Usage Intentions

To test hypotheses 2 to 4 we used the net regression method devised by Cohen et al. (1990). This method is applied here, because we do not want to test whether the effect of an independent on a dependent variable is significant, but whether the *difference between the effects* of one independent on two different dependent variables is statistically significant (see H2-H4). Cohen's net regression approach explicitly allows to test "[…] whether a set of predictors have, individually and collectively, a comparable relationship to two ore more different dependent variables in a single sample" (Cohen et al. 2003, p. 642). Thus, by employing net regression, the common practices of noting that an independent variable significantly influences one outcome but not the other, or "... that some estimate of magnitude of effect appears to be larger for one outcome than another, without assessment of the significance of these differences, can be avoided." (Brook et al. 1995, p. 87)

The approach consists of three steps: After standardizing all variables, a first regression is carried out to compute the regression coefficients for one of the dependent variables. Then the deviations between the data points measured for the second dependent variable and the corresponding values predicted by the regression equation for the first dependent variable are determined. If the effect of an independent variable on both dependent variables would be the same, this difference should not be dependent on this independent variable, If the difference is however significantly dependent on one of the independent variables, this means this variable has a significantly different influence on the two dependent variables. A second regression is therefore used to identify any structure in these deviations that can be attributed to the set of

independent variables. If the coefficients in this regression turn out as significant, this means the independent variable has in fact a different effect on the two dependent variables (Cohen et al. 2003). Before carrying out the actual analysis, the validity of the applied measures and the successful manipulation of the independent variables by our scenarios were verified.

3.4.2.1 Validity of the Survey Instrument

The internal consistency of the constructs was evaluated by means of Cronbach's α. The results are shown in Table 4 along with descriptive statistics. A second factor analysis including all items and promax rotation was carried out to check convergent validity (Straub 1989). All Items loaded higher on their intended construct than on any other with .271 as the highest cross loading. Inter-construct correlations can also be found in Table 4. A correlation of .613 between the utilitarian and the hedonic attitudes was found. However, variance inflation factors did not point to problematic multicollinearity between the independent variables during our regression analyses. All values were 1.956 or below (see Table 4) and therewith well below the proposed threshold of 10 (Cohen et al. 2003). Manipulation checks indicate successful manipulations of the perceived hedonic ($F = 6.839$, $p = .01$) and utilitarian ($F = 3.564$, $p = 0.06$) attitudes towards the wristband and the perceived risk ($F = 7.288$, $p = .008$).

	No. of Items	Mean	Std. Dev.	Cron-bach's α	utilitarian attitude (U)	hedonic attitude (H)	perceive d risk (R)	intention to disclose (ID)	Variance inflation factors
U	5	4.512	1.273	.874					1.956
H	5	4.403	1.408	.875	.613				1.845
R	3	4.177	1.548	.863	-.167	-.117			1.082
ID	4	3.080	1.654	.938	.490	.424	-.385		
IU	3	4.457	1.987	.973	.625	.507	-.215	.487	

Table 4: Descriptive statistics, Cronbach's α, variance inflation factors and correlations among all variables (IU = behavioral intention to use the wristband, Paper A).

3.4.2.2 Net Regression Analysis

As depicted before, we employed a 2 (utilitarian benefit – high/low) x 2 (hedonic benefit – high/low) x 2 (risk – high/low) factorial survey design to generate variance in the independent variables. A common approach to analyze such data is dummy coding the group assignment for each factor. However, this only allows an analysis on the level of groups in the factorial design, because one would implicitly assume that all participants in one group perceived the same risk, hedonic attitude and utilitarian attitude towards the wristband. In line with Komiak

and Benbasat (2006) and Keith et al. (2010), we used the manipulation check measures as independent variables instead, in order to analyze the data on the level of individual participants and thereby eliminate this shortcoming. This is also advantageous compared to using binary variables specifying the manipulation the participant was exposed to, because "[…] causation is conceived as a relation between variables or constructs in a theory and not between observed objects or events in the world. […] It is more sound theoretically to model cause and effect between theoretical variables which, in turn, are operationalized by measures of those variables" (Bagozzi 1977, p. 211f.). This means that the behavioral intention is not influenced by the presence or absence of (for example) the gamification-feature, but by the hedonic attitude towards the product resulting from its presence or absence.

According to the net regression approach of Cohen et al. (1990) presented above, we first standardized all variables and computed a regression of the intention to disclose on our three independent variables to obtain the standardized regression weights of the hedonic attitude, the utilitarian attitude and the perceived risk ($\beta_{H\text{-}ID}$, $\beta_{U\text{-}ID}$ and $\beta_{R\text{-}ID}$ – see Figures 3 and 4). The result is shown as model 1 in Table 5. We also report the results of the regression of the intention to use on the three independent variables ($\beta_{H\text{-}IU}$, $\beta_{U\text{-}IU}$ and $\beta_{R\text{-}IU}$ – model 2 in Table 5), although this is not necessary for the approach.

The results show significant effects of those independent variables hypothesized to be more important to the *should self* (utilitarian attitude and perceived risk, see section 2.2) on the (*should self* dominated) intention to disclose. The effect of the hedonic attitude is insignificant, which is consistent with our expectations. The intention to use the wristband seems to be determined primarily by the hedonic and utilitarian benefits. The effect of the perceived risk is weaker, but still significant at the 5%-level.

To examine whether those differences in regression coefficients are significant, we proceeded according to the net regression method (Cohen et al. 2003; Cohen et al. 1990). We used the regression coefficients obtained by regressing the intention to disclose to compute the vector of predicted values for the disclosure intentions. These scores were then subtracted from the measured values for the intention to use. A second regression was carried out with this difference as dependent variable and the same set of independent variables. The (unstandardized) coefficients of this regression now denote the difference between the independent variable's effect on the intention to use and the intention to disclose ($\beta_{H\text{-}IU}$ - $\beta_{H\text{-}ID}$, $\beta_{U\text{-}IU}$ - $\beta_{U\text{-}ID}$, $\beta_{R\text{-}IU}$ - $\beta_{R\text{-}ID}$) and their p-values denote whether the difference is significant (Cohen et al. 2003; Cohen et al. 1990). The result of this last regression is shown as model 3

in Table 5. Please note, that the beta coefficients of model 1 and the unstandardized coefficients of model 3 add up to the betas of model 2.

		Unstandardized Coefficients		Standardized Coefficients	t	p
		B	SE	β		
Model 1 (dependent variable: intention to disclose - coefficients are $\beta_{*\text{-ID}}$)	R			-.307***	-4.492	< .001
	H			.122	1.362	.175
	U			.392***	4.261	< .001
	$R = .631; R^2 = .398; AdjR^2 = .385$					
Model 2 (dependent variable: intention to use - coefficients are $\beta_{*\text{-IU}}$)	R			-.134*	-2.062	.041
	H			.311***	3.665	< .001
	U			.383***	4.384	< .001
	$R = .676; R^2 = .458; AdjR^2 = .446$					
Model 3 (dep. var.: intention to use minus predicted values for intention to disclose (by model 1)	R (H2)	.173**	.065		2.669	.009
	H (H3)	.189*	.085		2.231	.027
	U (H4)	-.009	.087		-.104	.917
	$R = .309; R^2 = .096; AdjR^2 = .076$					

Table 5: Results of the net regression analysis (R = perceived risk of information disclosure, H = hedonic attitude, U = utilitarian attitude, Paper A).

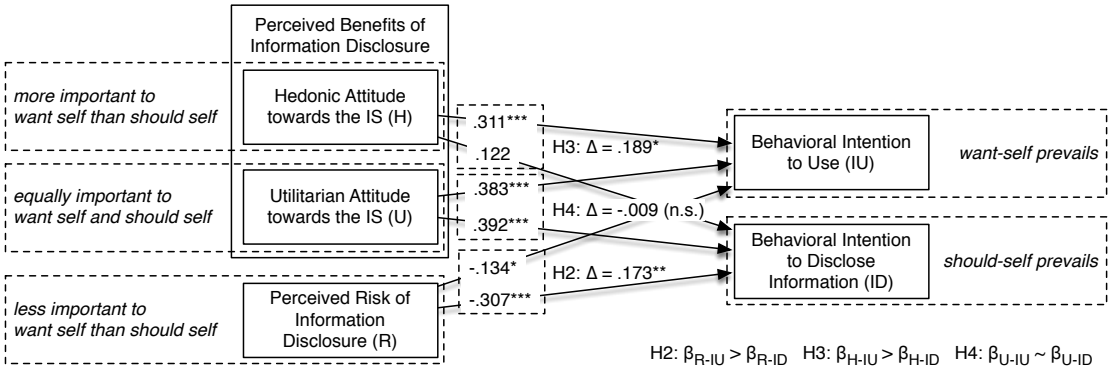

Figure 2: Research model with estimated regression parameters (Paper A).

This last regression allows us to make direct inferences about our hypotheses 2 to 4. The effect of the perceived risk of information disclosure increased from -.307 to -.134 between the regression of the intention to disclose and the intention to use, with the difference being significant according to model 3 ($\beta_{R\text{-}IU} - \beta_{R\text{-}ID} = .173^{**}$, p = .009). The effect of the perceived risk on the disclosure intention is therefore stronger than on the usage intention and H2 is supported. The regression coefficient of the hedonic attitude towards the wristband is significantly higher when regressing the intention to use compared to when the intention to disclose is regressed. Therefore, our data supports H2 ($\beta_{H\text{-}IU} - \beta_{H\text{-}ID} = .189^{*}$, p = .027). The difference between the impact of the utilitarian attitude towards the wristband on the intention

to use and the intention to disclose is not significant according to model 3 ($\beta_{U\text{-}IU} - \beta_{U\text{-}ID} = -.009$, $p = .917$) and thus supporting H3. An overview of the effects is depicted in Figure 2.

3.5 Discussion

The goal of our study was to prove the behavioral intention to use a privacy-invasive IS and the intention to disclose personal information to it to be different conceptualizations (RQ1) and represent outcomes of different types of deliberations (RQ2) despite being used interchangeably in research on privacy-invasive technologies (e.g., Chellappa and Sin 2005; Xu and Teo 2004). We examined the relationship between these two behavioral intentions in the context of a wearable technology, which stands out in respect to the linkage between usage and information disclosure. Despite this logical linkage, we found significant differences between the intention to use such a technology and the intention to disclose one's personal information to it. While the latter seems to underlie an evaluation taking into account mainly the perceived risk and utilitarian attitude towards the IS, the intentions to use a privacy-invasive IS are influenced primarily by the utilitarian as well as the hedonic dimension of attitudes towards an IS but neglecting the perceived risk.

The contributions of this study to IS privacy research are threefold. A first contribution is the distinction of the two conceptualizations of behavioral intentions. As we have shown, there exist profound differences between usage and disclosure intentions. This imposes important limitations when comparing or integrating results of studies using different intentions, because relationships found for the intention to disclose personal information might not necessarily also hold when investigating the behavioral intention to use privacy-invasive IS and vice versa. Future research should therefore be cautious when building theory from studies employing a different behavioral intention. The distinction of disclosure and usage intentions also raises the question, which behavioral intention is appropriate for which purpose in privacy research. While one intention might be better suited to analyze perceptions of people regarding privacy-invasive IS the other might fit better to predict actual behavior.

This question leads to our second contribution, the transfer of the distinction between *want* and *should* options (Bazerman et al. 1998) to the IS privacy context, and thereby the proposition of a new perspective on privacy-related cognitive processes. As we have shown, people seem to simultaneously hold different points of view regarding acts of information disclosure. This is in line with the multiple selves problem (e.g., Bazerman et al. 1998; Khan et al. 2005; O'Connor et al. 2002). These findings also support the notion of immediate

gratification as having a strong impact on information disclosure behavior (Acquisti 2004; Acquisti and Grossklags 2005a), as this phenomenon is typically considered to be a cause for the multiple selves problem (Bazerman et al. 1998). Given that research has found the *should self* to be more influential in advance of a decision, while the *want self* often prevails during the actual decision (O'Connor et al. 2002), this second contribution has implications for the question, which behavioral intention better predicts actual behavior. It is reasonable to assume, that the behavioral intention to use a privacy-invasive IS is a better predictor for actual behavior than the intention to disclose personal information in most contexts. This theoretical implication can also inform future research on the privacy paradox, a phenomenon describing a divergence between behavioral intentions and actual behavior oftentimes found in the privacy context (Norberg et al. 2007). One might assume, that the privacy paradox is more prominent when comparing actual behavior with a disclosure intention compared to a usage intention. However, an evaluation of predictive power of the two intentions for actual behavior was not the scope of this research project and thus these are only reasonable assumptions that should be investigated in future research.

The conceptualization of the benefits provided by a privacy-invasive IS as two-dimensional – this is in line with research on consumer attitudes (Batra and Ahtola 1991; Voss et al. 2003) and hedonic consumption (Hirschman and Holbrook 1982) – constitutes the third contribution. Based on this re-conceptualization, we were able to show, that these dimensions have different impacts depending on the behavioral intention under consideration. This result could inform, for example, the traditional privacy calculus (Laufer and Wolfe 1977) – with the intention to disclose personal information as dependent variable, more attention should be paid to the utilitarian qualities of the privacy-invasive IS under consideration, as the hedonic qualities might be considered less by potential users.

Apart from these theoretical contributions our results are also valuable for practitioners developing or offering privacy-invasive IS. With the knowledge that potential users weight risks and benefits differently depending on the prevalence of the *want* vs. *should self* during the evaluation of an IS, manufacturers can try to create conditions, that make people lean towards the one or the other. For example research has shown, that the shorter the time between purchasing a product and its delivery, the stronger people tend to follow their *want* preferences in the purchase decision (Milkman et al. 2010; Oster and Scott Morton 2005). Another way to bolster the *want self* is presenting products separately instead of jointly with other alternatives. This avoids direct comparisons between alternatives and thus makes *should*

/ *should-not* options less obvious (Bazerman et al. 1999). Consumers on the other side should pay close attention to the context in which they evaluate a privacy-invasive IS. Relying too strongly on their *want self* and neglecting the doubts of the *should self* might result in an underestimation of risks and thus an underestimation of possible negative long term consequences.

3.6 Limitations and Future Research

The results of our study should be interpreted in consideration of its limitations. First of all, intentions in real-life situations might deviate from those observed in a hypothetical scenario. Although the use of vignette-based surveys and hypothetical scenarios is common in privacy research (Hann et al. 2007; Malhotra et al. 2004; Pan and Zinkhan 2006) and this approach was chosen to create a controlled research setting and thereby guarantee a high internal validity, this high internal validity is on the other hand attended by a lower external validity (Taylor 2006). The wearable technology we chose as context for our study to control for cases in which disclosure of data is to some extent optional limits our sample to people who exercise regularly. Furthermore, the study was conducted in Germany and the majority of participants were between 17 and 24 years of age. We deliberately chose this age group, because market researchers have identified 16 to 24 year olds to find wearable technology the most appealing (GfK 2013), making them a suited target group for a first investigation of the multiple selves problem in the context of wearable devices. However, the generalizability of our findings is limited by these sample characteristics. Future studies should therefore try to replicate our results with more diverse and larger samples.

The divergence we found between usage and disclosure intentions calls for more research on privacy-related factors fostering either a *should*- or a *want*-perspective on the act of information disclosure. With the multiple selves problem in mind, the frequently investigated contextual factors like information sensitivity (Malhotra et al. 2004; Xu et al. 2008) or technological applications (Smith et al. 2011) should be investigated with regard to their impact on people's feelings concerning the need to justify their decisions and thus how strong they feel they *should* behave in a certain manner. Also societal norms and values might have an influence on this consideration resulting in larger or smaller divergences between usage and disclosure intentions. Apart from divergences between the two intentions themselves, future research might also investigate, how the two intentions relate to actual behavior, as both conceptualizations, albeit being different, are often used as tantamount predictors for the same behavior in current privacy research. The results obtained by our study might also serve

as a foundation to refine the privacy calculus by considering the multidimensionality of benefits, the distinction between usage and disclosure intentions as well as the role of the multiple selves in the determination of these intentions.

4 Paper B: The Moderating Role of the Regulatory Focus in the Privacy Calculus

Title

Calculating with Different Goals in Mind – the Moderating Role of the Regulatory Focus in the Privacy Calculus

Authors

Brakemeier, Hendrik, Technische Universität Darmstadt, Germany

Widjaja, Thomas, Universität Passau, Germany

Buxmann, Peter, Technische Universität Darmstadt, Germany

Publication Outlet

Proceedings of the 24th European Conference on Information Systems (ECIS 2016), June 12-15, 2016, Istanbul, Turkey

Abstract

Online social networks gather, store, process, and monetize personal information of their users. It is therefore important to understand in which situations people are willing to disclose private information. The most commonly applied theoretical framework to this class of problems in IS research is the privacy calculus. However, empirical research on the privacy calculus found strongly varying effect sizes of benefits and risks of information disclosure on the intention to disclose personal information. In this research, we propose a theoretical explanation for this phenomenon. Based on regulatory focus theory and an experimental study with 59 participants, we develop theoretical arguments, that (1) the perception of high privacy risks evokes a state of heightened vigilance (prevention-focus) and (2) this heightened vigilance in turn changes the weightings of the benefits and risks in the privacy calculus. Results from a second survey-based study with 208 participants provide first insights that perceptions of high risks of information disclosure are correlated with a prevention focus, which in turn increases the negative effect of perceived risks and reduces the positive effect of perceived benefits on an individual's intention to disclose personal information.

Keywords

Privacy Calculus, Information Disclosure, Regulatory Focus, Prevention-Focus, Promotion-Focus.

4.1 Introduction

Online social networks (Kane et al. 2014) are a prominent example for a class of information systems that gather, store and process personal information of their users (Gerlach et al. 2015; Krasnova et al. 2012) but also other social media systems are regularly inherently dependent on the disclosure of certain private information by their users. Therefore, users have to accept, that data about them is collected and processed by these systems if they want to use the respective information system. This poses challenges to the providers of such services, because they do not only have to serve customer needs in terms of functionality, but also have to consider privacy concerns of their users.

It is therefore important to understand in which situations people accept intrusions of their privacy and when they don't. A widely used approach to this question is privacy calculus theory, which posits, that, when faced with the decision between giving up and maintaining their privacy, individuals undertake trade-offs, whether a certain loss of privacy is acceptable for the benefits gained in exchange (Laufer and Wolfe 1977; Li 2012). Various studies have therefore investigated, how the *perceived risks of information disclosure* as well as the *perceived benefits of information disclosure* influence the *behavioral intention* to do so (e.g., Kehr et al. 2013; Keith et al. 2013; Keith et al. 2012; Li et al. 2014; Li et al. 2010; Xu et al. 2009). However, the findings are to some extent inconsistent. While the negative effect of the perceived risks and the positive impact of the perceived benefits on the intention to disclose personal information are uncontroversial, studies find very different effect sizes for these two relationships. For example Xu et al. (2009), Li et al. (2014) and Shibchurn and Yan (2015) found benefits to have stronger effects than privacy risk in studies about location-based websites and a personal health record system. On the other hand for example Keith et al. (2013) and Kehr et al. (2015) report the perceived risks as the more influential antecedent. Accordingly it seems, that an individual's sensitivity to benefits and risks differs across studies and contexts. However, a consistent theoretical explanation for this phenomenon is currently missing. This is for example problematic for providers that aim to maximize the adoption of information systems that rely on the collection of user data, because it remains unclear in which situations privacy risks are really hindering the dissemination and when they merely play a subordinate role.

A possible theoretical explanation of the above described inconsistent findings in prior research is regulatory focus theory (Higgins 1997). This theory proposes, that people can take different mental states, called *promotion-* and *prevention-focus*. Promotion focused

individuals are in a state of eagerness, which can lead to a "risky bias" (Higgins 1998, p. 30). A prevention focus in contrast is associated with heightened vigilance (Higgins et al. 1997). This mental state determines people's sensitivity to negative and positive decision outcomes (Higgins 1998) and is dependent on situational cues, one of which seems to be the risk people are exposed to (Herzenstein et al. 2007; Lee and Aaker 2004) and may therefore change across disclosure contexts. We therefore integrate the regulatory focus in the privacy calculus theory in order to dissolve the controversy described above and investigate the following research questions:

RQ 1: Does the regulatory focus determine the weighting of perceived benefits and risks in the decision whether to disclose personal information?

RQ 2: Is the regulatory focus dependent on the degree of perceived privacy risks in a disclosure situation and does it therefore systematically vary between different disclosure situations?

We contribute to the elucidation of these questions by extending the privacy calculus theory (Laufer and Wolfe 1977), by a regulatory focus perspective. Based on the integration of these theories and an experimental study we develop theoretical arguments, that when people merely perceive a low level of privacy risks, they take a state of incautiousness (named *promotion-focus*) and base their decisions on the expected benefits of their behavior whereas the perceived risks play a minor role. Only if a certain level of perceived privacy risk is exceeded, people take a state of heightened vigilance (named *prevention-focus*), which makes them especially sensitive to perceived risks and reduces the influence of perceived benefits. Thus, effect sizes of the perceived risk of information disclosure should be larger in studies investigating relatively invasive information systems, which are associated with high-perceived risks, compared to less invasive ones. The opposite should hold for the effects sizes of the perceived benefits of information disclosure. We provide empirical evidence for these propositions based on a survey among 208 participants and thereby show, that perceptions of high risks of information disclosure evoke a prevention focus, which increases the effect of perceived risks and reduces the effect of perceived benefits in the privacy calculus.

The remainder of this paper is structured as follows: We first outline the theoretical background for our research in two steps: First, we delineate the privacy calculus and depict potential improvements to the theory. Based on literature on regulatory focus theory and a first experimental study, we then develop arguments, that the level of the perceived privacy risks determines the weighting of benefits and risks in the privacy calculus. Afterwards we

describe the second survey-based study we conducted to empirically test our deduced hypotheses and present our findings. We then discuss our findings before the paper closes with a depiction of limitations of our study and propositions for future research efforts.

4.2 Theoretical Background

4.2.1 The Role of Benefits and Risks in the Privacy Calculus

A considerable amount of literature in the field of IS privacy research is dedicated to the question, under which circumstances people are willing to have their personal information gathered and processed by privacy invasive information systems. In this context, privacy "[…] refers to the claims of individuals that data about themselves should generally not be available to other individuals and organizations […]" (Clarke 1999, p. 60). However, keeping data private from other individuals and organizations is not always feasible when using modern information systems like online social networks (Gross and Acquisti 2005). This forces people to either protect their privacy and forego the benefits of using the information system or giving up their privacy and taking advantage of the benefits provided by the information system (e.g., relationship building, Krasnova et al. 2010). This trade-off between benefits and risks of information disclosure is reflected in the privacy calculus theory (Laufer and Wolfe 1977; Li 2012). The central constructs of privacy calculus theory are the *perceived risks of information disclosure* and the *perceived benefits of information disclosure*. These are weighted against each other and form a *behavioral intention to disclose personal information* (Li 2012; Smith et al. 2011). Thus, during the decision whether to disclose personal information or not, people basically evaluate a utility function like the following (e.g., Awad and Krishnan 2006):

$$Utility = Benefit - Cost$$

This formula illustrates, that the underlying assumption of privacy calculus theory is, that "… consumers perform the risk–benefit analysis in the privacy calculus and decide whether to disclose information based on the net outcomes" (Li 2012, p. 475). This net outcome utility is positive (a *net gain*) if the benefits outweigh the risks and negative (a *net loss*) if the risk outweighs the benefits. The resulting behavior is then depending on whether the net utility of disclosing personal information is positive or negative, that is to say, a net gain or a net loss. If the act of disclosure promises a net gain, privacy is given up to realize the utility, while maintaining one's privacy is the alternative of choice when the net utility of disclosing would be negative and thus a net loss.

However, this view of balancing out benefits and risk is problematic, because it implies, that risk-minimization and benefit-maximization are equivalent types of goals for consumers, both increasing net outcome utility. However, while some empirical findings based on the privacy calculus theory have found the effects of the perceived benefits of information disclosure to be stronger than those of the perceived risks (e.g., Li et al. 2014; Xu et al. 2009), others report that the perceived risks are the stronger determinant (e.g., Kehr et al. 2015; Keith et al. 2013) of the disclosure intention and therefore the assumed outcome utility. Some studies even find that risks sometimes have no impact on the disclosure intention and therefore do not to contribute to the net outcome utility of disclosing information at all (e.g., Krasnova et al. 2012). It therefore seems, that risks and benefits exhibit more complex relationships to the assumed net outcome utility than the simple trade-off reflected by the privacy calculus.

A theory "reach[ing] beyond the classic conception of outcome utility" (Florack et al. 2013, p. 128) is regulatory focus theory proposed by Higgins (1997). Research from this area has found that people do not simply act according to one goal of maximizing their net utility and do not simply decide based on whether the consequence is a net loss (net utility < 0) or a net gain (net utility > 0). Regulatory focus theory rather "suggests the need to consider a fuller picture regarding gains and losses; specifically, to examine people's reactions not only to gains (the presence of a positive outcome) and losses (the presence of a negative outcome) but also to nongains (the absence of a positive outcome) and nonlosses (the absence of a negative outcome)" (Idson et al. 2000, p. 253). In this regard, the theory distinguishes *promotion*- and *prevention goals*. While promotion goals are concerned with maximizing the presence of positive outcomes (gains) and minimizing their absence (nongains), prevention goals are concerned with maximizing the absence of negative outcomes (nonlosses) and minimizing their presence (losses) (Chernev 2004).

The privacy calculus is inherently characterized by incorporating these two types of goals in a conflicting manner. As depicted above, the two exogenous constructs in the privacy calculus are the *perceived benefits of information disclosure* and the *perceived risks of information disclosure*. Each of these two attributes of a disclosure decision can be mapped to one of the two types of goals introduced by the regulatory focus theory, because "a trade-off between attributes is essentially a trade-off between the goals that these attributes help attain" (Chitturi et al. 2007, p. 703). In the context of online social networks the benefits typically comprise relationship building, self presentation and enjoyment (Krasnova et al. 2010) and in a broader sense this dimension could also include monetary incentives, personalized service (Li 2012),

time savings or social adjustment (Tam et al. 2002). The presence or absence of such benefits determines, in how far the disclosure of personal information is associated with a gain or a nongain. Therefore, the perceived benefits of information disclosure help attain promotion goals. The perceived risk of information disclosure on the other hand determines in how far prevention goals are met. Again, prevention goals are concerned with the presence or absence of losses. The perceived risk of information disclosure is defined as "the expectation of losses associated with the disclosure of personal information" (Heng et al. 2011, p. 804). Thus, when no risks are perceived, there is no expectation of losses associated with disclosing personal information and prevention goals are perfectly met. When, however, there is risk involved, an individual expects a potential loss due to the disclosure of its information and prevention goals might be compromised.

4.2.2 Regulatory Focus as a Moderator in the Privacy Calculus

4.2.2.1 Moving Beyond Net Utility

In the previous section, we outlined that in the privacy calculus the perceived benefits of information disclosure help attain promotion goals, while the perceived risks of information disclosure determine in how far prevention goals are met. The question resulting from this distinction is in how far the degrees of achievement of prevention- and promotion goals influence an individual's decision. Regulatory Focus Theory postulates, that the weighting of each of these goals is determined by what is termed a person's *regulatory orientation* (Higgins 2000). In accordance with the distinction between prevention and promotion goals, a person's regulatory orientation can differ between a *prevention*- and a *promotion focus* (Higgins 1998). Promotion focused individuals are in a state of eagerness and concerned with the presence and absence of positive outcomes or gains (Higgins et al. 1997). This state of eagerness induces "advancement tactics ,[and] an inclination to approach accomplishments" (Higgins 1998, p. 30), which can lead to a "risky bias" (Higgins 1998, p. 30). A prevention focus in contrast is concerned with the absence and presence of negative outcomes (Higgins et al. 1997). It is associated with a state of vigilance (Higgins 1998), which induces precautionary tactics (Higgins 1998) and the desire to behave "in a safe and secure manner" (Chitturi et al. 2008, p. 50). These two regulatory orientations determine in how far people are sensitive for promotion and prevention goals. While prevention focused individuals act in favor of their prevention goals and thus try to minimize losses, promotion focused individuals try to fulfill promotion goals by maximizing gains (Chitturi et al. 2008). As risk minimization

represents a prevention goal and benefit maximization a promotion goal, promotion focused individuals should therefore be more sensitive to the benefits in the privacy calculus, while prevention-focused individuals are more sensitive to the perceived risks.

However, the term "sensitive to", which is usually used in reasoning based on regulatory focus (e.g., Florack et al. 2009; Yoon et al. 2012; Zhou and Tuan Pham 2004) can be interpreted in two ways. These are visualized in Figure 3. First, a prevention-focused individual could perceive the same situation as riskier and the benefits as lower compared to a promotion focused individual. In this case, the regulatory focus would moderate the effect of an objective risk or benefit, which is the risk or benefit one would reasonably assume given all relevant information and the capacity to process all this information, on the perceived risk or benefit, which is the subjective evaluation of a risk or benefit resulting from inferences based on heuristics, assumptions and personal beliefs (alternative A in Figure 3). A second possibility is that prevention and promotion-focused persons perceive equal degrees of risks and benefits, but those in a prevention focus are more sensitive to the risks and less sensitive to the benefits in their decision-making process. In this case, the regulatory focus would moderate the effect of the perceived risk and benefit on a person's behavioral intention (alternative B in Figure 3) and might therefore explain the different effect sizes found in research based on the privacy calculus. To rule out possibility A, we conducted an experimental study, which is presented in the following section.

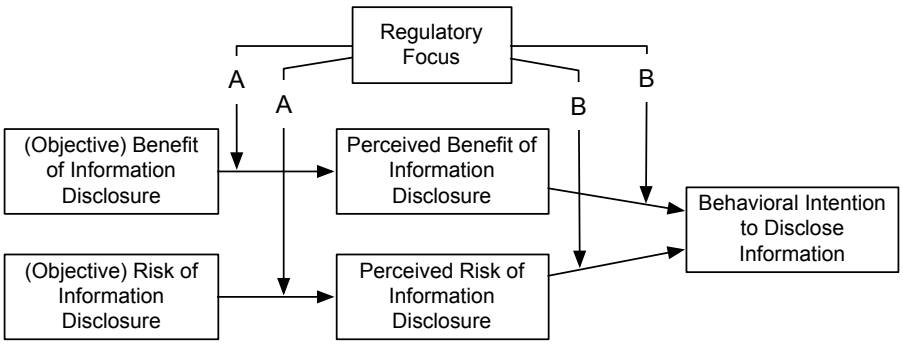

Figure 3: Two possible moderating roles of the regulatory focus.

4.2.2.2 Experimental Study: Perceptions of Benefits and Risks under Prevention and Promotion

The goal of this experiment was to test, whether perceptions of benefits and risks differ between prevention- and promotion-focused individuals (alternative A in Figure 3). Fifty-nine students of a German university took part in the experiment, which was carried out online via a browser. Participants were from different courses and requested to participate via E-Mail.

The majority (73%) were male and the age ranged from 19 to 29 with the median being 21. All participants were randomly assigned to one of two groups, which underwent a manipulation of regulatory focus evoking either a prevention- (29 participants) or a promotion-focus (30 participants). To manipulate the regulatory focus, we used an established approach that has successfully been applied in prior studies (e.g., Pham and Avnet 2004; Trudel et al. 2012). Participants in the primed-prevention-focus condition were asked to think about their past duties, obligations and responsibilities for two minutes and then list two of them. They were then asked to think about their current duties, obligations and responsibilities for two minutes and again list two of them. Participants in the primed-promotion-focus condition underwent the same procedure, but were asked to think of and write down their past and current hopes, aspirations and dreams instead of duties, obligations and responsibilities.

Both groups then read the description of a privacy-invasive fitness wristband and answered a questionnaire comprising established measures for the perceived risks of information disclosure (Heng et al. 2011, see Appendix) and the perceived benefits of information disclosure. The benefits were measured by the participant's utilitarian and hedonic attitudes towards the wristband (Voss et al. 2003). This measure asked the participants to rate the product (1-7) on bipolar scales for the utilitarian (effective/ineffective, helpful/unhelpful, functional/not functional, necessary/unnecessary and practical/impractical) and hedonic attitudes (not fun/fun, dull/exciting, not delightful/delightful, not thrilling/thrilling, enjoyable/unenjoyable) (Voss et al. 2003). We also included a measure for the situation specific regulatory focus proposed by Pham and Avnet (2004) as manipulation check. This measure consists of three differentials on which participants had to indicate in how far they lean towards either prevention-oriented or promotion-oriented behaviors and can be found in Appendix 3.

A multivariate analysis of variance (MANOVA) was used to analyze the data. The results indicate a successful manipulation of the regulatory focus (m_{prev} = 2.425, m_{prom} = 3.200, F = 5.682, p = 0.020). However, no significant difference could be observed for the perceived risk of information disclosure (m_{prev} = 5.319, m_{prom} = 5.200, F = 0.092, p = 0.736) and either of the dimensions of benefits (m_{prev} = 4.503, m_{prom} = 4.307, F = 0.355, p = 0.554 [hedonic]/ m_{prev} = 4.731, m_{prom} = 4.387, F = 1.116, p = 0.285 [utilitarian]). These results are in conflict with a moderation of the effect of an objective risk or benefit on the perceived risk or benefit (alternative A in Figure 3). We therefore opted for alternative B, when integrating the

regulatory focus into the privacy calculus theory: The regulatory focus moderates the effect of the perceived risk and benefits respectively on a person's behavioral intentions. The privacy calculus (H1 & H2) and the moderating effect of the regulatory focus (H3 & H4) are reflected by the following four hypotheses, which are also depicted in Figure 4.

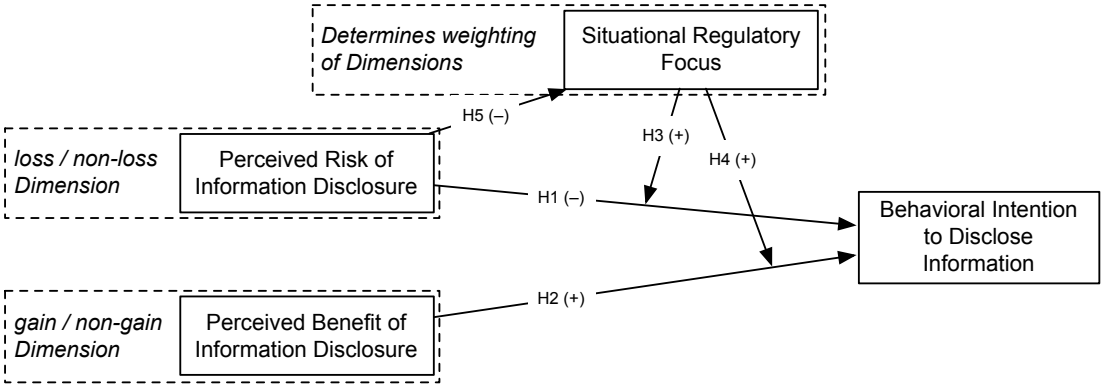

Figure 4: Research Model (Paper B).

H1: The perceived risk of information disclosure has a negative impact on the behavioral intention to disclose personal information.

H2: The perceived benefits of information disclosure have a positive impact on the behavioral intention to disclose personal information.

H3: The negative impact of the perceived risk of information disclosure on the behavioral intention to disclose personal information is stronger for prevention-focused compared to promotion-focused individuals.

H4: The positive impact of the perceived benefits of information disclosure on the behavioral intention to disclose personal information is stronger for promotion-focused compared to prevention-focused individuals.

4.2.3 Sources of Regulatory Focus

Now that we hypothesized the moderating effect of the regulatory focus in the privacy calculus (RQ 1) we turn to our second research question, which asked whether the regulatory focus depends on the degree of perceived privacy risks in a disclosure situation. Research on regulatory focus suggests three distinct sources of a person's regulatory focus: The chronic regulatory focus, a contextual priming before a decision task and the decision task itself (Florack et al. 2005). The chronic regulatory focus can be understood as a general baseline of regulatory focus or a general tendency of a person to be more or less prevention- or promotion focused (Higgins 1997; Higgins 1998), determined for example during childhood

socialization (Higgins and Silberman 1998). The second source of regulatory focus, contextual priming, is widely used in research to put people in a state of either prevention or promotion focus and then investigate subsequent behavior (e.g., Chernev 2004; Idson et al. 2000; Lee and Aaker 2004; Wang and Lee 2006). The most popular procedure in this context is asking people to think about either their duties and obligations (prevention) or their hopes and aspirations (promotion) and then write about them or list some of them (Higgins et al. 1994; Liberman et al. 2001; Pham and Avnet 2009; Sacchi and Stanca 2014; Wang and Lee 2006; Yoon et al. 2012) as we have done in our experimental study. Lastly, the regulatory focus can be influenced by a decision task itself (Lee and Aaker 2004; Zhou and Tuan Pham 2004). The regulatory focus induced by contextual priming or a decision task is usually referred to as *situational* or *situation specific regulatory focus*. Please note that, although being named differently, the chronic and the situation specific regulatory focus both refer to the same concept. The priming procedures described above simply let people deviate from their chronic regulatory focus towards being either more prevention or promotion focused than they chronically are for a certain period of time. Thus, the situation specific regulatory focus incorporates the chronic regulatory focus altered by the priming. If a decision context includes such a priming, it is therefore the situation specific regulatory focus that influences the decision.

Both, contextual priming and priming by a decision task itself are based on the general proposition of Higgins (1997), that people take a prevention focus when they see themselves in situations involving potential losses and a promotion focus when a situation makes potential gains salient (Seibt and Förster 2004). More specifically and in line with Lee and Aaker (2004, p. 206) we argue, that individuals are more likely to focus on negative outcomes when perceived risk is high and on positive outcomes when perceived risk is low [...]. Specifically, when individuals feel vulnerable, heightened vigilance associated with prevention focus should result" (Lee and Aaker 2004, p. 206). Although not directly testing the relationship between regulatory focus and perceived risks and a different context, findings from Lee and Aaker (2004) substantiate this assumption. In two experiments a manipulation of the perceived risks of getting a sunburn (1st experiment) and mononucleosis (2nd experiment) had the same effect, as one would have expected for a manipulation of the regulatory focus. Another study by Herzenstein et al. (2007) found that making risks explicit (vs. implicit) can rule out the effect of a primed promotion-focus. This could also be explained by high risks evoking a prevention focus and thereby nullifying the promotion-

priming. We therefore argue that an individuals' situational regulatory focus is endogenously dependent on the perceived risks of information disclosure.

H5: A high (low) perceived risk of information disclosure is associated with a more prevention-oriented (promotion-oriented) situation specific regulatory focus.

All hypothesized relationships are detailed in Figure 4.

4.3 Main Study

To empirically test the hypothesized relationships, we conducted an online survey study in which participants had the chance to win an Amazon Gift Card worth 50€ when they granted us access to certain information from their Facebook profile via a Facebook Web App we implemented for this study. By choosing a Facebook Web App as context for our study, we follow the call by Smith et al. (2011) to move away from hypothetical scenarios (e.g., Gerlach et al. 2015; Hann et al. 2007; Malhotra et al. 2004; Pan and Zinkhan 2006) to more realistic settings incorporating actual data disclosure in IS privacy research. Albeit we are able to monitor actual behavior with this App we use the behavioral intention to disclose information as dependent variable, because the intention is the direct outcome of the privacy calculus according to privacy calculus theory (Li 2012). However, we assume that the realistic context of our study enables us to obtain very reliable measurements for the participant's behavioral intentions. Furthermore, disclosure of Facebook profiles was chosen because we expected a high variance in the amount of information different people store on their Facebook profile and thus a high variance in the perceived risk of disclosing this information. This variance was required because we wanted our sample to contain individuals for whom the perceived risk is too low to evoke a prevention focus as well as those perceiving a high risk and thus becoming prevention focused.

Before being confronted with our Facebook Web App, the participants were told that we would only analyze the data in anonymized form and assured that there were no right or wrong answers and they can therefore answer all questions honestly. This was done to counteract common method biases (Podsakoff et al. 2003). As described before, regulatory focus theory distinguishes a chronic as well as a situation specific regulatory focus (Florack et al. 2005; Higgins et al. 1994). The relevant moderator in our study is the situation specific regulatory focus, because, as depicted in section 2.3, the situation specific regulatory focus incorporates the chronic regulatory focus altered by a potential priming by contextual factors. We assume the perceived risk of information disclosure to be such a factor (H5) and are

therefore interested in the situation specific regulatory focus evoked during the decision task. However, we also measured the chronic tendency to be prevention focused as a control variable for the situation specific regulatory focus with the composite regulatory focus scale by Haws et al. (2010). The perceived benefits of information disclosure were operationalized by the perceived value of the chance to win a 50€ gift card as described above. This perceived value was measured by means of a scale from Okada (2005).

After filling out these measures, participants were presented a text, which read that we were conducting a study investigating what information are publicly posted on Facebook in different countries. We made explicit that we were only interested in information that are publicly available, which means that every Facebook user can access this information. This information comprises the name, age group and gender of the user and further information like posts and the list of Facebook friends if they are explicitly marked as public by the user (Facebook 2015). We then told participants that we developed a Facebook Application to automatically read this information from their profile in order to avoid collecting the data manually. In exchange for their participation, that is granting our app the permission to access their public profile, they were offered the chance to win the 50€ Amazon gift card mentioned above. We also mentioned that the App would gather the user's e-mail addresses to contact them in case they won the gift card.

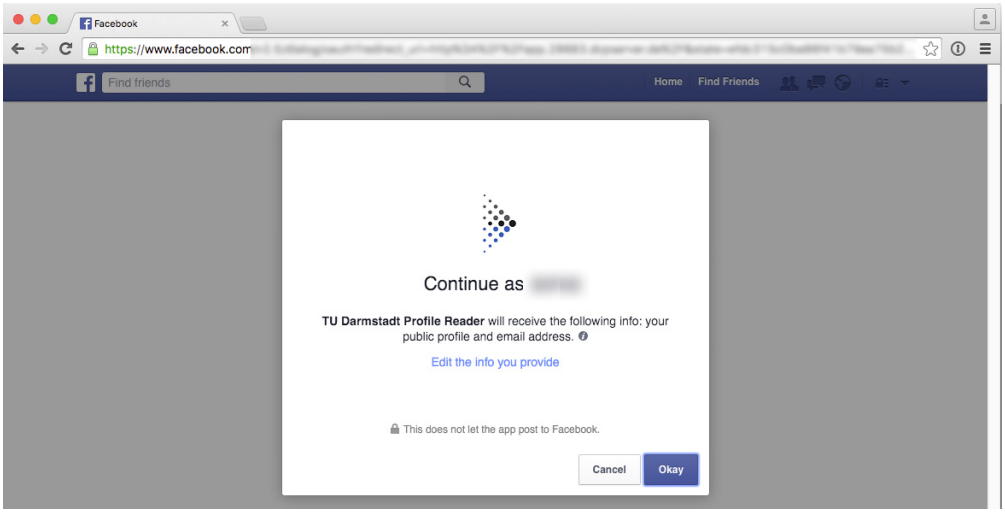

Figure 5: Screenshot of the Facebook Permission Dialog.

We then showed participants the steps they had to go through when taking part in our study by a series of screenshots. Participants had to click either a button reading "Allow Profile Access via Facebook" or a button reading "Deny profile access". When they chose to grant us access to their public profile they were forwarded to Facebook, which in turn presented the confirmation window depicted in Figure 5. Before actually forwarding them to our Facebook

Web App participants then had to state, in how far they would be willing to disclose their information via the Facebook Web App with the established scale from Malhotra et al. (2004). This was also the moment in which we measured the participants' situation specific regulatory focus with the three seven point semantic differentials (Pham and Avnet 2004) that were also used in our first experimental study. Afterwards, participants were forwarded to the Facebook Web App and either granted us access to their profile or not. Lastly, we measured the individuals' perceived privacy risks with the established scale from Heng et al. (2011). All measurement items in our research model can be found in Appendix 3.

Participants were recruited via Workhub, a crowdsourcing platform on which people are receiving money in exchange for performing short tasks via a browser. This channel was chosen because the users of Workhub are only paid by the platform if they enter a "validation code" after finishing a job, which was displayed on the last page of our survey. Thus, we prevented bias due to drop-out of participants that were not willing to disclose their information and thus had no chance to win the gift card.

4.4 Results

In total 208 Facebook users from Germany completed the survey of which 87 (41.8%) were female. The age ranged from 16 to 58 with the mean being 28.7. The major groups regarding the work background were salaried employees (43.3%) and students (34.6%). Another 9.1% were self-employed. We used structural equation modeling to analyze our data. This approach allows us to test the construct relationships as well as the psychometric properties of the measurement model simultaneously (Bagozzi and Youjae 1989; Gefen et al. 2000) and thus provides a comprehensive analysis of all relationships in our research model (Fornell and Bookstein 1982). The variance-based partial least squares method as implemented in SmartPLS (Ringle et al. 2015) was chosen over the covariance-based LISREL because it is particularly suited for testing theories in early stages (Fornell and Bookstein 1982).

4.4.1 Measurement Validation

Construct	Cr. α	CR	AVE	INT	RF	RSK	BEN
Intention to Disclose Personal Information (INT)	.958	.969	.888	**.942**			
Regulatory Focus (RF)	.836	.900	.749	.414	**.866**		
Perceived Risk of Information Disclosure (RSK)	.862	.901	.698	-.473	-.313	**.836**	
Perceived Benefit of Information Disclosure (BEN)	.786	.876	.702	.462	.225	-.103	**.838**

Table 6: Cronbach's α (Cr. α), Composite Reliability (CR), Average Variance Extracted (AVE) and Construct Correlations (Paper B).

We first evaluated the validity of the measurement model by investigating the convergent and discriminant validity of our survey instrument. Convergent validity is assessed by means of the loadings of items on their constructs, composite reliability (CR) of the constructs and the average variance extracted (AVE) by the constructs (Xu et al. 2012). Sufficient item reliability is achieved when all items have loadings higher than 0.65 on their construct (Falk and Miller 1992). This is the case, as can be seen in Table 7 (printed in bold type). Composite Reliability should exceed 0.7 (Bagozzi and Yi 2012) and the average variance extracted exceeds the value of 0.5 proposed by Hair et al. (2011). Cronbach's α is also larger than the proposed criterion of 0.7 (Bagozzi and Yi 2012) for all constructs, thus convergent validity is given (see Table 6).

	Item	INT	RF	RSK	VAL
Intention to Disclose Personal Information (INT)	INT1	**0.952**	0.387	-0.431	0.477
	INT2	**0.958**	0.373	-0.460	0.422
	INT3	**0.936**	0.366	-0.502	0.431
	INT4	**0.922**	0.435	-0.385	0.408
Regulatory Focus (RF)	RF1	0.280	**0.837**	-0.197	0.192
	RF2	0.360	**0.856**	-0.258	0.203
	RF3	0.409	**0.902**	-0.332	0.192
Perceived Risk of Information Disclosure (RSK)	RSK1	-0.485	-0.279	**0.900**	-0.153
	RSK2	-0.474	-0.368	**0.914**	-0.113
	RSK3	-0.303	-0.202	**0.821**	-0.016
	RSK4	-0.202	-0.090	**0.688**	0.021
Perc. Benefit of Information Disc. (BEN)	BEN1	0.352	0.172	-0.045	**0.779**
	BEN2	0.404	0.208	-0.088	**0.854**
	BEN3	0.401	0.185	-0.121	**0.877**

Table 7: Factor Analysis - Item Loadings and Cross-Loadings (Paper B).

scriminant validity is given when (1) all items load higher on their intended construct than on any other construct (Bagozzi and Yi 2012) and (2) the variance shared between each construct and its items is greater than the correlations between the construct and all other constructs

(Fornell and Larcker 1981). As can be seen in Table 7 all items load higher on their intended constructs than on any other constructs with the highest cross-loading being 0.477. The second criterion is met, when the square root of the AVE, the variance shared between a construct and its associated items, (diagonal elements in Table 6) is greater than the correlation between the construct and any other construct (non-diagonal elements in Table 6) in the model (Fornell and Larcker 1981). This criterion is also fulfilled, thus discriminant validity is also met.

Lastly, we performed Harman's single factor test (Podsakoff et al. 2003) to investigate whether a single factor can explain the majority of covariance among our measures, which would be an indication of potentially problematic common method variance. The most covariance explained by one factor turned out to be 30.17% and thus the test does not indicate problematic common method biases.

4.4.2 Analysis of the Structural Model

After ensuring our measurement model was valid we proceeded by analyzing the hypothesized relationships between the constructs as reflected by our research model (see Figure 6). The overall model fit is good with a standardized root mean square residual (SRMR) of 0.059 and therewith below the threshold of 0.8 (Hu and Bentler 1999). Predictive validity is assessed by the amount of variance explained in the dependent variables (R^2) and the cross-validated redundancy Q^2 (Geisser 1975; Stone 1974). Our model explains 13.9% of the variance in the situation specific regulatory focus and 50.8% of the variance in the intention to disclose information.[1] Q^2 is 0.089 for the situation specific regulatory focus and 0.444 for the intention to disclose personal information and therefore indicates predictive relevance ($Q^2 > 0$) (Chin 2010). The relative impact of each path in the model on the Q^2 values in terms of q^2 can be found in Appendix 4.

To investigate the significance of the path coefficients in our model a bootstrapping with 5000 resamples was performed. All path coefficients are significant at least at the 1% level ($p < 0.01$) and the directions of the effects are in line with our hypotheses. Therefore, all our hypotheses are supported. However, when modeling moderations in structural equation models, a direct effect between the moderator (the situation specific regulatory focus in our case) and the dependent variable (the intention to disclose personal information) is included

[1] A Nagelkerke-R^2 of 0.392 was obtained for a binary logistic regression with the disclosure intention as the only predictor for actual disclosure behavior, indicating that a considerable amount of variance in actual behavior is explained by the behavioral intention we measured.

(Chin et al. 2003). This relationship turned out to be significant and positive (β = 0.184**, p = 0.003) although we did not hypothesize a direct effect between the regulatory focus and the disclosure intention. According to Sharma et al. (1981) the situation specific regulatory focus is therefore not a "pure-" but a "quasi moderator" (Sharma et al. 1981, p. 292). Indicators of effect size f^2 (Cohen 1988) are given in Appendix 4 for each path in the model.

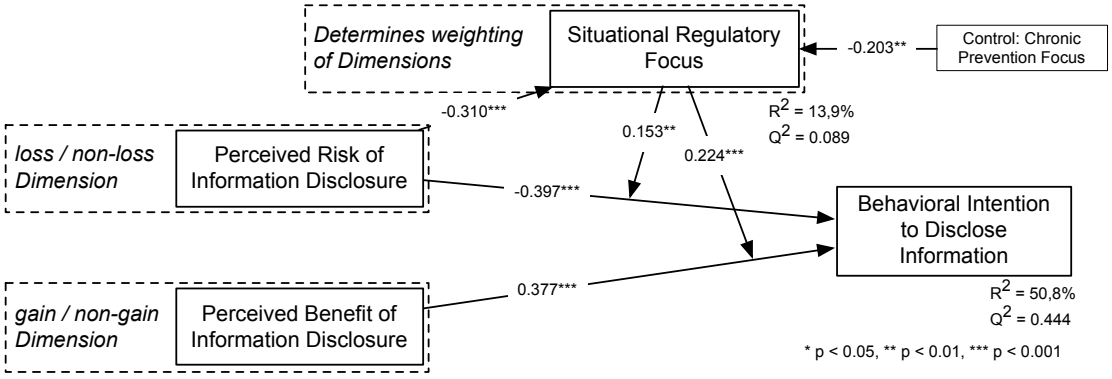

Figure 6: Results of the PLS estimation of the structural model (Paper B).

Slope analyses showing the influence of the perceived privacy risk and benefit on the disclosure intention for the mean regulatory focus as well as a regulatory focus one standard deviation above and below the mean are shown in Figure 7. While the negative impact of the privacy risks is stronger for the prevention focused (RF at -1 SD) participants the effect diminishes when people are less prevention focused (RF at +1 SD). The opposite holds for the effect of the perceived value of the chance to win the gift card. This effect hardly exists for prevention-focused individuals (RF a -1 SD), but gets more pronounced when people are less prevention focused (RF at +1 SD).

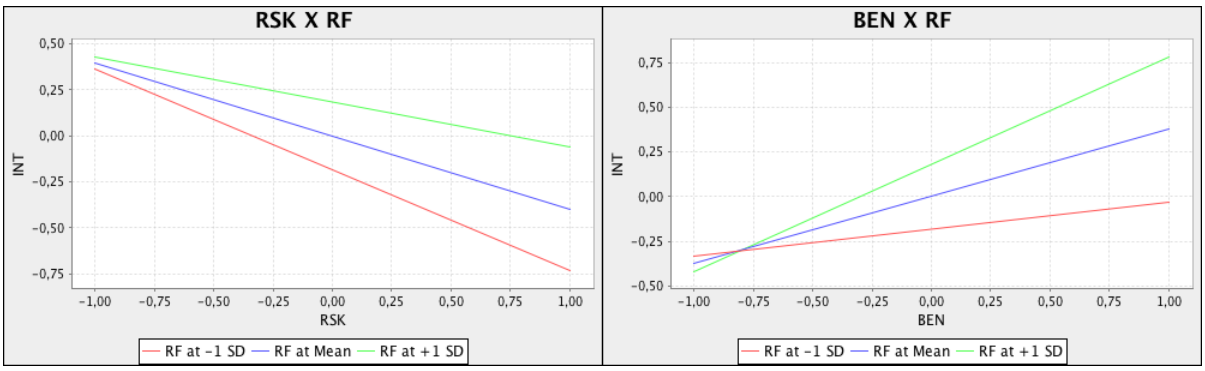

Figure 7: Slope analyses for the interaction between the regulatory focus (RF) and the perceived risk (RSK, left) as well as the perceived benefit of information disclosure (BEN, right).

4.5 Discussion

In this research we investigated the role of a person's regulatory focus (Higgins 1997) in the privacy calculus theory (Laufer and Wolfe 1977; Li 2012). We empirically found a positive

correlation between the perceived risks of information disclosure and a prevention-focus (RQ 2). This prevention-focus is associated with heightened vigilance (Higgins 1998). This in turn changes the weighting of benefits and risks in the privacy calculus. Therefore, an individual's regulatory focus moderates the effects of the perceived risks and benefits in the privacy calculus (RQ 1). Specifically, the more prevention focused (compared to promotion-focused) a person is, the more sensitive is this person to the perceived risks of information disclosure, while the opposite applies to the perceived benefits of information disclosure.

These findings have several implications for research based on the privacy calculus theory. We see three theoretical contributions that all extend privacy calculus theory: First, we integrated a regulatory focus perspective into the privacy calculus theory and thereby proposed a shift from considering only net outcome utility (Awad and Krishnan 2006) towards viewing risk minimization and benefit maximization as different types of goals serving either prevention or promotion needs (Higgins 1997; Higgins 1998). Therefore, an individual's regulatory focus acts as a moderating variable in the trade-off described by the privacy calculus. Future studies building upon the privacy calculus should consider this variable in their research models. Furthermore, the moderating effect of regulatory focus may also help to consolidate previous research based on the privacy calculus. While in some studies the perceived risks are more influential than the benefits (Kehr et al. 2015; Keith et al. 2013), others find that the disclosure intention is mainly dependent on the benefits (Li et al. 2014; Shibchurn and Yan 2015; Xu et al. 2009). These dissonant findings could be explained by varying regulatory foci.

This leads us to our second theoretical contribution. To our knowledge, this is the first study directly testing a correlation between the perceived risks of information disclosure and a person's regulatory focus. Other studies on regulatory focus theory usually employ experimental research designs and focus on the observation of decision outcomes (e.g., Chernev 2004; Idson et al. 2000; Lee and Aaker 2004; Wang and Lee 2006). However, the relationship between one's regulatory focus and the perceived risk and therefore an antecedent of the final decision has not been tested empirically yet. Our first study provided evidence that prevention- and promotion-focused individuals perceive the same degree of risks from a situation involving the disclosure of personal information. The findings from our second study then provided support for the hypothesis, that people weight the risks differently in the decision-process. This is in line with common reasoning in the domain of regulatory focus (Higgins 1998; Zhou and Tuan Pham 2004).

A third theoretical contribution arises from the non-linearity of the effects of risk and benefit perceptions on the intention to disclose personal information, i.e., the combination of the two contributions above. As we have shown, when perceiving a high risk for their privacy, people tend to adopt a state of heightened vigilance and become less incautious (contribution 2). This state in turn leads to a higher weighting of risks and a lower weighting of benefits in the privacy calculus (contribution 1). Consequently, one would expect the effect of the perceived risks of information disclosure in the privacy calculus to be higher for a more invasive technology compared to a less invasive one. Contrary, the effects of the perceived benefits of information disclosure should be lower the more invasive the technology is. Thus, the perceived risk of information disclosure as well as the corresponding benefits are not linearly related to the behavioral intention to disclose personal information, which has been a fundamental assumption in most research based on the privacy calculus theory (Laufer and Wolfe 1977; Li 2012). Research on relatively invasive information systems should in fact find stronger negative effects for privacy risks while the effects of perceived benefits on the disclosure intention should be lower compared to a relatively privacy-friendly information system.

Apart from these theoretical implications our research also has important implications for practitioners. Providers of privacy-invasive information systems should be aware which kind of regulatory focus their product evokes for customers. Research on regulatory focus, specifically the so-called regulatory fit (Higgins 2000) has shown, that advertising messages framed in accordance with one's regulatory focus are more persuasive than those with conflicting framing (Lee and Aaker 2004). Therefore, customers should find prevention-framed messages more persuasive for relatively invasive information systems while promotion-framed messages are more effective for systems carrying only minor risks.

A second practical implication addresses the shortcoming of the privacy calculus, that specific recommendations for providers could hardly be deduced. From the privacy calculus we know that, in simple terms, benefits are good and privacy risks are bad. The implication for application providers is therefore very general: Decrease the perceived privacy risks evoked by your application as much as possible. However, as privacy risks usually cannot be eliminated completely, because certain data is necessary to provide functionality and/or their reduction usually involves the investment of resources, the ability to make statements about which level of privacy is "good enough" is desirable. When taking the regulatory focus into consideration more specific recommendations can be made: If an information system involves

such high privacy risks that it evokes a prevention focus, the adoption decision is mainly driven by risk perceptions and providers should try to reduce these risks. When the risk however reaches a sufficiently low level, benefits are the more influential antecedent for the customer's disclosure intention and thus indirectly their likelihood of adoption. Lastly, to reduce the negative influence of risk perceptions on the adoption rate, providers could try to market their systems in a fashion that evokes a promotion-focus during the adoption decision (Florack et al. 2005).

4.6 Limitations and Future Research

The findings of this research have to be interpreted in consideration of its limitations. We contacted participants via a crowdsourcing platform to ensure demographic heterogeneity (Steelman et al. 2014) and prevent bias due to drop-out when participants were not willing to disclose their information and thus would have had no incentive to complete the survey. However, our sample still contains a lot of relatively young participants (mean age 28.7). Also the advantage of using a Facebook Web App to create a realistic setting incorporating actual information disclosure is on the other hand attended by a restriction of potential participants on Facebook users. These might possess special characteristics regarding their attitudes towards privacy, because using Facebook already requires a certain degree of information disclosure on the internet and trust towards the platform. Future research could therefore investigate whether the relationships found in our study also hold in different contexts. Finally, cultural aspects might limit the generalizability of our findings. Our study was conducted in Germany. Future research could extend our findings by investigating the role of regulatory focus in different cultural context, as different effect sizes of benefits and risks were found in privacy literature in different countries (Krasnova et al. 2012). These could partly be attributed to differences in regulatory foci and/or the interplay of regulatory focus and cultural dimensions.

Investigating the factors evoking a prevention focus in the privacy context in more detail can also make valuable contributions to IS research. For example Malhotra et al. (2004) distinguish concerns regarding the collection of data, the control about one's data and the awareness of privacy practices. These dimensions of privacy concerns might evoke a prevention focus to different degrees.

5 Paper C: An Evaluability Perspective on Privacy Risks

Title

When Risk Perceptions Are Nothing but Guesses – An Evaluability Perspective on Privacy Risks

Authors

Brakemeier, Hendrik, Technische Universität Darmstadt, Germany

Wagner, Amina, Technische Universität Darmstadt, Germany

Buxmann, Peter, Technische Universität Darmstadt, Germany

Publication Outlet

Proceedings of the 38th International Conference on Information Systems (ICIS 2017), December 10-13, 2017, Seoul, South Korea

Abstract

Traditionally, a majority of IS privacy research assumes that individuals are able to form confident privacy risk perceptions when being confronted with situations involving the disclosure of personal information. We challenge this assumption by offering theoretical arguments that privacy risks are difficult to evaluate for individuals. Based on an experimental survey study among 233 participants we show that (1) the formation of privacy risk perceptions is dependent on external reference information and (2) more external information allow a more confident risk judgment, which in turn has a stronger impact on an individual's privacy-related behavior. These findings extend privacy calculus theory by introducing the context-specific evaluability of privacy risks as a moderator of the effect of perceived privacy risks on usage intentions of privacy-invasive information systems. Theoretical and practical implications are discussed and future research suggestions are provided.

Keywords

Privacy Risks, Privacy Calculus, Evaluability, Confidence

5.1 Introduction

Suppose Jeff is scrolling through his smartphone's app store in search of a new task management app. His eyes wander through a long list of search results until he taps one that looks appropriate for his needs. Although there are not many, the ratings and reviews seem to be okay and the screenshots look promising. Jeffs' finger hovers above the download button, but suddenly a section listing a variety of personal information stored on his phone catches his attention: In order to use the application, it requires Jeff to grant access to his contact list, calendar information and his phone's camera. Jeff pauses asking himself, whether there would be a high potential for loss associated with giving these information to the application provider. What Jeff just experienced is exactly what IS privacy researchers ask survey participants to do when measuring the perceived risks of information disclosure. Consider for instance the items used by Malhotra et al. (2004) to measure the perceived risks of information disclosure: They ask survey participants to indicate the extent to which they agree to statements like "There would be high potential for loss associated with giving (the information) to online firms" (Malhotra et al. 2004, p. 352) and "Providing online firms with (the information) would involve many unexpected problems" (Malhotra et al. 2004, p. 352). According to privacy calculus theory (Laufer and Wolfe 1977; Li 2012), individuals would then perform a rational tradeoff between the perceived risks of information disclosure and the perceived benefits of information disclosure to form their intention to use privacy-invasive information systems. However, although it might well be that Jeff came to a risk perception in terms of a vague feeling, he might not necessarily be sure that his risk judgment is valid. Thus, the question whether individuals are able to perform confident privacy risk tradeoffs arises.

Based on evaluability theory, we argue that most individuals just like Jeff are not able to evaluate risks inherently. It might rather be that they lack sufficient information as well as clear and stable internal preferences to form consistent opinions regarding the quality of product attributes in general (Creyer and Ross 1997) and privacy threats in particular (Dinev et al. 2015). Such product attributes are referred to as *difficult to evaluate* in evaluability theory (Hsee and Zhang 2010). When being confronted with objectively observable product attributes that are difficult to evaluate, individuals generally react insensitive to changes in the quality of these (Hsee et al. 1999). However, if provided with external reference information facilitating evaluation, sensitivity increases, because individuals have guidance in telling whether a certain manifestation of a product attribute is good or bad and as a consequence regard their evaluation of the attribute quality as more valid and therefore incorporate it more

strongly in their decision-making (Hsee and Zhang 2010). Hence, the impact of privacy risk perceptions should depend on how they were formed. To date, this potential coupling between the formation and impact of perceived privacy risks has not been considered in IS privacy research. However, if proven true, measurements of perceived privacy risks and their empirically observed correlations with behavioral consequences would be rendered incomparable due to differences in available reference information across studies. Therefore, we challenge the assumption that individuals are inherently able to form confident risk perceptions. Consequently, we question the basic assertion of privacy calculus theory that perceived privacy risks as measured in current research uniformly influence usage intentions of privacy-invasive information systems independently of how they were formed. Accordingly, we investigate the following research questions:

RQ 1: Are users of privacy-invasive information systems able to evaluate the privacy risk associated with the disclosure of a certain amount of personal information independently?

RQ 2: Do perceived privacy risks influence behavior differently when they are formed in conditions that facilitate evaluation compared to when they are difficult to evaluate?

By incorporating an evaluability perspective (Hsee and Zhang 2010) into the privacy calculus (Laufer and Wolfe 1977; Smith et al. 2011), we develop theoretical arguments that individuals react relatively insensitive to changes in the amount of data gathered by an information system, when they have to rely entirely on their "inner scale" and hinge on intuitive risk judgments when deciding whether to use a privacy-invasive information system. Only if reference information facilitating the risk judgment is made available, the amount of data gathered by an application affects risk perceptions and these are perceived as sufficiently substantiated to serve as decision-basis. We provide empirical evidence for these propositions based on an experimental survey study among 233 participants and thereby show that the presence of reference information significantly increases the effect of the amount of data gathered by a privacy-invasive application on the perceived risk of information disclosure as well as the effect of the perceived risks of information disclosure on the behavioral intention to use a privacy-invasive information system.

The remainder of this paper is structured as follows: We begin by outlining the theoretical background of our research in two steps: First, we discuss in how far the amount of data gathered by a privacy-invasive information system constitutes a difficult-to-evaluate product attribute. We then extend privacy calculus theory by proposing that the effect of the perceived

risks of information disclosure on the intention to download an application depends on how risk perceptions were formed. Afterwards, we describe the experimental survey study we conducted to empirically test our deduced hypotheses and subsequently present our findings. We then discuss our findings, depict limitations of our study and propose promising future research opportunities. Finally, the paper closes with a conclusion.

5.2 Theoretical Background

5.2.1 The Evaluability of Personal Information Disclosures

IS privacy research is concerned with the reactions of individuals to privacy-invasive information systems (e.g., Dinev et al. 2006; Krasnova et al. 2012; Li et al. 2010; Xu et al. 2009). Privacy-invasive information systems refer to information systems that gather, store and process information about their users. As providers could use this information in unforeseen ways or share it with third parties, the use of a privacy-invasive information system is regularly associated with a loss of control about one's personal information (Malhotra et al. 2004). This loss of control can propagate and persist for an unpredictable span of time (Acquisti and Grossklags 2003). Thus, the central property of privacy-invasive information systems is that using them is associated with potentially negative consequences resulting from a loss of privacy. This potential loss is captured by the concept of *perceived risks of information disclosure* and has been investigated as an antecedent to information disclosure and usage behavior in numerous studies (e.g., Fortes and Rita 2016; Krasnova et al. 2010; Min and Kim 2015; Pavlou and Fygenson 2006; Sharma and Crossler 2014; Wang et al. 2016). Findings show that high perceptions of privacy risks are associated with a lower intention to use privacy-invasive information systems (e.g., Bélanger and Carter 2008; Xu and Gupta 2009; Xu et al. 2011) and intentions to disclose personal information in particular (e.g., Li et al. 2014; Xu et al. 2009).

Risk perceptions are thereby measured by asking survey participants to indicate the extent to which they agree to statements like "There would be high potential for loss associated with giving (the information) to online firms" or "Providing online firms with (the information) would involve many unexpected problems" (Malhotra et al. 2004, p. 352). However, what has remained unconsidered to date is whether survey participants are able to evaluate the risks associated with the disclosure of a certain set of their personal information in the first place. It might well be, that they are simply unable to tell whether disclosing, for example, address information while using a certain privacy-invasive information system is associated with low,

mediocre or high privacy risks. This ability or inability to inherently judge the quality of product attributes is discussed in psychology under the term *evaluability* (Hsee 1996b; Hsee 2000; Hsee and Zhang 2010). Evaluability is defined as "… the extent to which a person has relevant reference information to gauge the desirability of target values and map them onto evaluation" (Hsee and Zhang 2010, p. 344f.). Thus, if people lack the ability to inherently judge privacy risks, the evaluation of privacy risks becomes dependent on what information is available to survey participants in different contexts. The consequence for IS privacy research would be highly problematic. Measurements of perceived risks of information disclosure would have to be interpreted against the background of how easy to evaluate they were in the study at hand. This would impose vast limitation on the comparability and integratability of existing IS privacy studies.

The reason why privacy risks might be difficult to evaluate is that they are not a simple passive registration of sensory input. They are rather the result of a complex cognitive process, in which external stimuli are selected, organized and interpreted (Solomon et al. 2006). In the case of privacy risk perceptions, relevant stimuli include the requested amount of personal information (Phelps et al. 2000), privacy policies (Gerlach et al. 2015) or privacy seals (Huang et al. 2005). Firstly, these stimuli have to draw an individuals' attention to become incorporated in the perception formation process. During the following interpretation phase individuals "assign meaning to stimuli" (Solomon et al. 2006, p. 137) by relating them to personal preferences, knowledge acquired through prior experiences or external sources and other perceptions. Relevant preferences in the area of IS privacy research include, for example, one's individual risk-taking propensity (e.g., Xu et al. 2005) or innovativeness (e.g., Li et al. 2016). Knowledge or perceptions to be considered include, for example, prior experiences of privacy violations (e.g., Bansal et al. 2016; Xu et al. 2011), the awareness of legislative protection (e.g., Xu et al. 2012), the trust towards an application provider (e.g., Bélanger and Carter 2008; Kesharwani and Bisht 2012) or how relevant the information to be disclosed are for the purpose of the information system (e.g., Sarathy and Li 2007; Sharma and Crossler 2014). Consequently, the formation of privacy risk perceptions is a complex cognitive process based on a great number of external and internal information.

Now the question arises, whether all this information is typically available to individuals when they are asked to indicate their perceived privacy risks. Looking at extant research, it seems that oftentimes it is not (Acquisti et al. 2015; Acquisti and Grossklags 2005a; Acquisti and Grossklags 2005b; John et al. 2011; Tsai et al. 2011). For instance, it is usually not

observable for users when and which information is collected about them (Acquisti et al. 2015) or how their personal information is used by the party it was disclosed to (Acquisti and Grossklags 2005a; Acquisti and Grossklags 2005b). Furthermore, individuals seem to be unsure about their own privacy-related values and preferences (Acquisti et al. 2015), which could serve as reference information external stimuli can be compared to (Creyer and Ross 1997). The lack of (1) privacy-related knowledge, (2) information about the functioning of privacy-invasive information systems and (3) internal privacy-related preferences leads us to assume that the evaluability of the privacy risks associated with the disclosure of a certain set of personal information is low in general.

What are the consequences of this low evaluability when measuring the perceived risks of information disclosure? Various studies have been conducted, showing that individuals become unresponsive to changes in the value of an objective attribute if its evaluability is low (Hsee 1996b; Hsee 1998; Hsee 2000; Hsee and Zhang 2010). This results from the lack of "… knowledge about which value on the attribute is evaluatively neutral, which value is the best possible, which is the worst possible, what the distribution of the attribute is, and any other information that helps the evaluator map a given value of an attribute onto the evaluation scale" (Hsee et al. 1999, p. 578) described in the prior paragraph. Transferred to information disclosure situations, this implies that if sufficient information is unavailable to study participants, they cannot tell whether disclosing for example address information while using a privacy-invasive information system is associated with low, mediocre or high privacy risks. In such a situation, individuals have the tendency to rate an attribute to be neutral on average (Hsee et al. 1999). The statistically observable relationship between the amount of information gathered by a privacy-invasive information system and the perceived risk of information disclosure it evokes would therefore be insignificant or relatively small in low-evaluability situations.

However, the evaluability of a generally difficult to evaluate attribute can be increased by providing the evaluator with additional reference information (Hsee et al. 1999). An increased evaluability would result in an increased sensitivity to attribute values and therefore also a more pronounced statistical relationship between the amount of personal information gathered by a privacy-invasive information system and the perceived risk of information disclosure. A common and widely used approach of providing such reference information is by letting individuals evaluate products in two different evaluation modes: single and joint evaluation (Bazerman et al. 1999; González-Vallejo and Moran 2001; Hsee 2000; Hsee et al. 1999).

Suppose for example two information systems of which one requires users to disclose more information than the other. In single evaluation mode, each of the applications is evaluated by a different group of evaluators who are not aware of the other application. In this case evaluability should be low resulting in low sensitivity towards the amount of information to be disclosed and similar risk perceptions towards both applications. In joint evaluation mode one group of evaluators is confronted with both information systems and rates them simultaneously. In this mode, individuals can compare the amounts of information gathered by both systems. Such a comparison facilitates evaluation as the relationship between the amount of information disclosed and the resulting privacy risks is monotonic (disclosing additional information always alters the privacy risks in the same direction) and individuals know which direction of the attribute is associated with lower/higher risks (the more information being disclosed, the higher the resulting privacy risk). It is therefore obvious that the application requiring more personal information is associated with higher privacy risks in joint evaluation mode. Thus, the amount of personal information gathered by the information systems should exert a greater influence on the perceived risks of information disclosure. Therefore, our first two hypotheses as depicted in Figure 8 are the following:

H1: *The amount of personal information gathered by an information system is positively related to the perceived risk of information disclosure.*

H2: *The magnitude of effect of the amount of information gathered by an information system on the perceived risk of information disclosure is greater in joint evaluation mode compared to single evaluation mode.*

After elaborating on the formation of perceived privacy risks against the background of evaluability of the amount of information gathered by an information system (RQ 1), we now turn to the effects of perceived privacy risks formed under conditions of easy vs. difficult evaluability (RQ 2).

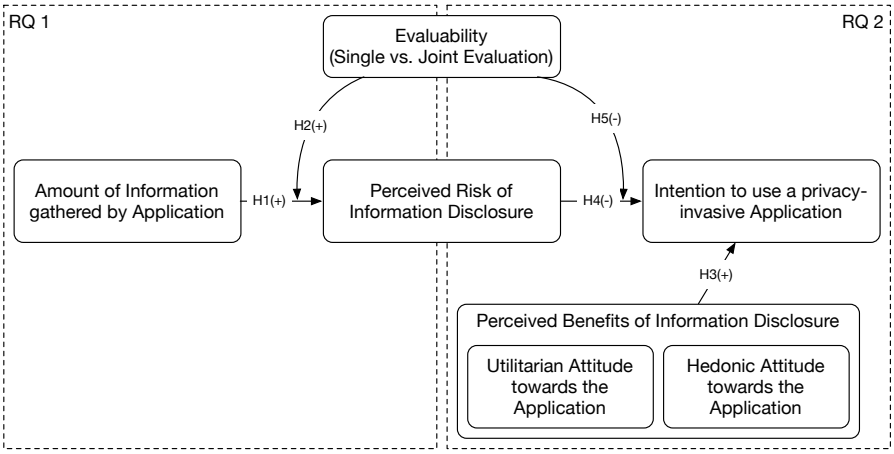

Figure 8: Research Model (Paper C).

5.2.2 The Effects of Risk Perceptions Formed in Different Evaluation Modes on User Behavior

In the previous section, we elaborated on how privacy risk perceptions are formed and thereby differentiated between contexts in which they are easy vs. difficult to evaluate. However, the evaluability of an attribute does not only influence an individual's reaction to objective stimuli and therefore the formation of perceptions, but also how these perceptions influence behavior. This is referred to as *evaluability bias*: "the tendency to weight the importance of an attribute in proportion to its ease of evaluation" (Caviola et al. 2014, p. 304). Hence, the evaluability of personal information disclosed via a privacy-invasive information system might not only affect the formation of risk perceptions but also the effect of privacy risk perceptions in subsequent decision-making. In the IS privacy context, subsequent decision making based on privacy risk perceptions almost unanimously refers to the decision whether the disclosure of personal information to a privacy-invasive information system is acceptable and therefore whether individuals intend to use a certain privacy-invasive information system (e.g., Bélanger and Carter 2008; Xu and Gupta 2009; Xu et al. 2011).

This section is therefore concerned with the question how risk perceptions formed under low vs. high evaluability conditions affect individuals' behavioral intentions to use privacy-invasive information systems (RQ 2). The theoretical basis of this consideration in IS privacy research is privacy calculus theory (Laufer and Wolfe 1977; Li 2012; Morosan and DeFranco 2015; Wang et al. 2016; Xu et al. 2009), which we adopt as foundation of our research. According to privacy calculus theory, individuals perform a rational tradeoff between the *perceived benefits* and *risks of information disclosure* when forming an *intention to use a privacy-invasive information system*. The corresponding research hypotheses are as follows:

H3: The perceived benefits of information disclosure are positively related to the behavioral intention to use a privacy-invasive information system.

H4: The perceived risks of information disclosure are negatively related to the behavioral intention to use a privacy-invasive information system.

These hypotheses imply, that privacy calculus theory assumes a simple linear relationship between the perceived risks of information disclosure and an individual's behavioral intention to disclose personal information. The higher the perceived risk of information disclosure, the less likely will an individual use a certain information system. The fact that risk perceptions can be the result of different types of deliberations is ignored here. Suppose that in single evaluation mode (and therefore under low evaluability conditions) individuals rate the risks of information disclosure according to gut feeling. They have a vague idea about how large risks might be, but cannot really reason their perceptions. However, if we measure an individual's perceived risk of information disclosure with established scales like those by Malhotra et al. (2004) or Dinev et al. (2006), individuals will still indicate some amount of risk – maybe even the same amount as a person with all information about the actual risk at hand (and therefore under high evaluability conditions). These two measurements are then indistinguishable with respect to state-of-the-art methods of measuring risk perceptions. Hence, they are regarded to be conceptually equivalent in privacy calculus theory and should exert the same effect on the behavioral intention to use a privacy information system.

Against the background of evaluability theory, this assumption does not hold. Evaluability theory proposes that the two risk ratings described above – albeit being equivalent in terms of their extremity – should differ with regard to their importance in decision making and therefore also behavior formation (Caviola et al. 2014). In particular, a risk perception formed in joint evaluation mode (and therefore high evaluability conditions) should exert greater impact on an individual's behavioral intention to use a privacy-invasive information system compared to a risk perception of equal extremity formed in single evaluation mode (and therefore under low evaluability conditions). This is because evaluability - as a property of a product attribute - is closely linked to the concept of confidence (Boldt et al. 2017), which is a property of a perception evoked by a product attribute (Lichtenstein and Burton 1988). The confidence of a perception is defined as the degree to which an individual has "… a sense that his beliefs and judgements are veridical" (Kelley 1973, p. 107). It resembles in how far individuals were able to use causal inferences to establish the validity of their perceptions. This ability depends on how much consistent information was at hand while forming a

perception (Mizerski et al. 1979) and therefore on evaluability. For product attributes with low-evaluability like privacy risks, only few reference information about the quality of the attribute is available to individuals inherently. If this information is missing, confidence in one's own perceived risks of information disclosure should be low. If evaluability is increased by providing additional information, individuals should be more confident that the privacy risks they perceive are valid.

The confidence of a perception resulting from the evaluability of underlying product attributes has been shown to moderate this perception's effect in subsequent decisions (Lichtenstein and Burton 1988). The lower the evaluability of a product attribute and therefore the confidence in a resulting perception, the lesser will this perception influence behavioral reactions. Therefore we extend privacy calculus theory by taking into account, that the magnitude of effect of risk perceptions formed in single evaluation mode (low evaluability and therefore low confidence) should be smaller than that of risk perceptions formed in joint evaluation mode (high evaluability and therefore high confidence). Thus, our last hypothesis is the following:

H5: The effect of the perceived risks of information disclosure on the intention to use a privacy-invasive information system is greater in joint evaluation mode compared to single evaluation mode.

The complete research model with all constructs and hypotheses is depicted in Figure 8.

5.3 Research Method

In order to test the formulated hypotheses, we designed a scenario-based experimental survey study, which investigates how different amounts of information gathered by a smartphone app are evaluated in single vs. joint evaluation mode (Hsee et al. 1999) and in how far these risk perceptions influence individuals' usage intentions. Our survey was based on a hypothetical scenario. The use of hypothetical scenarios is a common approach in IS privacy research (Hann et al. 2007; Malhotra et al. 2004; Pan and Zinkhan 2006), because contextual variables have been found to have a strong influence on privacy-related decisions (Smith et al. 2011). Scenario-based surveys allow to maintain a high degree of control over the independent and contextual variables and thereby minimize the effects of disturbance variables (Aviram 2012; Finch 1987; Xu and Teo 2004).

A smartphone application was deliberately chosen as context for our study because of (1) their broad dissemination and the resulting familiarity with this type of applications, (2) the simple adoption process, (3) the structured presentation in smartphone app stores facilitating

comparisons and the (4) clear and explicit presentation of information such applications require access to. The number of 149.3 billion smartphone app downloads worldwide in 2016 (Perez 2017) reflects how common it is for humans to search for and to evaluate this kind of applications. The presentation of apps to users is largely defined by the smartphone's app store and therefore similar across all apps. In addition, it is common for smartphone apps to ask users to grant them access to a wide range of personal information like photos, contacts or location services (Olmstead and Atkinson 2010). In contrast to other information systems, these permissions are clearly stated and can be precisely listed within an app description. This clearly delineates the personal information that is disclosed when users decide to adopt an application. All these aspects should make the evaluation process especially easy for users in this context. Hence, if we can observe our hypothesized relationships in this setting, they should also hold in settings where evaluability is lower due to the less structured presentation of information systems.

Two different screenshots showing the app store presentation of two hypothetical task management apps were used as experimental manipulations (see Figure 9). A task management app was chosen for three reasons: (1) it is reasonable to believe that this kind of app requires access to personal information stored on a smartphone, e.g., to be able to assign tasks to contacts or show due dates in a calendar, (2) no major market leader provides a task management app that would serve as an unwanted reference point for participants in our experimental study and (3) a task management app is relatively transparent regarding its functionality and therefore easy to evaluate in terms of the benefits it provides to users. This last point is especially important because our research focus is on the evaluability of privacy risks while keeping the benefits easy to evaluate in single- as well as in joint evaluation mode.

Two app store screenshots (see Figure 9) featuring two apps that differed with regard to the amount of personal information they require users to grant access to were carefully crafted. As both applications are presented side-by-side in joint evaluation mode, we followed the approach by Egelman et al. (2013), and also changed the design of the two app logos, so that the research topic under investigation is not too obvious for study participants. It also prevents the study setting from being too artificial. Two initial sets of permissions were chosen based on common permissions apps require access to on smartphones according to Olmstead and Atkinson (2010). Based on this initial set of permissions, we conducted a qualitative pre-study among 22 potential participants of our experimental survey study to iteratively refine and validate the sets of permissions, the app description and the logos. This was necessary,

because the requested permissions should not be too extreme. As individuals rarely have no knowledge at all about an attribute (Hsee et al. 1999), the number and types of permissions have to fall into a certain range which is not perceived as definitely extremely risky or definitely not risky at all in single evaluation mode. During the qualitative pre-study, students of a German university were shown the app screenshots in a randomized manner. Participants were then asked to assess the apps as if they would have just stumbled upon them in the app store and think aloud while doing so. This allowed us to asses which factors caught participants' attention, what they thought about the amount of information both applications required them to disclose and whether enough information about the functionalities of the app have been provided. After each round of interviews the amounts of information required by both apps, the app description as well as the logos were adjusted until both sets of personal information were neither seen as overly intrusive nor completely risk-free, the two logos, albeit being different, were not interfering with these assessments and participants were able to get an idea of the benefits the app provides. For example, an early set of permissions we approached participants with included access to the phone's microphone. This was nearly unanimously evaluated as being extremely invasive and inacceptable for a task management application and therefore unsuitable for the purpose of our study. The final sets comprised access to contacts and calendar for the less intrusive app (application A) and access to contacts, calendar, location data and photos for the more intrusive application (application B, see Figure 9). It is important to note that all information requested by the less intrusive app (application A) is also gathered by the more intrusive one (application B). Thus, the information collected by the less intrusive app is a strict subset of those information collected by the more invasive one. As a consequence, the more invasive app must (objectively) be at least equally risky compared to the less invasive one. The two final application screenshots used as experimental stimuli are depicted in Figure 9. The experimental materials were translated to English for presentation in this paper. The original materials shown to survey participants were in German language (all participants came from Germany) and colored.

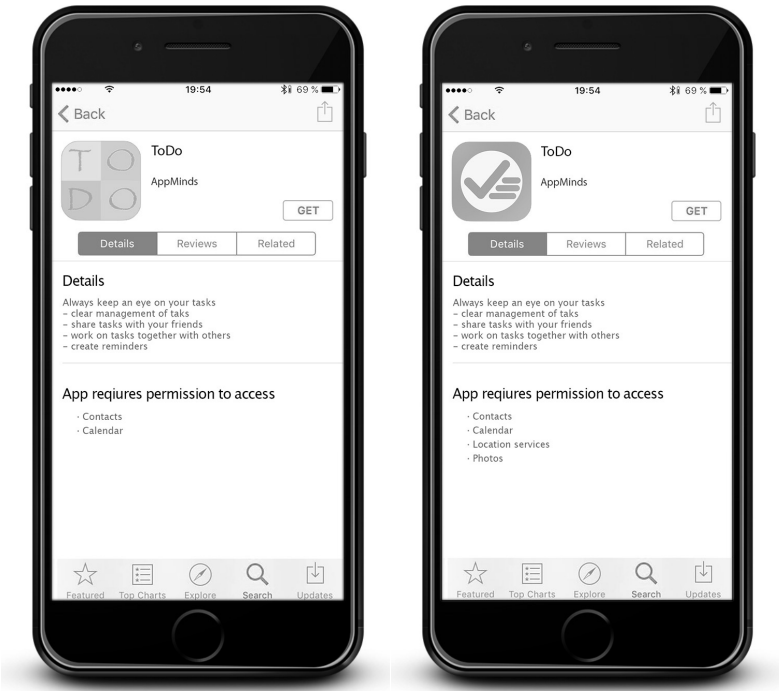

Figure 9: App Store Screenshots (translated to English).

The study was carried out as an online survey. Links to the survey were distributed to students of a large German university and via Facebook in February 2017. These channels were chosen because they allow us to reach especially younger participants in the age range between 18 and 34, as these are the largest group of users of mobile apps (comScore 2016). Additionally, younger individuals should have more technology-related knowledge (Margaryan et al. 2011). This knowledge should make it especially easy for them to evaluate the privacy risks associated with a privacy-invasive information system. If privacy risks are even difficult to evaluate for this group, the effect should also hold for less tech-savvy samples. To incentivize the respondents, we raffled gift vouchers.

Participants were first assured that their data would only be analyzed in anonymized form and that there were no right or wrong answers, so they could answer all questions honestly. This was done to counteract common method biases (Podsakoff et al. 2003). After filling out demographic measures (gender, age and employment status), participants were randomly assigned to one of three evaluation modes. Following the study design of Hsee et al. (1999), the evaluation modes are (1) single evaluation of application A, (2) single evaluation of application B, and (3) joint evaluation of both applications side-by-side. Participants were instructed to imagine that they were searching for a task management app in the app store and had just come across the depicted apps. They were then asked to thoroughly investigate them. Participants in the single evaluation modes only rated one app per participant, while those in joint evaluation mode rated both apps. According to Hsee et al. (1999), it is important for

participants in the single evaluation mode to only rate one application instead of both sequentially, to make sure that evaluations are made without any reference information. If participants would rate both applications sequentially, the second evaluation could still be influenced by the first one. To make sure this experimental manipulation is successful, a separate study was conducted as suggested by Perdue and Summers (1986). Compared to integrating manipulation checks in the main study, using a separate manipulation check study avoids measures of the dependent variable to bias the manipulation check measures or vice versa (Kidd 1976; Perdue and Summers 1986). While the manipulation check survey used the same three experimental treatments as our main study, it was limited to scales measuring the perceived privacy risks (Malhotra et al. 2004) and a measure of the perceived evaluability of privacy risks. The scale measuring perceived evaluability was self-developed based on the definition of evaluability provided by Hsee and Zhang (2010) and is given in the Appendix. Overall, 42 participants took part in the manipulation check survey (21 in single- and 21 in joint evaluation mode). The results show that evaluation modes successfully manipulated evaluability of privacy risks as participants who rated the applications in single evaluation mode perceived the evaluability of privacy risks to be significantly lower ($m = 3.16$) than those who were exposed to both applications in joint evaluation mode ($m = 4.27$, $t = -3.324$, $p = .002$).

In the main study, after being exposed to the application(s), established scales were used to measure all constructs in our research model. To abstract from concrete product features and cover utilitarian as well as hedonic aspects of product benefits, we followed the suggestion of Brakemeier et al. (2016b) and operationalized the perceived benefits of information disclosure by the hedonic and utilitarian attitudes towards the apps. These were measured by established scales from Voss et al. (2003). Both scales comprise five semantic differentials like unenjoyable/enjoyable for the hedonic and not effective/effective for the utilitarian dimension of benefits. The perceived risks of information disclosure were measured with the established scale by Malhotra et al. (2004) asking participants to indicate the degree to which they agree to statements like “There would be high potential for loss associated with providing my personal information to this application.” To measure the participants’ intention to use the app(s), they had to indicate to what extent they would download the application(s) to give it a try by means of four semantic differentials like not probable/probable. This scale was also adopted from Malhotra et al. (2004). Apart from these main constructs, we also measured the participants’ tendency to fantasize (Darrat et al. 2016) as marker variable to test for common method variance (Williams et al. 2010). The tendency towards fantasizing was chosen

because it has already been employed as marker variable in a similar context by Son and Kim (2008). Lastly, we adapted a scale by Montoya-Weiss et al. (2003) to measure the visual appeal of the two app logos as a control variable. This variable was incorporated to control for potential influences of the design of the logo on participants' risk perceptions. All survey items of the constructs in our research model can be found in the Appendix.

Apart from making sure all scales used in our survey instrument are established and empirically tested, we also placed emphasis on the fact that our measures comprise a mixture of seven point Likert scales and semantic differentials to prevent common method biases due to common scale formats (Podsakoff et al. 2003). Beyond that, we followed the suggestions of MacKenzie and Podsakoff (2012) and measured the dependent variable before measuring the independent variables and disabled the function to move back to earlier pages of the questionnaire. This was done to prevent participants from changing their answers post hoc to appear rational.

5.4 Results

A total of 265 participants completed the survey. To ensure high quality data, we incorporated an instructed response item (Meade and Craig 2012) in our survey. In about the middle of the survey one item was added along the other items measured on a 7-point Likert scale that asked participants to simply check the checkbox most to the right. We used this item to identify participants that did not thoroughly read all items. After eliminating all participants failing at the instructed response item (32), we were left with 233 participants. Of the 233 participants that correctly answered the instructed response item, 103 were assigned to joint evaluation mode and 130 to single evaluation mode (63 application A, 67 application B). To further assure data quality we also investigated the time it took participants to complete the survey. In particular, we checked for downward outliers by computing z-scores for the joint- and evaluation mode samples individually. The largest absolute z-score was 1.61 and therefore well below the threshold of 3 proposed by Kannan et al. (2015). We then conducted another post-hoc check for careless responses as described by Johnson (2005) and Meade and Craig (2012) for the 10% of participants that took the least amount of time to complete the survey. We programmed a visual basic script to compute the *Maximum LongString* for each participant. This index "… is computed as the maximum number of consecutive items on a single page to which the respondent answered with the same response option." (Meade and Craig 2012, p. 443). High *Maximum LongString* values indicate that participants tended to check the same response category for consecutive items and therefore point to inattentive

responding. We computed z-scores for the *Maximum LongString* for each participant and checked for outliers regarding this measure. The largest absolute z-score for participants in single-evaluation mode was 0.83 and for those in joint evaluation mode 0.81. Therefore, no conspicuous participants were found and we proceeded with the responses of all participants that correctly answered the instructed response item. Of those 233 participants, 101 (43.3%) were female. The age of participants ranged from 18 to 64 with the mean being 24.52 ages. The majority were students (79%) or employees (16.3%). As each participant in joint evaluation mode (103) rated both applications, our final dataset comprises a total of 336 observations in terms of application evaluations of which 130 were made in single evaluation mode and 206 in joint evaluation mode.

We used a structural equation modeling based multi-group-analysis to analyze our data. Structural equation modeling was chosen, because it allows us to test the construct relationships as well as the validity of the measurement model simultaneously (Bagozzi and Youjae 1989; Gefen et al. 2000) and thus provides a comprehensive analysis of all relationships in our research model (Fornell and Bookstein 1982). In particular, the variance-based partial least squares multi group analysis as implemented in SmartPLS (Ringle et al. 2015) was employed for two reasons: (1) It is particularly suited to test theories in early stages of development compared to variance-based approaches like LISREL (Fornell and Bookstein 1982) and (2) the multi-group-analysis provided by SmartPLS allows us to simultaneously estimate our research model for the two groups in our experimental study (single vs. joint evaluation) and test whether differences in effect sizes between those models are significant. In PLS multi group analyses, a structural equation model is estimated for two different subsamples. In our case one model is estimated for observations made in joint evaluation mode and one for participants in single evaluation mode. A bootstrapping procedure is then used to assess, whether path coefficients differ significantly between these two models (Hair et al. 2017; Henseler 2012). As we hypothesized that the effect of the amount of data gathered by a privacy-invasive application on the perceived risk of information disclosure as well as the perceived risk of information disclosure on the intention to use the app differ between single and joint evaluation mode (H2 and H5), this method is particularly suited. It allows us to avoid the common practices of noting that an independent variable significantly influences the outcome in one group but not in the other, or that an estimate of magnitude of effect appears to be larger for one group than another, without assessment of the significance of these differences (Brook et al. 1995).

Before analyzing the structural model and testing our hypotheses, we first ensure the validity of the applied measures in our survey for both samples.

5.4.1 Validation of the Measurement Model

The validity of a measurement model is assessed by means of convergent and discriminant validity of the survey instrument (Hair et al. 2014). Convergent validity refers to the degree to which items that were intended to measure the same construct are in fact statistically similar. It is assessed by means of the loadings of items on their constructs, reliability statistics like Cronbach's α and composite reliability (CR) and the average variance extracted (AVE) by the constructs (Xu et al. 2012). According to Hair et al. (2014), item reliability is given when all items have loadings higher than 0.7 on their construct. The item reliability, which is the square of its loading, then is higher than 0.5. This is the case for all items except UTL4, as can be seen in Table 8. However, we decided against omitting the item, because the loadings of 0.676 and 0.698 are only slightly below the threshold of 0.7 proposed by Hair et al. (2014) and well above the threshold of 0.55 suggested by Falk and Miller (1992). The other indicators are given in Table 9. Composite Reliability for all constructs exceeds the threshold value of 0.7 (Bagozzi and Yi 2012; Nunnally 1978) and the average variance extracted is larger than 0.5 for all constructs (Hair et al. 2011). Cronbach's α is also larger than the proposed criterion of 0.7 (Bagozzi and Yi 2012), hence all constructs meet the requirements for convergent validity in the single as well as in the joint evaluation sample.

Construct	Item	Single Evaluation Mode		Joint Evaluation Mode	
		Item Loading	Item Reliability	Item Loading	Item Reliability
Intention to Use the Application (INT)	INT1	.943	.889	.948	.899
	INT2	.955	.912	.948	.899
	INT3	.944	.891	.940	.884
	INT4	.951	.904	.927	.859
Hedonic Attitude (HED)	HED1	.859	.738	.864	.746
	HED2	.856	.733	.869	.755
	HED3	.875	.766	.908	.824
	HED4	.856	.733	.905	.819
	HED5	.810	.656	.827	.684
Utilitarian Attitude (UTL)	UTL1	.896	.803	.895	.801
	UTL2	.919	.845	.922	.850
	UTL3	.905	.819	.883	.780
	UTL4	.676	.457	.698	.487
	UTL5	.777	.604	.914	.835
Perceived Risk of Information Disclosure (RSK)	RSK1	.849	.721	.886	.785
	RSK2	.805	.648	.909	.826
	RSK3	.924	.854	.922	.850
	RSK4	.792	.627	.867	.752
	RSK5	.717	.514	.716	.513

Table 8: Item Loadings and Item Reliabilities (Paper C).

Construct	Cr. α	CR	AVE	INT	HED	UTL	RSK
Intention to Use the Application (INT)	.963 .957	.973 .969	.899 .885	**.948** **.941**			
Hedonic Attitude (HED)	.906 .924	.929 .942	.725 .766	.620 .259	**.825** **.875**		
Utilitarian Attitude (UTL)	.892 .914	.922 .937	.706 .751	.675 .465	.614 .470	**.840** **.866**	
Perceived Risk of Information Disclosure (RSK)	.877 .912	.911 .936	.673 .745	-.233 -.466	-.123 .096	-.210 -.158	**.820** **.863**

Table 9: Cronbach's α (Cr. α), Composite Reliability (CR), Average Variance Extracted (AVE) and Construct Correlations (single evaluation sample in first lines and joint evaluation sample in second lines, Paper C).

Discriminant validity is given when items intended to measure different constructs are in fact different from other constructs by empirical standards (Hair et al. 2014). For discriminant validity, two conditions have to be met: (1) all items have to load higher on their intended construct than on any other construct (Bagozzi and Yi 2012) and (2) the variance shared between each construct and its items has to be greater than the correlations between the construct and all other constructs (Fornell and Larcker 1981). Although we do not report them in this paper due to space limitations, we investigated all cross-loadings in both samples to assure that they are substantially lower than the loadings of each item on their respective

constructs. As can be seen in Table 9, the variance shared between a construct and its associated items, computed as the square root of the AVE (diagonal elements in Table 9) is greater than all correlations between the construct and any other construct (non-diagonal elements in Table 9) in our model (Fornell and Larcker 1981). Hence, all criteria for discriminant validity are also fulfilled. As a last step, we followed the guidelines by Rönkkö and Ylitalo (2011) to make sure common method variance (Podsakoff et al. 2003) is not an issue with our data and included the tendency to fantasize as a predictor for all endogenous constructs in our model. No regression paths that were significant in the baseline model became insignificant in the model with the marker variable included. Hence, common method variance does not seem to be an issue (Rönkkö and Ylitalo 2011). Descriptive statistics for all variables in our research model can be found in the Appendix.

5.4.2 Analysis of the Structural Models

After ensuring our measurement model is valid we proceed by analyzing the overall model quality and the hypothesized construct relationships as reflected by our research model separately for the single evaluation and the joint evaluation sample. Thereby age and gender were incorporated as control variables for the intention to download the application whereas the visual appeal of the logo was used as a control variable for the perceived risks of information disclosure. This was done to control for potential influences of the different logos on the privacy risks evoked by the applications. An issue to be addressed before we proceed with the analysis is the nested structure of our data. In the joint evaluation mode sample, each participant evaluated both apps. We treated these two evaluations as independent observations in the following analysis. This is valid, because "Whereas a covariance-based maximum likelihood (ML) estimation rests on the assumptions of a specific joint multivariate distribution and independence of observations, the PLS approach does not make these hard assumptions" (Chin 2010, p. 659; see also Hoyle 1999; Vilares et al. 2010).

The overall model fit as indicated by the standardized root mean square residual are .075 for the joint evaluation sample and .077 for the single evaluation sample. This is below 0.8 and therefore indicating good model fit (Hu and Bentler 1999). Predictive validity of PLS models is assessed by the amount of variance explained in the dependent variables (R^2). Our model explains 39.4% of variance in usage intentions in the joint evaluation sample and 53.3% in the single evaluation sample. R^2 values for the perceived risks of information disclosure are .248 in joint evaluation mode and .02 in single evaluation mode.

	Path Coefficients		p-Values		Multi Group Analysis	
	SE	JE	SE	JE	Difference	p-Value
Application (A=0, B=1) → Perceived Risk	.122 (H1)	.414*** (H1)	.185	.000	.292* (H2)	.031
Perceived Risk → Intention to Use	-.089 (H4)	-.425*** (H4)	.114	.000	.336*** (H5)	.000
Utilitarian Attitude → Intention to Use	.450*** (H3)	.327*** (H3)	.000	.000	.122	. 119
Hedonic Attitude → Intention to Use	.332*** (H3)	.158* (H3)	.000	.021	.174	.054

Table 10: Results of Structural Model Testing (Paper C).

To investigate significance of path estimates, a bootstrapping (Davison and Hinkley 1997) with 5.000 resamples was performed. The path coefficients and their corresponding p-values are reported in Table 10. None of the control variables had a significant influence in either of the models. In particular, the visual appeal of the app's logos was not associated with the perceived risk of information disclosure evoked by the applications. Our first two hypotheses (RQ 1) were concerned with the effect of the amount of personal information gathered by an information system on the perceived risk of information disclosure. We found this effect to be significant in joint evaluation mode (β=.414, p=.000). However, the amount of information required by the application did not influence risk perceptions (β=.122, p=.185) in single evaluation mode. Therefore, H1 is only partially supported. The multi group analysis revealed that this difference between path coefficients is significant (difference=.292, p=.031), hence supporting H2.

In line with H5, the effect of the perceived risk of information disclosure on the intention to use the applications also differs between joint and single evaluation (difference=.336, p=.000). While the effect is significantly negative in joint evaluation mode (β=-.425, p=.000), no effect was found in single evaluation mode (β=-.0989, p=.114). Hence, H4 is only supported for the joint evaluation sample.

The utilitarian dimension of the benefits of information disclosure influences the intention to use the applications equally strong (difference=.122, p=.119) in single (β=.450, p=.000) and joint evaluation mode (β=.327, p=.000). The same holds for the hedonic dimension of benefits (SE β=.332, p=.000; JE β=.158, p=.021; difference=.174, p=.054) thus supporting H3.

5.5 Discussion

In the following, we relate our findings to extant research and discuss the implications for research and practice. The goal of our research was to show that individuals have difficulties evaluating the privacy risk associated with the disclosure of a certain amount of personal information independently (RQ 1) and, as a consequence, perceived privacy risks influence behavior differently when they are formed in conditions that facilitate evaluation compared to when they are difficult to evaluate (RQ 2).

By integrating an evaluability perspective (Hsee and Zhang 2010) into IS privacy research and providing empirical evidence for our propositions based on an experimental survey study among 233 participants, we extend existing theory in two ways: First, we provide empirical evidence that individuals react more sensitive to the amount of personal information they are required to disclose in order to use a smartphone app in joint evaluation mode compared to single evaluation mode in terms of privacy risks perceptions. In our study, the perceived privacy risks were not even significantly related at all to whether an app only requires disclosure of contacts and calendar information or location data and photos additionally when apps were evaluated independently. Only if the two apps were shown to participants simultaneously allowing them to compare the two sets of permissions, the perceived privacy risks differed significantly between the two applications.

Empirically showing that the effect of the perceived risks of information disclosure formed in single evaluation mode on the intention to use the apps differs from that of risk perceptions formed in joint evaluation mode constitutes our second extension of theory. In our experiment, the intention to use the applications is completely independent of the perceived risk of information disclosure in single evaluation mode. Only in joint evaluation mode we observed a significantly negative effect of the perceived risk of information disclosure on the intention to use the apps. These findings have several implications for theory and practice, which we will discuss in the following.

5.5.1 Implications for Research

We see three contributions our findings make to IS privacy research. First, we introduce the context-specific evaluability of information disclosures as an important moderator of the extent to which privacy risks are evoked by the disclosure of a certain amount of personal information. This finding is in line with evaluability theory (Hsee 1996b; Hsee and Zhang 2010) and supports the notion that individuals are regularly lacking clear and consistent innate

privacy-related preferences (Acquisti et al. 2015). In our study, we used single vs. joint evaluation modes to alter evaluability. Hence, by simply showing two apps side by side, we altered the risk perceptions towards those apps compared to single evaluation mode. Thus, the perceived risk of information disclosure evoked by an information system is not only dependent on properties of this focal system, but also on those of other information systems that serve as reference. We deliberately chose task management apps as context of our study. For this type of app, there is no clear market leader that intuitively comes to one's mind and might therefore serve as reference. However, if risk perceptions towards instant messaging apps are investigated, it might well be that privacy features of, for example, WhatsApp serve as a reference and alter risk perceptions towards other messaging apps. Still, information systems that might serve as a reference do not have to be exogenous. Evaluability of personal information disclosures could also be altered by factors inherent to a study. This would render measurements of perceived privacy risks incomparable across studies. IS privacy researchers should therefore take this effect into account and consciously reflect which external or internal information could serve as reference for privacy risk evaluation and control for those carefully if necessary.

A second theoretical contribution lies in the conception that the perceived risks of information disclosure may not only be characterized by an extremity (the amount of risk indicated by study participants) but also by their confidence. The concept of confidence is discussed in psychology as a property of perceptions referring to "… a belief about the validity of our own thoughts" (Grimaldi et al. 2015). The confidence of a perception is thereby dependent on "… the evidence on which decisions are based" (Boldt et al. 2017). In our experiment, evidence available for perception formation differed between single and joint evaluation mode. It seems, that the increased amount of reference information in joint evaluation mode has led to reduced "evidence variance" and therefore increased confidence in risk perceptions. (Meyniel et al. 2015; Yeung and Summerfield 2014). This could explain the stronger influence of risk perceptions on usage intentions in joint evaluation mode as confidence moderates the effect of perceptions in decision processes (Lichtenstein and Burton 1988). Furthermore, this calls for a reconceptualization of perceived privacy risks as comprising the two dimensions of extremity and confidence (Lichtenstein and Burton 1988) and therefore constituting a more complex concept than is assumed in current IS privacy research. Apart from evaluation mode, the degree to which study participants perceive their risk judgments as valid could also depend on other reference information made available to study participants like privacy policies (Gerlach et al. 2015) or privacy seals (Huang et al. 2005). Thus, confidence might be a moderating

variable that should be incorporated in research based on privacy calculus theory (Laufer and Wolfe 1977; Li 2012). This leads us to our third contribution.

Demonstrating that the adverse effect of perceived risks of information disclosure on the intention to use a privacy-invasive information system is stronger, the easier those privacy risks were to evaluate, constitutes a third contribution. The idea that the way in which risk perceptions are formed affects their consequences has not been considered in extant IS privacy research. It challenges the common conception of privacy calculus theory, that individuals perform rational tradeoffs between benefits and risks when forming an intention to use a privacy-invasive information system (Awad and Krishnan 2006). A rational tradeoff would require an individual to weight the perceived risks of information disclosure equally, independent of how they were formed (Hsee 1996b). As we have shown, this assumption cannot be maintained. Our study highlights that the tradeoff between risks and benefits of information disclosure is much more guided by misperceptions and unstable preferences. Individuals are rather insensitive to privacy risk perceptions in low evaluability situations whereas sensitivity increases in high evaluability conditions. Thus, we introduce evaluation mode as a new moderator in the privacy calculus. On a more general level and taking into consideration our second contribution as well as common theoretical reasoning (Lichtenstein and Burton 1988), one could also argue that the confidence in one's own perceived privacy risks moderates their effect on the behavioral intention to use privacy-invasive information systems. Future studies building upon privacy calculus theory should consider the moderating effect of the evaluability of privacy-relevant information system properties in their research models. This could help to explain inconsistencies in previous research based on the privacy calculus. Among these studies, the effects of the perceived risks of information disclosure on behavioral intentions vary widely. While some studies found no effect at all (e.g., de Kerviler et al. 2016; Kelley et al. 2013), others found very strong relationships (e.g., Lee 2009). These dissonant findings could be explained by differences in the evaluability of privacy risks. Furthermore, omitting differences in evaluability could threaten the external validity of privacy calculus studies. External validity denotes the degree to which research results can be transferred to real life settings (Kirk 2003). If evaluability differs between oftentimes artificial situations in privacy studies (e.g., Pan and Zinkhan 2006; Sheng et al. 2008; Son and Kim 2008) and the corresponding real life situations research aims to explain, transferability of research results to real life situations might be impaired.

5.5.2 Implications for Practice

Apart from these theoretical contributions, our findings can also inform users and providers of privacy-invasive information systems as well as policy-makers. Users of privacy-invasive information systems should be aware of their fallibility when assessing the privacy risks associated with the disclosure of a certain amount of personal information to an information system. Privacy risks might be underestimated due to an individual's inability to adequately judge privacy risks independently and therefore users might put their privacy at unreasonable risks. Providers of privacy-invasive information systems could make use of this effect by providing users with information helping them to correctly assess privacy risks and thereby turn privacy-friendliness into a competitive advantage. Malicious providers might, however, also take advantage of lacking evaluability by being vague about how risky their application actually is to profit from the tendency to rate risk as mediocre under low-evaluability conditions. As it is their duty to protect individuals from such malicious market actors, policy-makers should intervene here and stipulate providers to facilitate evaluability. This could for instance be realized by requiring providers to make easy-to-interpret cues accessible that provide users with all information necessary about the actual risk associated with a certain information system. Additionally, app store providers are on duty to offer a consistent design and a standardized way to communicate privacy-invasive properties of applications. One could draw parallels to the political discourse about traffic light labels for food to make it easier for customers to differentiate between healthy and unhealthy food here. Similar indicators could be introduced for privacy-invasive information systems to promote safer behavior and strengthen privacy-friendliness as a competitive advantage.

5.6 Limitations and Future Research Suggestions

Our research is the first to integrate evaluability issues into the privacy calculus and thereby question the ability of humans to comprehensively assess the privacy risks associated with the disclosure of personal information independently. Nevertheless, as is the case with every research, the results of this project are subject to certain limitations. A first limitation lies in the fact that we employed a hypothetical scenario in our experimental survey study. Intentions in such a hypothetical scenario might deviate from those in real-life situations. Nevertheless, employing hypothetical scenarios is a common approach in IS privacy research (e.g., Hann et al. 2007; Malhotra et al. 2004; Pan and Zinkhan 2006; Son and Kim 2008). Furthermore, we deem the approach of employing a hypothetical scenario acceptable for our study, because our goal was not to explain or predict real life adoption behavior of privacy-invasive information

systems. However, future research should also investigate the evaluability of privacy risks in real life situations and thereby provide a clearer inspection of the actual implications of our findings in real-life situations.

Another limitation is of methodological nature. Generally, in experimental designs only one factor should be altered between experimental conditions to prove causality. However, we followed the approach of numerous studies on evaluability (Hsee 1996a), information privacy in general (Bansal et al. 2010) and the study of Egelman et al. (2013) in the app-context and did not only manipulate the amount of permissions requested between the two apps in our study but also changed their logos. This was done in order to avoid the research topic under investigation from being too obvious and artificial in joint evaluation mode. It is therefore not possible to unambiguously state that the different risk perceptions were a result of differences in the amounts of permissions requested by the two apps from a purely methodological standpoint. However, based on theoretical arguments (Malheiros et al. 2013), the insignificant effect of the visual appeal of the logos on the perceived risk of information disclosure as well as evidence from our qualitative pre-study, we deem it reasonable to assume that the different logos did not severely confound our findings.

Future studies could investigate in more detail whether specific personal information or certain sets of information are easier to evaluate in terms of privacy risks than others. The sets of personal information required by the two applications in our experiment were deliberately chosen to evoke different perceptions in joint vs. single evaluation mode. Our qualitative pre-study suggests that certain information (e.g., access to the phone's microphone) are perceived as very risky per se. Evaluability might not be an issue in this case. Our results might therefore not be transferrable to arbitrary situations involving the disclosure of personal information.

The composition of our sample constitutes a third limitation. The majority of our sample was composed by students of relatively young age (mean 24.52). We deliberately chose this age group, because apps are intensively used by younger individuals (comScore 2016). Additionally, younger individuals should have more technology-related knowledge (Margaryan et al. 2011), which should make it especially easy for them to evaluate the privacy risks associated with a privacy-invasive information system. We therefore deem our results transferable to less tech-savvy samples. However, the generalizability of our findings is limited by these sample characteristics. Future studies should try to replicate our results with more diverse and larger samples.

A fruitful area for future research might also be to investigate in more detail, which cues or reference information assist individuals in evaluating information disclosure situations. Researchers could for example investigate different ways of presenting apps to users (Kelley et al. 2013) or highlighting privacy-relevant properties of applications (Bal 2014).

5.7 Conclusion

Despite the limitations presented above, we were able to offer theoretical arguments and empirical evidence that individuals have difficulties assigning risk judgments to different amounts of data that is requested from them by privacy-invasive information systems. It can therefore occur that individuals do not incorporate their risk perception into the decision whether to use privacy-invasive information systems, because they are unsure in how far their risk judgement is valid. Future research should therefore deliberately control the amount of information available to participants to ensure external validity of IS privacy studies.

We hope these findings make a useful contribution to IS privacy research by challenging the assumption that individuals perform purely rational risk assessment and proposing that they might frequently go with gut feeling when asked to rate privacy risks.

6 Thesis Contributions and Conclusion

The goal of this thesis was to improve the understanding of how individuals make decisions about the protection of their privacy in a world full of privacy-invasive information systems. In particular, the goal was to investigate how individuals perceive privacy risks and how these perceived privacy risks are incorporated into privacy-related decision processes. An improved understanding of these mental processes can have far-reaching implications for individuals, organizations as well as policy-makers in terms of personal privacy management, the design of privacy-invasive information systems and consumer protection legislation.

To approach this goal, three studies have been conducted, which focus on different stages of the mental process of processing privacy-relevant attributes of information systems. In particular, the studies were guided by three assumptions underlying the classical view of privacy calculus theory (Laufer and Wolfe 1977): (1) individuals are able to assess the perceived privacy risks and perceived benefits of information disclosure, (2) these perceptions are weighted against each other uniformly to determine the net utility associated with the disclosure of personal information and (3) an individuals' intention to disclose personal information is dependent on this net utility.

By integrating more complex theories of human decision-making into this presumably rational process, the recent call for research on principles from the area of behavioral economics that affect privacy-related decisions (Dinev et al. 2015) has been followed. All three studies provide empirical evidence, that privacy-related decision-processes should not be assumed to be deliberate and entirely rational. Rather, the process should be conceptualized as being subject to bounded rationality, cognitive shortcuts and influenced by perceptual biases (Acquisti 2009; Dinev et al. 2015).

The findings make several contributions, which will be addressed in the following sections. First, the contributions made to theory are depicted in section 6.1 and afterward the implications for users, information system providers and policy-makers are outlined in section 6.2. All contributions that will be mentioned are subject to certain limitations, which can be

found in the respective chapters of the thesis and will not be recapitulated here to avoid redundancies.

6.1 Theoretical Contributions

The contributions of this thesis can all be related to the assumptions of privacy calculus theory they put into question. The first study (see chapter 3) has shown the behavioral intention to use a privacy-invasive information system and the intention to disclose personal information to it to be different conceptualizations and represent outcomes of different types of deliberations despite being used interchangeably in research on privacy-invasive technologies (e.g., Chellappa and Sin 2005; Xu and Teo 2004). We were able to provide evidence that there exist profound differences between usage and disclosure intentions and they should therefore be considered as outcomes of different types of deliberations. In particular, the perceived risk of information disclosure has a stronger impact on the behavioral intention to disclose information than on the intention to use a privacy-invasive information system. The opposite holds for hedonic benefits provided by the information system, which have more influence on the intention to use the system than on the intention to disclose information to it. Therefore, the singular concept of a net utility does not seem to exist (assumption 2 mentioned in the previous section). People rather seem to determine the overall utility associated with the disclosure of personal information from two different standpoints simultaneously resulting in different behaviors being favored. This finding contradicts assumptions 2 and 3 mentioned above and is in line with research on the multiple selves problem (e.g., Bazerman et al. 1998; Khan et al. 2005; O'Connor et al. 2002) and a distinction between so-called *want* and *should* options (Bazerman et al. 1998). While people often *want* to use privacy-invasive information systems to realize the benefits they provide, they simultaneously know they *should not* disclose their personal information to it, albeit this is usually inevitable. Given that research has found the *should self* to be more influential in advance of a decision, while the *want self* often prevails during the actual decision (O'Connor et al. 2002), this second contribution has implications for the question, which behavioral intention better predicts actual behavior. It is reasonable to assume, that the behavioral intention to use a privacy-invasive information system is a better predictor of actual behavior than the intention to disclose personal information.

Paper B further extends these contributions by investigating not only differences of effect sizes in the privacy calculus when different dependent variables are used, but whether such differences can also be observed inherently with only one dependent variable. Thereby, it

further investigates the assumption that privacy risks and benefits of information disclosure possess additive utility and are therefore weighted against each other linearly. By integrating regulatory focus theory into the privacy calculus, arguments are provided why the result of the privacy calculus should not be considered to be a net outcome utility (Awad and Krishnan 2006). It is rather proposed, that risk minimization and benefit maximization should be considered different types of goals serving either prevention (concerned with the absence of negative outcomes) or promotion needs (concerned with the presence of positive outcomes) (Higgins 1997; Higgins 1998). Whether prevention or promotion goals are given stronger weights is in turn determined by an individuals' regulatory focus – a person's sensitivity to negative (risk-related) and positive (benefit-related) decision outcomes. This regulatory focus can be altered by as little as letting people recall their current hopes and aspirations (for a promotion focus) or duties and obligations (for a prevention focus). Therefore, the effect sizes measured in extant information systems privacy research based on privacy calculus theory might be very unstable across contexts.

The study is also the first to directly test a correlation between the perceived risks of information disclosure and a person's regulatory focus, which constitutes another contribution of Paper B. In particular, the higher privacy risks an individual perceives, the more prevention-focused will it become and therefore the importance of privacy risks will increase in subsequent decisions. Thus, instead of linearly influencing the overall utility of information disclosures, individuals rather seem to have an internal risk threshold. If risks are below this threshold, people adopt a state of incautiousness and are focused on the benefits provided by information systems while not caring much about risks. Only if a certain level of risks is exceeded, sensitivity for risks increases and they become more influential in the determination of overall utility and therefore behavior. Consequently, one would expect the effect of the perceived risks of information disclosure in the privacy calculus to be higher for a more invasive technology compared to a less invasive. Contrary, the effects of the perceived benefits of information disclosure should be lower the more invasive the technology is. The fundamental assumption in most research based on privacy calculus theory (Laufer and Wolfe 1977; Li 2012) therefore cannot be maintained.

The third study refutes the first assumption of privacy research mentioned above by showing that human beings are not always able to assess the privacy risks associated with the disclosure of certain personal information. In particular, the results show that by simply displaying two applications to individuals side by side, risk perceptions were altered

compared to when the same applications were shown to participants separately. This finding suggests that perceived risks of information disclosure evoked by privacy-invasive applications do not solely depend on properties of the system. It rather seems that individuals are unsure whether disclosing certain information to a certain information system is associated with low, mediocre or high risks and therefore base their assessments on external reference information in form of different applications they can compare the focal one to. Without considering this effect, measurements of perceived risk of information disclosure are rendered incomparable across studies.

As privacy risks seem to be difficult to evaluate, another theoretical contribution emerges: Perceived risks of information disclosure may not only be characterized by an extremity (the amount of risk indicated by study participants) but also a confidence (Lichtenstein and Burton 1988). The concept of confidence is discussed in psychology as a property of perceptions referring to "… a belief about the validity of our own thoughts" (Grimaldi et al. 2015) and is dependent on "… the evidence on which decisions are based" (Boldt et al. 2017). This dimension of privacy risks should therefore be integrated into information systems privacy research because empirical findings suggest that it might moderate the effect of privacy risks in subsequent decision-making. Taken together, these findings from Paper C suggest that the assumption that individuals are able to perform thorough and deliberate risk estimations also has to be treated with caution.

Apart from these theoretical implications, this thesis can also inform practitioners developing privacy-invasive applications, users of such systems and policy-makers. These practical implications are discussed in the following section.

6.2 Practical Contributions

The studies in this thesis offer valuable insights that can be applied by providers of privacy-invasive information systems, users of such systems as well as policy-makers. The implications for each of these groups will be addressed in this order.

Given that individuals rate risks and benefits in the privacy calculus differently depending on (1) the prevalence of the *want* vs. *should self* during the evaluation of an information system and (2) their predominant regulatory focus at the moment of evaluation, manufacturers can leverage these effects by creating conditions, that make people lean towards either being more or less sensitive towards risks or benefits respectively. For example, research has shown, that the shorter the time between purchasing a product and its delivery, the stronger people tend to

follow their *want* preferences in purchase decisions (Milkman et al. 2010; Oster and Scott Morton 2005). Reducing the time between deciding on the adoption of an application and the realization of the benefits it provides may analogously bolster the influence of the *want self* and thereby reduce the influence of privacy risks. Furthermore, presenting products separately instead of jointly with other alternatives avoids direct comparisons between alternatives and thus makes *should* / *should-not* options less obvious (Bazerman et al. 1999).

Another important managerial implication addresses the shortcoming of privacy calculus theory that specific recommendations for providers of privacy-invasive information systems could hardly be deduced due to the assumption of a simple linear negative influence of perceived privacy risks on an individuals' intention to disclose his or her personal information. From this perspective, providers of privacy-invasive information systems should simply reduce the privacy risks evoked by their applications as much as possible. However, this is usually unfeasible as data is oftentimes inevitably needed to provide certain functionalities and limited resources in terms of money, time and manpower. The findings in this thesis contribute to a better understanding of which level of privacy is *good enough*. Thus, more specific recommendations can be made: If an information system evokes such extreme privacy risks that it evokes a prevention focus, the adoption decision of potential users is mainly driven by risk perceptions and providers should try to reduce these risks. If the risk already is at a sufficiently low level, benefits are the more influential antecedent for the customers' disclosure intention and thus indirectly their likelihood of adoption. In such cases, investments should focus on improved quality and functionality instead of privacy friendliness.

Apart from these managerial considerations, the research in this thesis can also help to promote safer and conscious behaviors among users of privacy-invasive information systems. They should be aware, that minimal situational cues can vastly influence their willingness to take privacy risks and they are oftentimes unable to confidently evaluate privacy risks. Therefore, they should pay close attention to the context in which they evaluate a privacy-invasive information system and assure themselves of how much risk they expose themselves to. Otherwise, they might underestimate or neglect privacy risks, which can result in unreasonable behaviors, that may be regretted later.

The finding that individuals have difficulties assessing the privacy risks they take also has implications for policy-makers, in particular, consumer protection legislation. The purpose of such legislation would be to prevent customers from putting themselves at unreasonable risks

and avoid firms to exploit the inability of individuals to evaluate privacy risks. This could be achieved by forcing firms to provide easily interpretable information that helps users to determine the actual risk associated with the disclosure of personal information to an information system. One could draw parallels to the political discourse about traffic light labels for food to make it easier for customers to differentiate between healthy and unhealthy food. Similar indicators could be introduced for privacy-invasive information systems to promote safer behavior and strengthen privacy-friendliness as a competitive advantage.

6.3 Conclusion

The research in this thesis improved the understanding of how individuals form privacy risk perceptions and how these risk perceptions are incorporated into privacy-related decision processes. The findings contribute to an improved understanding of these mental processes based on the results of three large-scale quantitative studies using experimental approaches and supported by multiple qualitative and quantitative pre-studies.

In particular, the findings show that widely accepted assumptions underlying information systems privacy research are over-simplified. By integrating more complex theories of human decision-making into information systems privacy research, different stages of the mental process of processing privacy-relevant attributes of information systems have been investigated. The results provide empirical evidence that privacy-related decisions are oftentimes not the result of deliberate and thoughtful considerations and privacy-related preferences of individuals are oftentimes unstable. This thesis therefore offers more detailed insights concerning the mechanisms leading to the acceptance of privacy-invasive information systems.

I hope these findings make a useful contribution to information systems privacy research by informing future research and provide a theoretical basis for future studies aiming to further investigate how risk perceptions are formed and how they are processed mentally.

References

Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," *Proceedings of the 5th ACM Conference on Electronic Commerce*, pp. 21-29.

Acquisti, A. 2009. "Nudging Privacy: The Behavioral Economics of Personal Information," *Security & Privacy* (7:6), pp. 82-85.

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), pp. 509-514.

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

Acquisti, A., and Grossklags, J. 2005a. "Privacy and Rationality in Individual Decision Making," *Security & Privacy* (3:1), pp. 26-33.

Acquisti, A., and Grossklags, J. 2005b. "Uncertainty, Ambiguity and Privacy," *Fourth Workshop on The Economics of Information Security*, Cambridge, MA.

Acquisti, A., John, L. K., and Loewenstein, G. 2012. "The Impact of Relative Standards on the Propensity to Disclose," *Journal of Marketing Research* (49:2), pp. 160-174.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.

Ajzen, I., and Fishbein, M. 1969. "The Prediction of Behavioral Intentions in a Choice Situation," *Journal of Experimental Social Psychology* (5:4), pp. 400-416.

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behaviour*. Upper Saddle River, NJ: Prentice-Hall.

Ajzen, I., and Fishbein, M. 2000. "Attitudes and the Attitude-Behavior Relation: Reasoned and Automatic Processes," *European Review of Social Psychology* (11:1), pp. 1-33.

Alba, J. W., and Williams, E. F. 2013. "Pleasure Principles: A Review of Research on Hedonic Consumption," *Journal of Consumer Psychology* (23:1), pp. 2-18.

Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339-370.

Ariely, D. 2009. "The End of Rational Economics," *Harvard Business Review* (87:7/8), pp. 78-84.

Aviram, H. 2012. "What Would You Do? Conducting Web-Based Factorial Vignette Surveys," in *Handbook of Survey Methodology for the Social Sciences,* L. Gideon (ed.). New York, NY: Springer, pp. 463-473.

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13-28.

Babin, B. J., Darden, W. R., and Griffin, M. 1994. "Work and/or Fun: Measuring Hedonic and Utilitarian Shopping Value," *Journal of Consumer Research* (20:4), pp. 644-656.

Bagozzi, R. P. 1977. "Structural Equation Models in Experimental Research," *Journal of Marketing Research* (14:2), pp. 209-226.

Bagozzi, R. P., and Yi, Y. 2012. "Specification, Evaluation, and Interpretation of Structural Equation Models," *Journal of the Academy of Marketing Science* (40:1), pp. 8-34.

Bagozzi, R. P., and Youjae, Y. I. 1989. "On the Use of Structural Equation Models in Experimental Designs," *Journal of Marketing Research* (26:3), pp. 271-284.

Bal, G. 2014. "Designing Privacy Indicators for Smartphone App Markets: A New Perspective on the Nature of Privacy Risks of Apps," *Proceedings of the Americas Conference on Information Systems*, Savannah, GA.

Bansal, G., Zahedi, F. M., and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49:2), pp. 138-150.

Bansal, G., Zahedi, F. M., and Gefen, D. 2016. "Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online," *Information & Management* (53:1), pp. 1-21.

Bartlett, M. S. 1950. "Tests of Significance in Factor Analysis," *British Journal of Statistical Psychology* (3:2), pp. 77-85.

Batra, R., and Ahtola, O. T. 1991. "Measuring the Hedonic and Utilitarian Sources of Consumer Attitudes," *Marketing Letters* (2:2), pp. 159-170.

Bazerman, M. H., Moore, D. A., Tenbrunsel, A. E., Wade-Benzoni, K. A., and Blount, S. 1999. "Explaining How Preferences Change across Joint Versus Separate Evaluation," *Journal of Economic Behavior & Organization* (39:1), pp. 41-58.

Bazerman, M. H., Tenbrunsel, A. E., and Wade-Benzoni, K. 1998. "Negotiating with Yourself and Losing: Making Decisions with Competing Internal Preferences," *Academy of Management Review* (23:2), pp. 225-241.

Bélanger, F., and Carter, L. 2008. "Trust and Risk in E-Government Adoption," *Journal of Strategic Information Systems* (17:2), pp. 165-176.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1042.

Bitterly, T. B., Mislavsky, R., Dai, H., and Milkman, K. L. 2014. "Dueling with Desire: A Synthesis of Past Research on Want/Should Conflict," in *The Psychology of Desire,* W. Hofmann and L.F. Nordgren (eds.). New York, NY: Guilford Press.

Boldt, A., de Gardelle, V., and Yeung, N. 2017. "The Impact of Evidence Reliability on Sensitivity and Bias in Decision Confidence," *Journal of Experimental Psychology: Human Perception and Performance* (43:8), pp. 1520-1531.

Brakemeier, H., Widjaja, T., and Buxmann, P. 2016b. "Distinguishing Usage and Disclosure Intentions in Privacy Research: How Our Two Selves Bring About Differences in the Effects of Benefits and Risks," *Proceedings of the European Conference on Information Systems*, Istanbul, Turkey.

Breckenridge, A. C. 1970. *The Right to Privacy*. Lincoln, NE: University of Nebraska Press.

Brook, J. S., Whiteman, M., and Cohen, P. 1995. "Stage of Drug Use, Aggression, and Theft/Vandalism: Shared and Unshared Risks," in *Drugs, Crime, and Other Deviant Adaptions: Longitudinal Studies,* H.B. Kaplan (ed.). New York: Springer Science and Business Media, pp. 83-96.

Brown, B. L., Hendrix, S. B., Hedges, D. W., and Smith, T. B. 2011. "Multiple Regression and the General Linear Model," in *Multivariate Analysis for the Biobehavioral and Social Sciences*. Hoboken, NJ: John Wiley & Sons, Inc., pp. 373-442.

Bruner, G. C., Hensel, P. J., and James, K. E. 2001. *Marketing Scales Handbook*, (5 ed.). Chicago: American Marketing Association.

Buxmann, P. 2015. "Big Data: Neue Geschäftsmodelle Für Die Future Internet Economy," in *Digitales Neuland: Warum Deutschlands Manager jetzt Revolutionäre werden,* T. Becker and C. Knop (eds.). Wiesbaden: Springer, pp. 139-153.

Camerer, C. F., and Loewenstein, G. 2011. "Behavioral Economics: Past, Present, Future," in *Advances in Behavioral Economics,* C.F. Camerer, G. Loewenstein and M. Rabin (eds.). Princeton, NJ: Princeton University Press.

Campbell, J. E., and Carlson, M. 2002. "Panopticon.Com: Online Surveillance and the Commodification of Privacy," *Journal of Broadcasting & Electronic Media* (46:4), pp. 586-606.

Caviola, L., Faulmüller, N., Everett, J. A. C., Savulescu, J., and Kahane, G. 2014. "The Evaluability Bias in Charitable Giving: Saving Administration Costs or Saving Lives?," *Judgment and Decision Making* (9:4), pp. 303-315.

Checkland, P., and Scholes, J. 1999. *Soft Systems Methodology in Action*. Hoboken, NJ: John Wiley & Sons Inc.

Chellappa, R. K., and Sin, R. G. 2005. "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6:2-3), pp. 181-202.

Chen, H., Chiang, R. H., and Storey, V. C. 2012. "Business Intelligence and Analytics: From Big Data to Big Impact," *MIS Quarterly* (36:4), pp. 1165-1188.

Chernev, A. 2004. "Goal-Attribute Compatibility in Consumer Choice," *Journal of Consumer Psychology* (14:1), pp. 141-150.

Chin, W. W. 2010. "How to Write up and Report PLS Analyses," in *Handbook of Partial Least Squares: Concepts, Methods and Applications,* V.E. Vinzi, W.W. Chin, J. Henseler and H. Wang (eds.). Berlin, Heidelberg: Springer, pp. 655-690.

Chin, W. W., Marcolin, B. L., and Newsted, P. R. 2003. "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study," *Information Systems Research* (14:2), pp. 189-217.

Chitturi, R., Raghunathan, R., and Mahajan, V. 2007. "Form Versus Function: How the Intensities of Specific Emotions Evoked in Functional Versus Hedonic Trade-Offs Mediate Product Preferences," *Journal of Marketing Research* (44:4), pp. 702-714.

Chitturi, R., Raghunathan, R., and Mahajan, V. 2008. "Delight by Design: The Role of Hedonic Versus Utilitarian Benefits," *Journal of Marketing* (72:3), pp. 48-63.

Clarke, R. 1999. "Internet Privacy Concerns Confirm the Case for Intervention," *Communications of the ACM* (42:2), pp. 60-67.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*, (2 ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Cohen, J., Cohen, P., West, S. G., and Aiken, L. S. 2003. *Applied Multiple Regression/Correlation Analyses for the Behavioral Sciences*, (3 ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Cohen, P., Brook, J. S., Cohen, J., Velez, C. N., and Garcia, M. 1990. "Common and Uncommon Pathways to Adolescent Psychopathology and Problem Behavior," in *Straight and Devious Pathways from Childhood to Adulthood.,* L.N. Robins and M. Rutter (eds.). New York, NY: Cambridge University Press, pp. 242-258.

comScore. 2016. "The 2016 U.S. Mobile App Report."

Creyer, E. H., and Ross, W. T., Jr. 1997. "Tradeoffs between Price and Quality: How a Value Index Affects Preference Formation," *Journal of Consumer Affairs* (31:2), pp. 280-302.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

Darrat, A. A., Darrat, M. A., and Amyx, D. 2016. "How Impulse Buying Influences Compulsive Buying: The Central Role of Consumer Anxiety and Escapism," *Journal of Retailing and Consumer Services* (31), pp. 103-108.

Davies, S. G. 1997. "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in *Technology and Privacy,* E.A. Philip and R. Marc (eds.). Cambridge, MA: MIT Press, pp. 143-165.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319-340.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp. 982-1003.

Davis, G. B., and Olson, M. H. 1985. *Management Information Systems: Conceptual Foundations, Structure, and Development*, (2 ed.). New York, NY: McGraw-Hill.

Davison, A. C., and Hinkley, D. V. 1997. *Bootstrap Methods and Their Application*. Cambridge, UK: Cambridge University Press.

de Kerviler, G., Demoulin, N. T. M., and Zidda, P. 2016. "Adoption of in-Store Mobile Payment: Are Perceived Risk and Convenience the Only Drivers?," *Journal of Retailing and Consumer Services* (31), pp. 334-344.

Deterding, S., Dixon, D., Khaled, R., and Nacke, L. 2011. "From Game Design Elements to Gamefulness: Defining "Gamification"," *15th International Academic MindTrek Conference: Envisioning Future Media Environments*, Tampere, Finland, pp. 9-15.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. "Privacy Calculus Model in E-Commerce - a Study of Italy and the United States," *European Journal of Information Systems* (15:4), pp. 389-402.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Research Commentary—Informing Privacy Research through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box," *Information Systems Research* (26:4), pp. 639-655.

Dziuban, C. D., and Shirkey, E. C. 1974. "When Is a Correlation Matrix Appropriate for Factor Analysis? Some Decision Rules," *Psychological Bulletin* (81:6), pp. 358-361.

Egelman, S., Felt, A. P., and Wagner, D. 2013. "Choice Architecture and Smartphone Privacy: There's a Price for That," in *The Economics of Information Security and Privacy*. Springer, pp. 211-236.

European Commission. 2012. "Data Protection Reform: Frequently Asked Questions." Retrieved 16.12.2017, from http://europa.eu/rapid/press-release_MEMO-12-41_de.htm

Facebook. 2015. "Permissions Reference - Facebook Login." Retrieved 26/11/2015, from https://developers.facebook.com/docs/facebook-login/permissions/v2.5 - reference-public_profile

Falk, R. F., and Miller, N. B. 1992. *A Primer for Soft Modeling*. Ohio: The University of Akron Press.

Ferdinand, J.-P., and Jetzke, T. 2017. "Voice Computing - Allgegenwärtige Spracherkennung." Retrieved 16.11.2017, from http://www.tab-beim-bundestag.de/de/pdf/publikationen/themenprofile/Themenkurzprofil-015.pdf

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., and Toval, A. 2013. "Security and Privacy in Electronic Health Records: A Systematic Literature Review," *Journal of Biomedical Informatics* (46:3), pp. 541-562.

Ferstl, O. K., and Sinz, E. J. 2015. *Grundlagen Der Wirtschaftsinformatik*. Munich: Oldenbourg Wissenschaftsverlag.

Finch, J. 1987. "The Vignette Technique in Survey Research," *Sociology* (21:1), pp. 105-114.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention, and Behavior : An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Florack, A., Ineichen, S., and Bieri, R. 2009. "The Impact of Regulatory Focus on the Effects of Two-Sided Advertising," *Social Cognition* (27:1), pp. 37-56.

Florack, A., Keller, J., and Palcu, J. 2013. "Regulatory Focus in Economic Contexts," *Journal of Economic Psychology* (38:0), pp. 127-137.

Florack, A., Scarabis, M., and Gosejohann, S. 2005. "Regulatory Focus and Consumer Information Processing," in *Applying Social Cognition to Consumer-Focused Strategy,* F.R. Kardes, P.M. Herr and J. Nantel (eds.). Mahwah, NJ: Lawrence Erlbaum Associates.

Floridi, L. 2005. "Is Semantic Information Meaningful Data?," *Philosophy and Phenomenological Research* (70:2), pp. 351-370.

Floridi, L. 2015. "Stanford Encyclopedia of Philosophy: Semantic Conceptions of Information." Retrieved 12.10.2017, 2017, from https://plato.stanford.edu/entries/information-semantic/

Fornell, C., and Bookstein, F. L. 1982. "Two Structural Equation Models: Lisrel and Pls Applied to Consumer Exit-Voice Theory," *Journal of Marketing Research* (19:4), pp. 440-452.

Fornell, C., and Larcker, D. F. 1981. "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics," *Journal of Marketing Research* (18:3), pp. 382-388.

Foroohar, R. 2017. "Privacy Is a Competitive Advantage." Retrieved 03.01.2018, from https://www.ft.com/content/0247b8f2-b012-11e7-beba-5521c713abf4

Fortes, N., and Rita, P. 2016. "Privacy Concerns and Online Purchasing Behaviour: Towards an Integrated Model," *European Research on Management and Business Economics* (22:3), pp. 167-176.

Garfinkel, R., Gopal, R., and Goes, P. 2002. "Privacy Protection of Binary Confidential Data against Deterministic, Stochastic, and Insider Threat," *Management Science* (48:6), pp. 749-764.

Gefen, D., Straub, D., and Boudreau, M. C. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the Association for Information Systems* (4:1), pp. 1-79.

Geisser, S. 1975. "The Predictive Sample Reuse Method with Applications," *Journal of the American Statistical Association* (70:350), pp. 320-328.

Gerlach, J., Widjaja, T., and Buxmann, P. 2015. "Handle with Care: How Online Social Network Providers' Privacy Policies Impact Users' Information Sharing Behavior," *Journal of Strategic Information Systems* (24:1), pp. 33-43.

GfK. 2013. "Wearable Tech: The Price Isn't Right."

González-Vallejo, C., and Moran, E. 2001. "The Evaluability Hypothesis Revisited: Joint and Separate Evaluation Preference Reversal as a Function of Attribute Importance," *Organizational Behavior and Human Decision Processes* (86:2), pp. 216-233.

Gorsuch, R. L. 1983. *Factor Analysis*, (2 ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Grimaldi, P., Lau, H., and Basso, M. A. 2015. "There Are Things That We Know That We Know, and There Are Things That We Do Not Know We Do Not Know: Confidence in Decision-Making," *Neuroscience & Biobehavioral Reviews* (55), pp. 88-97.

Gross, R., and Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks," in: *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. Alexandria, VA: pp. 71-80.

Grover, V., and Lyytinen, K. 2015. "New State of Play in Information Systems Research: The Push to the Edges," *MIS Quarterly* (39:2), pp. 271-A275.

Gulliksen, H. 1968. "Methods for Determining Equivalence of Measures," *Psychological Bulletin* (70:6p1), pp. 534-544.

Hair, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2014. *A Primer on Partial Least Squares Structural Equation Modeling*. Los Angeles, CA: Sage Publications Inc.

Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. "PLS-SEM: Indeed a Silver Bullet," *Journal of Marketing Theory and Practice* (19:2), pp. 139-152.

Hair, J. F., Sarstedt, M., Ringle, C., and Gudergan, S. P. 2017. *Advanced Issues in Partial Least Squares Structural Equation Modeling*. Thousand Oaks, CA: SAGE Publications.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., and Png, I. P. L. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13-42.

Haws, K. L., Dholakia, U. M., and Bearden, W. O. 2010. "An Assessment of Chronic Regulatory Focus Measures," *Journal of Marketing Research* (47:5), pp. 967-982.

Hempel, C. G. 1952. *Fundamentals of Concept Formation in Empirical Science*. Chicago, IL: The University of Chicago Press.

Heng, X., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798-824.

Henseler, J. 2012. "PLS-MGA: A Non-Parametric Approach to Partial Least Squares-Based Multi-Group Analysis," in *Challenges at the Interface of Data Analysis, Computer Science, and Optimization.,* W.A. Gaul, A. Geyer-Schulz, L. Schmidt-Thieme and J. Kunze (eds.). Berlin, Heidelberg: Springer, pp. 495-501.

Henson, R. K., and Roberts, J. K. 2006. "Use of Exploratory Factor Analysis in Published Research: Common Errors and Some Comment on Improved Practice," *Educational and Psychological Measurement* (66:3), pp. 393-416.

Herzenstein, M., Posavac, S. S., and Brakus, J. J. 2007. "Adoption of New and Really New Products: The Effects of Self-Regulation Systems and Risk Salience," *Journal of Marketing Research* (44:2), pp. 251-260.

Higgins, E. T. 1997. "Beyond Pleasure and Pain," *American Psychologist* (52:12), pp. 1280-1300.

Higgins, E. T. 1998. "Promotion and Prevention: Regulatory Focus as a Motivational Principle," in *Advances in Experimental Social Psychology,* J.M. Olson and M.P. Zanna (eds.). Cambridge, MA: Academic Press, pp. 1-46.

Higgins, E. T. 2000. "Making a Good Decision: Value from Fit," *American Psychologist* (55:11), pp. 1217-1230.

Higgins, E. T., Roney, C. J. R., Crowe, E., and Hymes, C. 1994. "Ideal Versus Ought Predilections for Approach and Avoidance Distinct Self-Regulatory Systems," *Journal of Personality and Social Psychology* (66:2), pp. 276-286.

Higgins, E. T., Shah, J., and Friedman, R. 1997. "Emotional Responses to Goal Attainment: Strength of Regulatory Focus as Moderator," *Journal of Personality and Social Psychology* (72:3), pp. 515-525.

Higgins, E. T., and Silberman, I. 1998. "Development of Regulatory Focus: Promotion and Prevention as Ways of Living," in *Motivation and Self-Regulation across the Life Span.,* J. Heckhausen and C.S. Dweck (eds.). New York, NY: Cambridge University Press, pp. 78-113.

Hirschman, E. C., and Holbrook, M. B. 1982. "Hedonic Consumption: Emerging Concepts, Methods and Propositions," *Journal of Marketing* (46:3), pp. 92-101.

Hoffman, D. 2014. "Privacy Is a Business Opportunity." Retrieved 03.01.2018, 2018, from https://hbr.org/2014/04/privacy-is-a-business-opportunity

Hoyle, R. H. 1999. *Statistical Strategies for Small Sample Research*. Thousand Oaks, CA: Sage Publications.

Hsee, C. K. 1996a. "Elastic Justification: How Unjustifiable Factors Influence Judgments," *Organizational Behavior & Human Decision Processes* (66:1), pp. 122-129.

Hsee, C. K. 1996b. "The Evaluability Hypothesis: An Explanation for Preference Reversals between Joint and Separate Evaluations of Alternatives," *Organizational Behavior and Human Decision Processes* (67:3), pp. 247-257.

Hsee, C. K. 1998. "Less Is Better: When Low-Value Options Are Valued More Highly Than High-Value Options," *Journal of Behavioral Decision Making* (11:2), pp. 107-121.

Hsee, C. K. 2000. "Attribute Evaluability: Its Implications for Joint-Separate Evaluation Reversals and Beyond," in *Choices, Values, and Frames,* D. Kahneman and A. Tversky (eds.). Cambridge, MA: Cambridge University Press, pp. 543-563.

Hsee, C. K., Loewenstein, G. F., Blount, S., and Bazerman, M. H. 1999. "Preference Reversals between Joint and Separate Evaluations of Options: A Review and Theoretical Analysis," *Psychological Bulletin* (125:5), pp. 576-590.

Hsee, C. K., and Zhang, J. 2010. "General Evaluability Theory," *Perspectives on Psychological Science* (5:4), pp. 343-355.

Hu, L. t., and Bentler, P. M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1-55.

Huang, L.-T., Farn, C.-K., and Yin, K.-L. 2005. "On Initial Trust Building for Ecommerce: Revisiting from the Perspective of Signal Theory and Trust Transference," in: *Proceedings of the European Conference on Information Systems*. Regensburg, Germany.

Huotari, K., and Hamari, J. 2012. "Defining Gamification: A Service Marketing Perspective," *16th International Academic MindTrek Conference*, Tampere, Finland, pp. 17-22.

Idson, L. C., Liberman, N., and Higgins, E. T. 2000. "Distinguishing Gains from Nonlosses and Losses from Nongains: A Regulatory Focus Perspective on Hedonic Intensity," *Journal of Experimental Social Psychology* (36:3), pp. 252-274.

Ja-Chul, G., Liu, F., Yung Ho, S., and Sang-Chul, L. 2010. "Comparing Utilitarian and Hedonic Usefulness to User Intention in Multipurpose Information Systems," *CyberPsychology, Behavior & Social Networking* (13:3), pp. 287-297.

John, L. K., Acquisti, A., and Loewenstein, G. 2011. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research* (37:5), pp. 858-873.

Johnson, J. A. 2005. "Ascertaining the Validity of Individual Protocols from Web-Based Personality Inventories," *Journal of Research in Personality* (39:1), pp. 103-129.

Jöreskog, K. G. 1969. "A General Approach to Confirmatory Maximum Likelihood Factor Analysis," *Psychometrika* (34:2), pp. 183-202.

Kahneman, D. 2003. "Maps of Bounded Rationality: Psychology for Behavioral Economics," *The American Economic Review* (93:5), pp. 1449-1475.

Kaiser, H. F. 1960. "The Application of Electronic Computers to Factor Analysis," *Educational and Psychological Measurement* (20:1), pp. 141-151.

Kaiser, H. F. 1970. "A Second Generation Little Jiffy," *Psychometrika* (35:4), pp. 401-415.

Kane, G. C., Alavi, M., Labianca, G., and Borgatti, S. P. 2014. "What's Different About Social Media Networks? A Framework and Research Agenda," *MIS Quarterly* (38:1), pp. 275-304.

Kannan, K. S., Manoj, K., and Arumugam, S. 2015. "Labeling Methods for Identifying Outliers," *International Journal of Statistics and Systems* (10:2), pp. 231-238.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607-635.

Kehr, F., Wentzel, D., and Mayer, P. 2013. "Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect," *Proceedings of the International Conference on Information Systems*, Milan, Italy.

Keith, M. J., Babb Jr, J. S., Furner, C. P., and Abdullat, A. 2010. "Privacy Assurance and Network Effects in the Adoption of Location-Based Services: An iPhone Experiment," *Proceedings of the International Conference on Information Systems*, St. Louis, MO.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior," *International Journal of Human-Computer Studies* (71:12), pp. 1163-1173.

Keith, M. J., Thompson, S. C., Hale, J. E., and Greer, C. 2012. "Examining the Rationality of Information Disclosure through Mobile Devices," *Proceedings of the International Conference on Information Systems*, Orlando, FL.

Kelley, H. H. 1973. "The Processes of Causal Attribution," *American Psychologist* (28:2), pp. 107-128.

Kelley, P. G., Cranor, L. F., and Sadeh, N. 2013. "Privacy as Part of the App Decision-Making Process," in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Paris, France: pp. 3393-3402.

Kenny, D. A., Kaniskan, B., and McCoach, D. B. 2014. "The Performance of RMSEA in Models with Small Degrees of Freedom," *Sociological Methods & Research* (44:3), pp. 1-22.

Kesharwani, A., and Bisht, S. S. 2012. "The Impact of Trust and Perceived Risk on Internet Banking Adoption in Indiaan Extension of Technology Acceptance Model," *International Journal of Bank Marketing* (30:4), pp. 303-322.

Khan, U., Dhar, R., and Wertenbroch, K. 2005. "A Behavioral Decision Theory Perspective on Hedonic and Utilitarian Choice," in *Inside Consumption: Frontiers of Research on Consumer Motives, Goals, and Desires,* S. Ratneshwar and D.G. Mick (eds.). London: Routledge, pp. 144-165.

Kidd, R. F. 1976. "Manipulation Checks: Advantage or Disadvantage?," *Representative Research in Social Psychology* (7:2), pp. 160-165.

Kirk, R. E. 2003. "Experimental Design," in *Handbook of Psychology,* I.B. Weiner (ed.). Hoboken, NJ: John Wiley & Sons, Inc.

Komiak, S. Y. X., and Benbasat, I. 2006. "The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents," *MIS Quarterly* (30:4), pp. 941-960.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.

Krasnova, H., Veltri, N. F., and Gunther, O. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus," *Business & Information Systems Engineering* (54:3), pp. 123-132.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22-42.

Lee, A. Y., and Aaker, J. L. 2004. "Bringing the Frame into Focus: The Influence of Regulatory Fit on Processing Fluency and Persuasion," *Journal of Personality and Social Psychology* (86:2), pp. 205-218.

Lee, M.-C. 2009. "Predicting and Explaining the Adoption of Online Trading: An Empirical Study in Taiwan," *Decision Support Systems* (47:2), pp. 133-142.

Li, H., Gupta, A., Zhang, J., and Sarathy, R. 2014. "Examining the Decision to Use Standalone Personal Health Record Systems as a Trust-Enabled Fair Social Contract," *Decision Support Systems* (57), pp. 376-386.

Li, H., Sarathy, R., and Xu, H. 2010. "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems* (51:1), pp. 62-71.

Li, H., Sarathy, R., and Xu, H. 2011. "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems* (51:3), pp. 434-445.

Li, H., Sarathy, R., and Zhang, J. 2008. "The Role of Emotions in Shaping Consumers' Privacy Beliefs About Unfamiliar Online Vendors," *Journal of Information Privacy and Security* (4:3), pp. 36-62.

Li, H., Wu, J., Gao, Y., and Shi, Y. 2016. "Examining Individuals' Adoption of Healthcare Wearable Devices: An Empirical Study from Privacy Calculus Perspective," *International Journal of Medical Informatics* (88), pp. 8-17.

Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Support Systems* (54:1), pp. 471-481.

Liberman, N., Molden, D. C., Idson, L. C., and Higgins, E. T. 2001. "Promotion and Prevention Focus on Alternative Hypotheses: Implications for Attributional Functions," *Journal of Personality and Social Psychology* (80:1), pp. 5-18.

Lichtenstein, D. R., and Burton, S. 1988. "The Measurement and Moderating Role of Confidence in Attributions," *Advances in Consumer Research* (15:1), pp. 468-475.

Lycett, M. 2013. "'Datafication': Making Sense of (Big) Data in a Complex World." Heidelberg, Berlin: Springer.

Lyytinen, K., and Yoo, Y. 2002. "Ubiquitous Computing," *Communications of the ACM* (45:12), pp. 63-96.

MacCallum, R. C., Browne, M. W., and Sugawara, H. M. 1996. "Power Analysis and Determination of Sample Size for Covariance Structure Modeling," *Psychological Methods* (1:2), pp. 130-149.

MacKenzie, S. B., and Podsakoff, P. M. 2012. "Common Method Bias in Marketing: Causes, Mechanisms, and Procedural Remedies," *Journal of Retailing* (88:4), pp. 542-555.

Madden, G. J. 2000. "A Behavioral Economics Primer," in *Reframing Health Behavior Change with Behavioral Economics,* W.K. Bickel and R.E. Vuchinich (eds.). Mahwah, NJ: Larwrence Erlbaum Associates.

Malheiros, M., Brostoff, S., Jennett, C., and Sasse, M. A. 2013. "Would You Sell Your Mother's Data? Personal Data Disclosure in a Simulated Credit Card Application," in *The Economics of Information Security and Privacy,* R. Böhme (ed.). Berlin, Heidelberg: Springer, pp. 237-261.

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

Margaryan, A., Littlejohn, A., and Vojt, G. 2011. "Are Digital Natives a Myth or Reality? University Students' Use of Digital Technologies," *Computers & Education* (56:2), pp. 429-440.

Margulis, S. T. 1977. "Conceptions of Privacy: Current Status and Next Steps," *Journal of Social Issues* (33:3), pp. 5-21.

Meade, A. W., and Craig, S. B. 2012. "Identifying Careless Responses in Survey Data," *Psychological Methods* (17:3), p. 437.

Meyniel, F., Sigman, M., and Mainen, Zachary F. 2015. "Confidence as Bayesian Probability: From Neural Origins to Behavior," *Neuron* (88:1), pp. 78-92.

Milkman, K. L., Rogers, T., and Bazerman, M. H. 2008. "Harnessing Our Inner Angels and Demons: What We Have Learned About Want/Should Conflicts and How That Knowledge Can Help Us Reduce Short-Sighted Decision Making," *Perspectives on Psychological Science* (3:4), pp. 324-338.

Milkman, K. L., Rogers, T., and Bazerman, M. H. 2009. "Highbrow Films Gather Dust: Time-Inconsistent Preferences and Online Dvd Rentals," *Management Science* (55:6), pp. 1047-1059.

Milkman, K. L., Rogers, T., and Bazerman, M. H. 2010. "I'll Have the Ice Cream Soon and the Vegetables Later: A Study of Online Grocery Purchases and Order Lead Time," *Marketing Letters* (21:1), pp. 17-35.

Miller, J., and Doyle, B. A. 1987. "Measuring the Effectiveness of Computer-Based Information Systems in the Financial Services Sector," *MIS Quarterly* (11:1), pp. 107-117.

Min, J., and Kim, B. 2015. "How Are People Enticed to Disclose Personal Information Despite Privacy Concerns in Social Network Sites? The Calculus between Benefit and Cost," *Journal of the Association for Information Science & Technology* (66:4), pp. 839-857.

Mizerski, R. W., Golden, L. L., and Kernan, J. B. 1979. "The Attribution Process in Consumer Decision Making," *Journal of Consumer Research* (6:2), pp. 123-140.

Montoya-Weiss, M. M., Voss, G. B., and Grewal, D. 2003. "Determinants of Online Channel Use and Overall Satisfaction with a Relational, Multichannel Service Provider," *Journal of the Academy of Marketing Science* (31:4), pp. 448-458.

Morosan, C., and DeFranco, A. 2015. "Disclosing Personal Information Via Hotel Apps: A Privacy Calculus Perspective," *International Journal of Hospitality Management* (47), pp. 120-130.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100-126.

Nunnally, J. C. 1978. *Psychometric Theory*. New York: McGraw-Hill.

O'Connor, K. M., De Dreu, C. K. W., Schroth, H., Barry, B., Lituchy, T. R., and Bazerman, M. H. 2002. "What We Want to Do Versus What We Think We Should Do: An Empirical Investigation of Intrapersonal Conflict," *Journal of Behavioral Decision Making* (15:5), pp. 403-418.

Okada, E. M. 2005. "Justification Effects on Consumer Choice of Hedonic and Utilitarian Goods," *Journal of Marketing Research* (42:1), pp. 43-53.

Olmstead, K., and Atkinson, M. 2010. "Apps Permissions in the Google Play Store," Pew Research Center.

Oster, S. M., and Scott Morton, F. M. 2005. "Behavioral Biases Meet the Market: The Case of Magazine Subscription Prices," *B.E. Journal of Economic Analysis and Policy* (5:1), pp. 1-30.

Overall, J. E., Spiegel, D. K., and Cohen, J. 1975. "Equivalence of Orthogonal and Nonorthogonal Analysis of Variance," *Psychological Bulletin* (82:2), pp. 182-186.

Pan, Y., and Zinkhan, G. M. 2006. "Exploring the Impact of Online Privacy Disclosures on Consumer Trust," *Journal of Retailing* (82:4), pp. 331-338.

Pavlou, P. A., and Fygenson, M. 2006. "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly* (30:1), pp. 115-143.

Perdue, B. C., and Summers, J. O. 1986. "Checking the Success of Manipulations in Marketing Experiments," *Journal of Marketing Research* (23:4), pp. 317-326.

Perez, S. 2017. "App Annie: Android to Top Ios in App Store Revenue This Year," TechCrunch.

Pham, M. T., and Avnet, T. 2004. "Ideals and Oughts and the Reliance on Affect Versus Substance in Persuasion," *Journal of Consumer Research* (30:4), pp. 503-518.

Pham, M. T., and Avnet, T. 2009. "Contingent Reliance on the Affect Heuristic as a Function of Regulatory Focus," *Organizational Behavior & Human Decision Processes* (108:2), pp. 267-278.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing* (19:1), pp. 27-41.

Podsakoff, P. M., MacKenzie, S. B., Jeong-Yeon, L., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

Ringle, C. M., Wende, S., and Becker, J.-M. 2015. *SmartPLS 3*. Bönningstedt: SmartPLS.

Roese, N. J., and Sherman, J. W. 2007. "Expectancy," in *Social Psychology: Handbook of Basic Principles,* A.W. Kruglanski and E.T. Higgins (eds.). New York, London: The Guildford Press, pp. 91-115.

Rönkkö, M., and Ylitalo, J. 2011. "PLS Marker Variable Approach to Diagnosing and Controlling for Method Variance," in: *Proceedings of the International Conference on Information Systems*. Shanghai, China.

Rosendaal, A. 2010. "Facebook Tracks and Traces Everyone: Like This!," in: *Tilburg Law School Legal Studies Research Paper Series*. Delft: Tilburg Law School.

Rossi, P. H., and Nock, S. L. 1982. *Measuring Social Judgments: The Factorial Survey Approach*. New York: Sage Publications.

Rule, J. B. 1974. *Private Lives and Public Surveillance*. New York: Schocken Books.

Sacchi, S., and Stanca, L. 2014. "Asymmetric Perception of Gains Versus Non-Losses and Losses Versus Non-Gains: The Causal Role of Regulatory Focus," *Journal of Behavioral Decision Making* (27:1), pp. 48-56.

Sarathy, R., and Li, H. 2007. "Understanding Online Information Disclosure as a Privacy Calculus Adjusted by Exchange Fairness," in: *Proceedings of the Internation Conference on Information Systems*. Montreal, Canada.

Schelling, T. C. 1985. *Choice and Consequences: Perspectives of an Errant Economist*. Cambridge, MA: Harvard University Press.

Schoeman, F. D. 1984. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge, UK: Cambridge University Press.

Schwarze, J. 2000. *Einführung in Die Wirtschaftsinformatik*. Berlin: NWB Verlag.

Seibt, B., and Förster, J. 2004. "Stereotype Threat and Performance: How Self-Stereotypes Influence Processing by Inducing Regulatory Foci," *Journal of Personality and Social Psychology* (87:1), pp. 38-56.

Sharma, S., and Crossler, R. E. 2014. "Disclosing Too Much? Situational Factors Affecting Information Disclosure in Social Commerce Environment," *Electronic Commerce Research & Applications* (13:5), pp. 305-319.

Sharma, S., Durand, R. M., and Gur-Arie, O. 1981. "Identification and Analysis of Moderator Variables," *Journal of Marketing Research* (18:3), pp. 291-300.

Sheng, H., Nah, F. F.-H., and Siau, K. 2008. "An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns," *Journal of the Association for Information Systems* (9:6), pp. 344-376.

Shibchurn, J., and Yan, X. 2015. "Information Disclosure on Social Networking Sites: An Intrinsic–Extrinsic Motivation Perspective," *Computers in Human Behavior* (44), pp. 103-117.

Simon, H. A. 1955. "A Behavioral Model of Rational Choice," *The Quarterly Journal of Economics* (69:1), pp. 99-118.

Sledgianowski, D., and Kulviwat, S. 2009. "Using Social Network Sites: The Effects of Playfulness, Critical Mass and Trust in a Hedonic Context," *Journal of Computer Information Systems* (49:4), pp. 74-83.

Slovic, P., Fischhoff, B., and Lichtenstein, S. 2000. "Rating the Risks," in *The Perception of Risk*. New York, NY: Earthscan, pp. 104-120.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1016.

Solomon, M. R., Bamossy, G. J., Askegaard, S. T. A., and Hogg, M. K. 2006. *Consumer Behaviour: A European Perspective*. Upper Saddle River, NJ: Prentice Hall.

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

Statista. 2017a. "Number of Smartphones Sold to End Users Worldwide from 2007 to 2016 (in Million Units)." Retrieved 29.12.2017, from https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/

Statista. 2017b. "Smart Appliances Segment Outlook Report." Retrieved 29.12.2017, from https://www.statista.com/outlook/389/100/smart-appliances/worldwide

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

Stone, E. F., Gueutal, H. G., Gardner, D. G., and McClure, S. 1983. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations," *Journal of Applied Psychology* (68:3), pp. 459-468.

Stone, M. 1974. "Cross-Validatory Choice and Assessment of Statistical Predictions," *Journal of the Royal Statistical Society* (36:2), pp. 111-147.

Strahilevitz, M., and Myers, J. G. 1998. "Donations to Charity as Purchase Incentives: How Well They Work May Depend on What You Are Trying to Sell," *Journal of Consumer Research* (24:4), pp. 434-446.

Straub, D. W. 1989. "Validating Instruments in MIS Research," *MIS Quarterly* (13:2), pp. 147-169.

Tam, E.-C., Hui, K.-L., and Tan, B. 2002. "What Do They Want? Motivating Consumers to Disclose Personal Information to Internet Businesses," *Proceedings of the International Conference on Information Systems*, Barcelona, Spain.

Taylor, B. J. 2006. "Factorial Surveys: Using Vignettes to Study Professional Judgement," *British Journal of Social Work* (36:7), pp. 1187-1207.

Thaler, R. H., and Shefrin, H. M. 1981. "An Economic Theory of Self-Control," *Journal of Political Economy* (89:2), pp. 392-406.

Trudel, R., Murray, K. B., and Cotte, J. 2012. "Beyond Expectations: The Effect of Regulatory Focus on Consumer Satisfaction," *International Journal of Research in Marketing* (29:1), pp. 93-97.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254-268.

Turk, V. 2016. "Home Invasion," *New Scientist* (232:3104), pp. 16-17.

Venkatesh, V., and Davis, F. D. 2000. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science* (46:2), pp. 186-204.

Venkatesh, V., Thong, J. Y. L., and Xin, X. 2012. "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MIS Quarterly* (36:1), pp. 157-178.

Vilares, M. J., Almeida, M. H., and Coelho, P. S. 2010. "Comparison of Likelihood and Pls Estimators for Structural Equation Modeling: A Simulation with Customer Satisfaction Data," in *Handbook of Partial Least Squares: Concepts, Methods and Applications,* V.E. Vinzi, W.W. Chin, J. Henseler and H. Wang (eds.). Berlin: Springer Science & Business Media, pp. 289-305.

Voss, K. E., Spangenberg, E. R., and Grohmann, B. 2003. "Measuring the Hedonic and Utilitarian Dimensions of Consumer Attitude," *Journal of Marketing Research* (40:3), pp. 310-320.

Wakefield, R. 2013. "The Influence of User Affect in Online Information Disclosure," *Journal of Strategic Information Systems* (22:2), pp. 157-174.

Wang, J., and Lee, A. Y. 2006. "The Role of Regulatory Focus in Preference Construction," *Journal of Marketing Research* (43:1), pp. 28-38.

Wang, T., Duong, T. D., and Chen, C. C. 2016. "Intention to Disclose Personal Information Via Mobile Applications: A Privacy Calculus Perspective," *International Journal of Information Management* (36:4), pp. 531-542.

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

Williams, L. J., Hartman, N., and Cavazotte, F. 2010. "Method Variance and Marker Variables: A Review and Comprehensive CFA Marker Technique," *Organizational Research Methods* (13:3), pp. 477-514.

Woerner, S. L., and Wixom, B. H. 2015. "Big Data: Extending the Business Strategy Toolbox," *Journal of Information Technology* (30:1), pp. 60-62.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," *Proceedings of the International Conference on Information Systems*, Paris, France.

Xu, H., and Gupta, S. 2009. "The Effects of Privacy Concerns and Personal Innovativeness on Potential and Experienced Customers' Adoption of Location-Based Services," *Electronic Markets* (19:2), pp. 137-149.

Xu, H., Luo, X., Carroll, J. M., and Rosson, M. B. 2011. "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing," *Decision Support Systems* (51:1), pp. 42-52.

Xu, H., and Teo, H.-H. 2004. "Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective," *Proceedings of the International Conference on Information Systems*, Washington, DC.

Xu, H., Teo, H.-H., and Tan, B. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk," *Proceedings of the International Conference on Information Systems*, Las Vegas, NV.

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-173.

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2012. "Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," *Information Systems Research* (23:4), pp. 1342-1363.

Yeung, N., and Summerfield, C. 2014. "Shared Mechanisms for Confidence Judgements and Error Detection in Human Decision Making," in *The Cognitive Neuroscience of Metacognition*. Berlin, Heidelberg: Springer, pp. 147-167.

Yoon, Y., Sarial-Abi, G., and Gürhan-Canli, Z. 2012. "Effect of Regulatory Focus on Selective Information Processing," *Journal of Consumer Research* (39:1), pp. 93-110.

Yuan, L. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the Association for Information Systems* (28), pp. 453-496.

Zhou, R., and Tuan Pham, M. 2004. "Promotion and Prevention across Mental Accounts: When Financial Products Dictate Consumers' Investment Goals," *Journal of Consumer Research* (31:1), pp. 125-135.

Zhou, T. 2011. "The Impact of Privacy Concern on User Adoption of Location‐Based Services," *Industrial Management & Data Systems* (111:2), pp. 212-226.

Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., and Grover, V. 2010a. "Knowing Your Customers: Using a Reciprocal Relationship to Enhance Voluntary Information Disclosure," *Decision Support Systems* (48:2), pp. 395-406.

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., and Grover, V. 2010b. "Investigating Online Information Disclosure: Effects of Information Relevance, Trust and Risk," *Information & Management* (47:2), pp. 115-123.

Appendix

Utilitarian Benefit (low)	*Utilitarian Benefit (high)*
The wristband has several sensors like GPS, accelerometer and position-, pulse- and blood oxygen-sensors. In combination with a free smartphone app is it possible, to track the exertion levels during different sports activities. On leaving a certain preset pulse range, the wearer is notified by a vibration alarm und receives a notification via the linked smartphone.	The wristband has several sensors like GPS, accelerometer and position-, pulse- and blood oxygen-sensors. In combination with a free smartphone app is it possible, to track diverse sports activities. If an exercise is done technically wrong or with the wrong intensity, the wearer is notified by a vibration alarm und receives tips to improve his training via the linked smartphone. In everyday life, the wristband can be used to count steps or even monitor sleeping cycles and being woken up at the optimal time. Modern wireless technologies enable the wristband to be used as digital admission ticket.
Hedonic Benefit (low)	*Hedonic Benefit (high)*
[no further features]	The wearer of the wristband can collect points through certain behaviors. For example, exercising with a constant pulse or a high number of steps per day are rewarded with a digital badge. The smartphone-app allows access to the badges already gained and more available badges. At regular intervals, the wearer is confronted with special tasks to achieve special badges, for example gain 25 meters in altitude in the next ten minutes.
Risk (low)	*Risk (high)*
All data recorded by the wristband are transferred to the provider's servers and stored in encrypted form. The data will not be disclosed to third parties.	All data recorded by the wristband are transferred to the provider's server and stored there. The provider reserves the right to analyze the data and provide third parties access to anonymized data.

Appendix 1: Scenarios used to manipulate the independent variables (Paper A).

Hedonic Attitude towards the Product - (Voss et al. 2003) 7-pt semantic differential	**Utilitarian Attitude towards the Product** - (Voss et al. 2003) 7-pt semantic differential
H1 not fun / fun	U1 not effective / effective
H2 dull / exciting	U2 not helpful / helpful
H3 not delightful / delightful	U3 not functional / functional
H4 not thrilling / thrilling	U4 not necessary / necessary
H5 unenjoyable / enjoyable	U5 not practical / practical
Behavioral Intention to Use (Sheng et al. 2008) 7-pt Likert scale (agreement)	**Behavioral Intention to Disclose Personal Information** (Xu et al. 2009) 7-pt semantic differential
When faced with this scenario, ...	ID1 Unlikely / Likely
IU1 ... I intend to adopt this product.	ID2 Not probable / Probable
IU2 ... I predict I will use this product.	ID3 Impossible / Possible
IU3 ... I plan to use this product.	ID4 Unwilling / Willing
Perceived Risk of Information Disclosure - (Xu et al. 2009) 7-pt Likert (strongly disagree / strongly agree)	
R1 Providing the provider of the wristband with my personal information would involve many unexpected problems.	
R2 It would be risky to disclose my personal information to the provider of the wristband.	
R3 There would be high potential for loss in disclosing my personal information to the provider of the wristband.	

Appendix 2: Measurement items (Paper A).

Perceived Risk of Information Disclosure (RSK) – Heng et al. (2011) – 7pt Likert *(agreement)*			
RSK1	In general, it would be risky to give personal information to this Facebook App.		
RSK2	There would be high potential for privacy loss associated with giving personal information to this Facebook App.		
RSK3	Personal information could be inappropriately used by this Facebook App.		
RSK4	Providing this Facebook App with my personal information would involve many unexpected problems.		
Perceived Benefits of Information Disclosure (Operationalized by Value of the Gift Card) – Okada (2005)			
BEN1	What is the value of the chance to win the gift card? *(1 = not at all valuable / 7 = extremely valuable)*		
BEN2	How well off are you with the chance to win the gift card? *(1 = not at - / 7 = extremely well off)*		
BEN3	How happy are you with the chance to win the gift card? *(1 = I would not care about it at all / 7 = extremely happy)*		
Situational Regulatory Focus (RF) – Pham and Avnet (2004) – I would prefer to... *(1 – 7)*			
RF1	do whatever it takes to keep my promises / go wherever my heart takes me		
RF2	do what is right / do whatever I want		
RF3	pay back my loans / take a trip around the world		
Behavioral Intention to Disclose Personal Information (INT) – Malhotra et al. (2004) Please specify the extent to which you would reveal your personal information to the Facebook App. *(1 - 7)*			
INT1	unlikely / likely	INT3	impossible / possible
INT2	not probable / probable	INT4	unwilling / willing
Chronic Prevention Focus (Control variable) – (Haws et al. 2010) – 7pt Likert *(agreement)*			
CRF1	I frequently think about how I can prevent failures in my life.		
CRF2	I worry about making mistakes.		
CRF3	I see myself as someone who is primarily striving to become the self I "ought" to be—fulfill my duties, responsibilities and obligations.		
CRF4	I usually obeyed rules and regulations that were established by my parents.		
CRF5	Not being careful enough has gotten me into trouble at times. (R)		

Appendix 3: Measurement Items (Paper B).

Path	f^2	q^2
RSK → RF	0.111	0.070
CRF → RF	0.049	0.025

Path	f^2	q^2
RSK → INT	0.307	0.243
BEN → INT	0.392	0.304

Path	f^2	q^2
BEN x RF → INT	0.122	0.095
RSK x RF → INT	0.049	0.038

Appendix 4: Effect Sizes (f2) and relative predictive relevance (q2) of each path in the model (Paper B).

Perceived Risk of Information Disclosure - (Malhotra et al. 2004) 7 pt. Likert Scale anchored with "strongly disagree" and "strongly agree"			
RSK1	In general, it would be risky to disclose my personal information to this application.		
RSK2	There would be high potential for loss associated with providing my personal information to this application.		
RSK3	There would be too much uncertainty associated with having my personal information gathered by this application.		
RSK4	Providing the provider of the application with my personal information would involve many unexpected problems.		
RSK5	I would feel safe giving my personal information to the provider of this application. *(reverse)*		
Hedonic (HED) and Utilitarian (UTL) Attitudes towards the Application - (Voss et al. 2003) 7 pt. semantic differentials			
HED1	Not fun / Fun	UTL1	Ineffective / Effective
HED2	Dull / Exciting	UTL2	Unhelpful / Helpful
HED3	Not delightful / Delightful	UTL3	Not functional / Functional
HED4	Not thrilling / Thrilling	UTL4	Unnecessary / Necessary
HED5	Unenjoyable / Enjoyable	UTL5	Impractical / Practical
Intention to use the Application - (Malhotra et al. 2004) To what extent would you download this application to give it a try? *(1 – 7)*		**Visual Appeal of App Logo - (based on Montoya-Weiss et al. 2003)** 7 pt. semantic differentials	
INT1	Unlikely / Likely	VIS1	I like the look of the logo.
INT2	Not probable / Probable	VIS2	The logo is attractive to me.
INT3	Impossible / Possible	VIS2	I like the graphics of the logo.
INT4	Unwilling / Willing		
Perceived Evaluability of Privacy Risks (self-developed) 7pt Likert Scale anchored with "strongly disagree" and "strongly agree" | While rating the privacy risks...			
EVA1	... I had sufficient information at hand.	EVA4	… I was able to decide by instinct.
EVA2	… I had a good judgment.	EVA5	… I knew exactly how I would answer.
EVA3	… it was easy for me to tick the checkboxes.		

Appendix 5: Survey Items (Paper C).

			Perceived Risk		Hedonic Att.		Utilitarian Att.		Beh. Intention	
	App	N	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Single Evaluation	A	63	3.95	1.41	2.89	1.18	4.70	1.16	4.04	1.76
	B	67	4.32	1.28	3.39	1.10	4.95	1.15	4.35	1.71
Joint Evaluation	A	103	3.27	1.35	3.12	1.14	4.90	1.14	4.71	1.40
	B	103	4.78	1.32	4.02	1.17	4.76	1.16	3.68	1.66

Appendix 6: Descriptive Statistics of Constructs in the Research Model (Paper C)