Bayreuther Arbeitspapiere zur Wirtschaftsinformatik

Christoph Buck, Simone Burster, Torsten Eymann

# Priming App Information Privacy Concerns in Mobile Ecosystems

No. 63
October 2017
ISSN 1864-9300

# Priming App Information Privacy Concerns in Mobile Ecosystems

*Working Paper*

## Introduction

With the mass adoption of personal computers, notebooks, and predominantly smart mobile devices (SMD) like smartphones and tablets the average user of information systems (IS) has dramatically changed (Yoo 2010). As early as Lamb and Kling (2003) in the beginning of this century pointed out that the traditional notion of users is not broad enough for the complex social reality of organizational computing. They highlighted the importance of contextual and environmental factors and noted that users of IS are socially embedded in networks of relationships that mobilize the exchange of information and the use of IS. The call of Lamb and King (2003) is today even more relevant because of users' integration of IS into their everyday life. This leads to fundamental changes concerning how users interact with computing devices and systems (Venkatesh et al. 2012).

Disruptive innovations like the iPhone, the iPad, and software in form of mobile applications (apps), diffused into the everyday life of users. Apps are integral to the functioning of SMD and are key elements for the interface design and functionality. Therefore, apps can be interpreted as today's archetype example of ubiquitous computing, i.e. the creation of environments saturated with computing and communication capability, integrated with human users (Weiser 1991). While ubiquitous computing focuses on hardware components, today's apps are the logical consequence of experiential computing: the "digitally mediated embodied experiences in everyday activities through everyday artefacts with embedded computing capabilities" (Yoo 2010, p.213). Apps are used to perform every kind of task and users benefit while handling their everyday routine. Everyday activities are almost 'naturally' carried out or supported by apps, or as Apple puts it in one of their slogans: "There's an app for that®" (Apple Inc. 2017) – which addresses the broad scope of applications apps are used for.

However, this excessive level of integration does not come without consequences. Individuals' use of apps poses multiple challenges for IS research, especially in the field of privacy and the exposure of personal data. Privacy as digital personal information and highly personalized data collected via apps has a huge economic value and most apps are traded for privacy because of their valuable data (Acquisti et al. 2015). However, in contrast to most economic exchanges individuals are usually not able to estimate the quality and performance characteristics of the app they download and use, as well as the amount and economic value of privacy and personal data they disclose and pay with (Buck et al. 2017; Grossklags and Acquisti 2007; Spiekermann et al. 2015b). Nevertheless, research brings to light that individuals are concerned about their privacy and that they are very sensible regarding the collection and use of their personal data (Grossklags and Acquisti, 2007).

As a result, digital markets, and app markets in particular, are characterized by highly asymmetrical information endowments of consumers and providers. Economic theory exhibits, that markets which cannot reduce uncertainty come to a standstill (Akerlof 1970; Hirshleifer 1973). In app markets the opposite is observable: to date, more than five million apps are available in and more than 181 billion apps were downloaded from the leading apps store (Statistic Brain 2016). The average consumer holds more than 30 apps on his SMD (Fox 2013), most of which were downloaded without a monetary price tag (Statista 2017). An emerging stream in IS and privacy research to investigate this perceived disequilibrium is to integrate frameworks and theories from social psychology and behavioral economics. These perspectives incorporate the user as human being as a part of the socio-technical IS for getting a better understanding of the existing inconsistencies. Following the call of Dinev et al. (2015), who claim for more research considering human beings as users of IS, we provide a behavioral economics approach on privacy, app information privacy concerns. In this paper we present six experiments to investigate the following research question:

- Which priming stimuli influence app information privacy concerns?

To answer this research question, the remainder of this article is structured as follows. In the following section information privacy and its relevance regarding apps is marked out. According to the call of (Dinev et al. (2015), effects of extraneous influences are introduced and hypotheses are provided. Furthermore, six independent online experiments in the observed field are presented. The supposed and literature driven relations between the dependent and independent variables are shortly introduced and the results of the data analysis are presented. Subsequently, the results are interpreted and the limitations are discussed. Finally, a conclusion is provided containing implications and future research.

## Privacy, Social Psychology and Behavioral Economics

### *Information Privacy as Part of an Economic Exchange*

Dinev and Hart (2006) stated that privacy "is a highly cherished value, few would argue that absolute privacy is unattainable" (Dinev and Hart 2006, p.61). Since privacy is addressed in many fields of social sciences and in various areas of everyday life, it lacks a holistic definition (Smith et al. 2011; Solove 2006). First of all, physical and information privacy have to be distinguished. Physical privacy relates to the "access of an individual and/or the individual's surroundings and private space" (Smith et al. 2011, p.990). Contrary, information privacy only refers to information that is individually identifiable or describes the private informational spheres of an individual. Although information privacy is rooted in the fundamental concept of physical privacy, both are subsumed under the term of "general privacy" (Smith et al. 2011).

In this paper information privacy is defined as the ability to control the acquisition and use of one's personal information (Stone et al. 1983; Westin 1967). The concept of autonomous and self-determined control over the disclosure of private information is closely related to information and communication technologies and therewith to SMD and apps (Dinev and Hart 2006). Within the scope of IS, such as SMD and apps, personal information is gathered by personal data. Thus, this article treats personal information and personal data as equal. We will keep the following principle throughout the remainder of this article: we will use the term privacy as a reference to information privacy, which is our immediate focus.

As the "pocket knife of communication" (Wellman 2010), SMD possess a vast number of connected sensors, devices, and functions. SMD in combination with apps are the most common user interface to merge the broad opportunities given by the connected entities. Due to these functions, the possibilities of gathering personal data are virtually endless. Future prospects in relation to these applications promise even more opportunities to expand data collection and immediate analysis of data. Regarding data quality, recent developments in mobile technology and an ever-increasing digitization of everyday tasks, lead to an unprecedented precision of continuously updated and integrated personal data, which is generated within mobile ecosystems (Buck et al. 2014). Consequently, apps layer everyday activities and lives in a digital way; or how Clarke rephrased it: "Cyberspace is invading private space" (Clarke 1999, p.60).

With the description of personal data as a new asset class, the World Economic Forum (2011) is in line with the argumentation of many researchers (Smith et al. 2011; Spiekermann et al. 2015a). Derived from the perspective of personal data and privacy as a commodity (Bennett 1995), many researchers conceive privacy as a tradeable good or asset (Spiekermann et al. 2015a). According to this view, privacy is no longer an absolute societal value, but has an economic value, which leads to the possibility of a cost-benefit trade-off calculation made by individuals or a society (Smith et al. 2011). According to the view of personal information as a tradable good, in this paper the control-oriented definition, according to Westin (Westin 1967), was chosen. In app markets, individuals are able to control their privacy disclosure during the purchasing process. Thus, individuals can actively control their disclosure of personal data and the grasping of privacy from third parties (Chen and Chen 2015), which exposes the chosen definition of privacy as appropriate for the context of mobile apps.

### *Relevant Work in Information Privacy Research*

A lot of research has been undertaken in the field of information privacy from various disciplines, in particular in the field of IS and individuals' online information privacy (Dinev et al. 2015; Li 2011). Contradicting behaviors have been discovered regarding the information disclosure of individuals and the related concerns about their information privacy. While most individuals are concerned about their information privacy and would like to protect it, they do not act in equal manner as the same individuals are willing to give away their personal information for relatively small rewards (Grossklags and Acquisti 2007). This inconsistency of privacy attitudes and privacy behavior, the so-called privacy paradox (Norberg et al. 2007), got the attention of various scholars, but there is no comprehensive explanation for it (Kokolakis 2015). An emerging approach comes from the field of social psychology and behavioral economics containing cognitive biases and heuristics (Acquisti and Grossklags 2005; Acquisti and Grossklags 2008; Brandimarte et al. 2012; Grossklags and Acquisti 2007). Drawing from all relevant findings, the behavior should not be described paradox anymore, as research also provides logical justifications and shows systematic inconsistencies, but no irrational behavior (Acquisti 2012; Acquisti et al. 2015).

Besides the phenomenon of the privacy paradox, privacy and its relation with other constructs have been investigated in various studies. Bélanger and Crossler (2011), Li (2011), and Smith et al. (2011) coincidently investigated the vast privacy literature and established three macro models. Central to all of the three macro models is the construct of privacy concerns. As monitoring of personal information is ubiquitous the concerns about information privacy are growing and it has been a major research field since the mid-1990s (Dinev et al. 2015). It is almost impossible to measure privacy itself as it depends more on cognitions and perceptions rather than on rational decision-making. Therefore, almost all empirical privacy studies in social sciences are based on a privacy-related proxy used as a measurement of information privacy (Bélanger and Crossler 2011; Smith et al. 2011; Xu et al. 2012). Although different wordings have been used like attitudes, beliefs and perceptions, the underlying measurements are generally privacy concerns which were developed to empirically measure information privacy. There is no universal definition for privacy concerns. However, in general it refers to the "degree to which an individual perceived a potential for a loss associated with personal information" (Pavlou 2011: 981).

In their work, Bélanger and Crossler (2011) developed a multilevel framework to classify information privacy concerns. They came up with the premises that privacy concern is a multilevel concept fragmented into individual, group, and organizational level. At an individual level expressed in "individual information privacy concern" is determined by individual differences, external factors also known as antecedents that refer to personality traits, age, education etc. The group level described as group information privacy concern has not yet been subject of any research except the framework and definitions which have been provided by (Skinner et al. 2006). Since groups develop their own identity and structures it is possible that groups have their own privacy concerns which can be different from the privacy concern of an individual within the group (Watson-Manheim and Belanger 2002). Organizational information privacy concerns typically arise from management policies and practices. It reflects the overall concern organizational leaders have regarding privacy of the information the organization holds and has access to. So far, there has been only limited research on the linkage between organizational privacy policies and individual information privacy concerns. Earp et al. (2005) demonstrated that there is no linkage between individual concerns for information privacy and the organizations privacy policies. The last and highest level is societal information privacy concern and it stands for the overall concerns regarding the privacy of information citizens have in a society collectively.

The focus of the model of Li (2011) is on privacy concerns, the antecedents and consequences. He conducted an extensive literature review on empirical studies that deal with online information privacy concerns. According to the literature review, multiple theories (e.g. information boundary theory, personality theory, principle-agent theory, privacy calculus theory etc.) were used to interpret the development of individuals' privacy concerns as well as to study the corresponding behavioral consequences. Grounded on those theories various antecedents were studied and regarding their level of research summarized into individual factors, social-relational factors, organizational and task environmental factors, macro-environmental factors and information contingency. To create a holistic view of all factors Li (2011) built an integrative framework for the study on online information privacy upon the theory of reasoned action (TRA) (Ajzen and Fishbein 1980). The framework is developed around two key factors: General Concern for Information Privacy (General CFIP) and Specific Concern for Information Privacy (Specific CFIP).

Smith et al. (2011) developed their macro model summarizing antecedents, privacy concerns and its outcomes (APCO) with privacy concerns as the central construct. According to the model, privacy concerns can be examined from two different perspectives: as a dependent variable, which is based on information boundary theory explaining privacy concerns by antecedents like individual privacy experience and awareness, individual differences regarding personality, demographics as well as culturally and climatically differences (Xu et al. 2008). According to those antecedents individuals' privacy concern is shaped. For example, individuals who fall victim to personal information abuse should have higher privacy concerns (Smith et al. 1996). Moreover, individuals with different cultural background have different attitudes towards information disclosure and thus have different levels of privacy concerns (Dinev et al. (2006).

Summarizing the three macro models, it can be concluded that various factors have an impact on privacy concerns at different levels. The linkages between privacy concerns, intentions and behaviors are moderated and mediated by various factors. Moreover, privacy-related behavior and intensions can be noted at several levels (Smith et al. 2011; Bélanger and Crossler 2011; Li 2011). Even though different approaches have been used to come up with the macro models in several major findings. First, antecedents influence and shape privacy concerns of individuals which result in behavioral outcomes depending on the individual's information processing. However, in which way they affect privacy concern is not well known (Smith et al. 2011; Bélanger and Crossler 2011; Li 2011).

Furthermore, Smith et al. (2011) and Li (2011) pointed out the importance of the privacy calculus, suggesting that individuals engage in privacy trade-offs between risk and benefits while engaging in decisions regarding their personal information disclosure (Stone and Stone 1990; Culnan and Armstrong 1999; Dinev and Hart 2006). According to the privacy calculus "individuals are assumed to behave in ways that they believe will result in the most favorable net level of outcomes" (Stone and Stone 1990, p.363). Therefore, users are supposed to undertake an anticipatory, rational weighing of risks and benefits when confronted with the decision to disclose personal information (Culnan and Armstrong 1999; Malhotra et al. 2004) or conduct transactions (Pavlou 2011). This ties in with the view the of neoclassical economics where rational consumers disclose personal information to marketers in exchange for certain benefits but keep other information private if they do not expect to receive benefits (Varian 1996). The privacy calculus often represents an empirical subset examined in isolation from other constructs (Smith et al. 2011).

However, attention should be drawn to the fact that generally intentions were measured and they do not necessary lead to actual behaviors. Moreover the contextual dependence is an important factor in the models (Bélanger and Crossler 2011; Smith et al. 2011; Li 2011)

### *Behavioral Economics and Information Systems*

The existing macro models disregard the fact that individuals usually do not fully reflect on their behavior regarding privacy options and thus do not exhaustively reflect the status quo of information privacy research. Smith et al. (2011) indicated that several linkages are affected by the privacy paradox but they did not provide any further explanation of it. So far, IS research, and the APCO model as the most applied macro model and a reflection of the existing information privacy literature, has supposed that privacy-related behaviors are represented by deliberate, high-effort processes (Li 2011; Bélanger and Crossler 2011; Smith et al. 2011; Dinev et al. 2015). Thus, all macro models are making the critical assumption that "responses to external stimuli result in deliberate analyses, which lead to fully informed privacy-related attitudes and behaviors" (Dinev et al. 2015, p.639). Taking the mass adoption of modern IS and the 'new user' in experiential computing into account, the current state of IS research does not incorporate enough knowledge known from social psychology and behavioral economics.

Dinev et al. (2015) proposed an enhanced APCO model, shown in figure 1, with a set of related propositions (D1-D8) deriving from the influences of extraneous factors. The propositions consider cognitive responses and low-effort responses (what the current macro models neglect) inspired by research findings from (social) psychology and behavioral economics. Although several researchers contributed valuable research to the field, (Acquisti et al. 2015; Acquisti and Grossklags 2005; Acquisti and Grossklags 2008; Brandimarte et al. 2012) most of the raised questions of Dinev et al. (2015) are not investigated yet.

There are two important implications of the enhanced APCO model for privacy research with regard to the level of effort: primarily, privacy-related decisions can occur in a range from low-effort up to high-effort processing. Secondly, attitudes that are changed and behaviors that are enacted by low-effort processing are usually weaker and shorter lived than attitudes and behaviors in high-effort processing. This is, due to the transient factors involved in low-effort processing, not necessarily related to privacy decisions (e.g. emotions, mood, time constraints etc.). However, it influences individuals' decision-making significantly (Dinev et al. 2015). Low-effort processes are characterized by relatively low cognitive effort or less conscious awareness (Dinev et al. 2015; Kahneman 2013). Thus, behavior-relevant information is evaluated using mental shortcuts based on former experienced habits and routines (Polites and Karahanna 2013). However, simple heuristics and spontaneous reactions during information processing can lead to suboptimal behaviors that are in contrary to individuals expressed believes and values (Dinev et al. 2015). It is possible to create situations in which one can take advantage of these pitfalls in decision-making and/or to nudge individuals to a more desired behavior (Acquisti 2012; Ariely 2009).

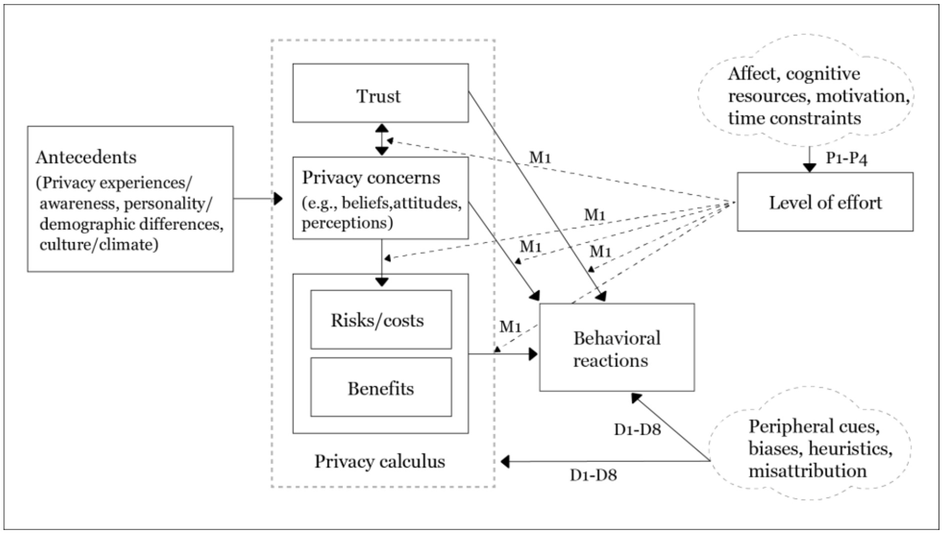


**Figure 1. Enhanced APCO-model (Dinev et al. 2015)**

From our point of view, apps as the embodiment of experiential computing, in general, can be classified as low effort processing. The app download can be classified as an impulsive and habitualized purchase (Buck et al. 2014; Weinberg 1995), which leads to a judgement under limited time and incomplete information about risks and benefits. Furthermore, apps are a fusion between fast moving consumer goods and traditional software products. Because of the highly standardized processes for the search, download, and payment of apps in the underlying mobile ecosystems and their uniform appearance in app stores we classify their purchase as low effort processes.

In combination with the high value of app data a more in-depth investigation of privacy related extraneous influences (our focus is on priming effects and misattributions) is the goal for the following series of experiments.

## Experimental Studies: Priming Privacy

### *Priming and the Experimental Approach*

In this chapter, we present a series of experiments, all conducted in the field of priming information privacy behavior. Generally, priming is described as a form of cognitive bias that influences individuals in how they perceive and process information (Kahneman 2013; Tulving et al. 1982). Furthermore, the effect includes that information is not doubted and directly classified as correct information. Priming effects do occur in situations of low cognitive effort and are defined as misattributions that can influence actions as well as emotions (Tulving et al. 1982; Dinev et al. 2015). While existing research, based on neuro science, social psychology, and behavioral economics classifies priming in different characteristics, this research has its focus on forms of indirect priming (mostly denominated as associative or conceptual priming). It is based on the meaning of a stimulus and is enhanced by a semantic field. A simple example is that the word "table" can prime on "chair" because the two words belong for most people into the same category (Vaidya et al. 1999). Hence, it is a psychological technique and process that engages people in a task or exposes them to a stimulus (Samson and Loewenstein 2014). Primes can occur or be implemented in different forms and in consequence activate associated memories (stereotypes, attitudes etc.). This cognitive and subconscious process may then affect individuals' performance or attitude on a subsequent task (Tulving et al. 1982). Within the scope of the exposed series of experiments, we apply several priming stimuli (as independent variable) and examine its effect on privacy concerns as the dependent variable. Therewith, we assume a direct influence from primed misattributions (shown in the enhanced APCO-model) on privacy concerns as a proxy for privacy behavior.

Online surveys were used for data collection and the experiments were set up as follows: the participants got a short introduction and were asked a filter question whether they own or do not own a SMD. If they did not, they skipped automatically to the end of the survey and were excluded from the study as experiences with SMD, and thus with apps, is essential for valid responses (Payne et al. 1999). Subsequently, the prevailing priming stimulus was applied randomly. As dependent variable, the App Information Privacy Concern (AIPC) was tested immediately afterwards. The 17 items of the AIPC were displayed in randomized order. Subsequently, the participants had to pass an experiment-specific manipulation check before answering some general questions regarding gender, age, and their primary used smartphone device. Respondents' OS affiliation was identified according to the device manufacturer and grouped into iOS and non-iOS.

The specific experimental settings are literature driven and applied to the field of apps. To address the research question we conducted six independent experiments using a one factorial-subject design for each experiment. The data collection took place from the November 2016 until December 2016. Students from the same university applied to the experiments. We ensured that there was no overlap of participants. Five experiments were conducted by personally address students before their lectures started. The (same) experimenter gave a short and always similar introduction about the conducted experiment. Thus, we aimed to exclude the experimenter bias and ensured independent samples. The sixth experiment was conducted by an anonymous online experiment distributed via social media. In each experiment the participants were randomly assigned to either the treatment group(s) or the control group. Overall 1599 individuals participated in the six experiments. 1126 responses were used for analysis.

## *The App Information Privacy Concern (AIPC) as Dependent Variable*

To investigate the causal relation between the stimulus and participants' privacy concern, an App Information Privacy Concern (AIPC) was developed. To address the contextual factors and the recommendation to "create and utilize more validated instruments so that future privacy research can more readily build upon one another" (Bélanger and Crossler 2011, p.1035), we developed an AIPC, based on extant literature. As a basis we employed the multidimensional scale of Smith et al. (1996), who came up with the Concern For Information Privacy (CFIP). Further, we took the Internet Users' Information Privacy Concerns (IUIPC) of Malhotra et al. (2004), the Mobile Users' Information Privacy Concerns (MUIPC) of Xu et al. (2012), and the Global Information Privacy Concern (GIPC) of Smith et al. (1996) into account. Based on the mentioned measurements we rearranged the existing items and adapted it to the contextual factors of apps. After analyzing the constructs, the underlying items, and the existing overlaps in terms of applicability to apps and mobile ecosystems, we identified 17 items for further investigation and restatement.

To evaluate our construct and extract the latent variables, we conducted a principal axis factoring analysis (PFA) to test the 17-items construct on validity. Therefore, we collected data via an online survey and measured all items of the AIPC by a 7-point Likert-scale ranging from "totally disagree" (1) to "agree completely" (7). A "no opinion" was used prohibiting that responses were forced (Bellman et al. 2004). Data collection took place in October 2016 in Germany. 355 participants (n=355) conducted the survey. After deleting incomplete data sets, 269 participants (n=269) were included in the subsequent data analysis.

The age of participants ranges from 13 to 66 years (MV=21.57; SD=8.49). Of the remaining participants, 52.8% (n=142) were female and 47.2% were male (n=127). The Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO = 0.920) and Bartlett's measure being highly significant, provide that our data is suitable for factor analysis. We applied Kaiser-Guttmann rule and extracted three factors out of initial 17-item construct with an eigenvalue greater than 1. The three factors explain 60.64% of overall variance and all items are significant with a Cronbach's alpha of 0.920. Oblique rotation (Promax) was applied to account for interpretability of the extracted factors. Based on this result the AIPC is suitable for measuring the dependent variable in our experimental design.

The AIPC defines to which degree individuals are concerned about their information privacy regarding mobile apps. In particular it states the "anxiety", "requirements" and "requirements" individuals have regarding the collection, usage and processing of the data gained by mobile apps. The extracted dimensions are described as follows: "anxiety" is defined as degree to which a person is concerned about the usage and processing of the collected personal data via mobile apps. The second factor defined as "personal attitude" specifies how important it is for a person to protect their personal data and how sensitive they handle it. "Requirements" as the third is defined as the degree to which an individuals has request towards third parties regarding the handling of their personal data.

### *Experiment 1: What You See Is All There Is*

What you see is all there is, is a prime created by low mental processing as the given information is not questioned or verified by users (Brenner et al. 1996; Kahneman 2013). Therefore, individuals do not assess the relevance or the quality of the information which leads to a more coherent picture of the situation (Kahneman 2013). Following this, experiment one tries to prime the participants with certain information. To influence individuals' perceptions the treatment group was exposed to the stimulus, while this was absent for the control group. The stimulus for the treatment group was implemented by displaying a chart to the participants with the reference, that about 75% of all apps have access to at least one of the displayed functions (location, device id, access to other profiles, camera, contacts, list of all calls, microphone, sms, calendar) (Statista 2014). Due to the displayed information, we hypothesize that the prime will lead individuals towards a higher AIPC in comparison to the control group.

The experiment was conducted as an online experiment the third week of November 2016 with undergraduate students in business studies in an IS-related lecture. 177 participants (n=177) attended to the study. After deleting questionnaires which contained no-smartphone users, incomplete questionnaires and ineffective stimuli (negative manipulation check) 147 (n=147) data sets were included in the analysis. The participants were randomly distributed to the two groups: 80 participants (n=80) to treatment I and 67 participants (n=67) to the control group. The MV of participants' age was 20.00 (SD=1.85). Of the remaining participants, 57.8% (n=85) were female and 42.2% were male (n=62). 83 participants (n=83) used iOS and 64 (n=64) used non-iOS.

Major results of the first experiment are as follows. Following the classical experimental analysis (Bargh et al. 1996; Tversky and Kahneman 1981; Schwarz 1990), we compared MV (t-test) of the experimental group (exposed to stimulus) and the control group regarding their overall AIPC and its three dimensions "anxiety", "personal attitude" and "requirements". An independent sample t-test indicated that there was no significant difference between treatment group I and the control group, t(145)=1.577, p=.117, for overall AIPC, t(145)=1.096, p=.275 for "anxiety" and t(145)=.935, p=.352, for "requirements". However, there was a significant difference for "personal attitude" t(145)=2.051, p=.420, at a 5% level. For female ($n_{treat}$=47; $n_{con}$=38) an independent sample t-test indicated that there was no significant difference between treatment group I and the control group, t(83)=.547, p=.586, for overall AIPC, t(83)=.407, p=.685, for "anxiety", t(83)=.490, p=.626, for "personal attitude" and t(83)=.370, p=.713, for "requirements". For male ($n_{treat}$=33; $n_{con}$=29) an independent sample t-test showed that there was a significant difference between treatment group I and the control group, t(60)=1.689, p=.097, for overall AIPC at a 10%-level and a significant difference t(60)=2.654, p=.010 for "personal attitude" at a 1% level. No significant difference was found t(60)=1.183, p=.242, for "anxiety" and t(60)=.958, p=.342, for "requirements". For iOS users ($n_{treat}$=45; $n_{con}$=38) an independent sample t-test indicated that there was no significant difference between treatment group I and the control group, t(81)=.296, p=.768, for overall AIPC and neither t(81)=-.243, p=.809, for "anxiety", t(81)=1.422 p=.159, for "personal attitude" and t(81)=-.0250, p=.980, for "requirements". For non-iOS users ($n_{treat}$=35; $n_{con}$=29) an independent sample t-test showed that there was a significant difference between treatment group I and the control group, t(62)= 1.875 p=.065, for overall AIPC and for "anxiety" t(62)=1.711, p=.092 at a 10%-level. No significant difference were found t(62)=1.470, p=.146, for "personal attitude" and t(62)=1.441, p=.155 for "requirements".

The experiment shows that the prime leads to higher concerns on the level of "personal attitude". However, this is only confirmed on a gender level for male for the AIPC and "personal attitude". For OS-affiliation the prime was confirmed for non-iOS for the AIPC and anxiety.

### *Experiment 2: Prior Privacy Experience*

Experiment two aims to prime the influence of prior experience on AIPC. It focuses on the influence of antecedents in combination of the extraneous factors and their influence on the AIPC (Smith et al. 2011; Dinev et al. 2015). Research has suggested that prior privacy experience may influence the individual's information privacy concern (Culnan 1993; Stone and Stone 1990). Merely by being exposed to questions about the personal prior privacy experience can lead to misattribution effects which are closely related to peripheral cues. Those misattribution effects can arise when individuals wrongly ascribe an experience and act upon it with a misunderstanding of the situation (Bem 1967; Kahneman and Frederick 2002).

To conduct the experiment the treatment group had to answer several questions about their prior privacy experience, based on the dimensions for prior privacy experience by Xu et al. (2012) (deduced from Smith et al. 1996).For the control group this stimulus was absent. We hypothesize that the prime will lead individuals towards a higher AIPC because of the misattribution effect on questions about their prior experience. Hypothetically, the participants will overestimate privacy problems, even if they had no negative prior experience.

The experiment was conducted as an online experiment in the third week of November 2016 with undergraduate students in business studies in an IS-related lecture. 156 participants (n=156) attended to the study. After deleting questionnaires which contained no-smartphone users, incomplete questionnaires and ineffective stimuli (negative manipulation check) 125 (n=125) data sets were included in the analysis. The participants were randomly distributed to the two groups: 58 participants (n=58) in treatment I and 67 participants (n=67) to the control group. The MV of participants' age was 19.9 (SD=1.83). Of the remaining participants were 48.8% (n=61) female and 51.2% (n=64) were male. 68 (n=68) participants used iOS and 64 (n=64) used non-iOS.

Major results of the second experiment are as follows. Following the classical experimental analysis (Bargh et al. 1996; Schwarz 1990; Tversky and Kahneman 1981), we compared MV (t-test) of the experimental group (exposed to stimulus) and the control group regarding their overall AIPC and its three dimensions "anxiety", "personal attitude" and "requirements". An independent sample t-test indicated that there was a significant difference between treatment group I and the control group t(123)=1.648, p=.103, for overall AIPC on a 10%-level. No significant difference were found t(123)=1.381, p=.170, for "anxiety" t(123)=1.553, p=0.123, for "personal attitude" and t(123)=1.182, p=.240, for "requirements". For female ($n_{treat}$=23; $n_{con}$=38) an independent sample t-test indicated that there was no significant difference between treatment group I and the control group, t(59)=-.375, p=.709, for overall AIPC, t(59)=-.401, p=.690 for "anxiety", t(59)=-.401, p=.690, for "personal attitude" t(59)=-.303, p=.763, and for "requirements" t(59)=-.829 p=.411. For male ($n_{treat}$=35; $n_{con}$=29) an independent sample t-test showed that there was a significant difference between treatment group I and the control group, t(62)=2.353, p=.022, for overall AIPC and t(62)=2.296, p=.0250 for "personal attitude" at a 5% level. At a 10%-level there was a significant difference t(62)=1.920, p=.0590, for "anxiety". No significant difference was found t(62)=1.620, p=.110, for "requirements". For iOS users ($n_{treat}$=27; $n_{con}$=38) an independent sample t-test indicated that there was no significant difference between treatment group I and the control group, t(63)=1.484, p=.145, for overall AIPC, t(63)=1.125, p=.267, for "anxiety" and t(63)=1.350, p=.182, for "requirements". However, there was a significant difference t(63)=1.946, p=.056, for "personal attitude" at a 10%-level. For non-iOS users ($n_{treat}$=31; $n_{con}$=29) an independent sample t-test showed that there was no significant difference between treatment group I and the control group, t(58)=.994, p=.324, for overall AIPC, t(58)=.971, p=.336, for "anxiety" t(58)=.255, p=.800, for "personal attitude" and t(58)=.768, p=.445, for "requirements".

The experiment shows that the prime with prior experience leads to higher AIPC on an overall level. However, this is only confirmed on a gender level for male for the AIPC, "personal attitude" and "anxiety". For OS-affiliation the prime was confirmed for iOS on the factor "personal attitude".

### *Experiment 3: Scrambled Sentences*

Experiment three makes use of a scrambled sentence test (Bargh et al. 1996; Srull and Wyer 1979) to prime individuals' AIPC. Bargh et al. (1996) showed in the "Florida-Effect" that actions and emotions can be primed by occasions individuals are not even conscious about. For the experiment the two groups were exposed to a series of 10 scrambled word groupings. The task was to construct a grammatical correct four-word sentence out of a set of five-word elements. The five words for each sentence were displayed in a scrambled order such as "my privacy threaten apps respect". For the treatment group, it was intended to prime AIPC. Therefore, the sentence contained words related to the topic: personal data, apps, privacy. For each four-word combination can be created with either a positive verb: use, trustworthy, protect etc. or with negative verbs: dubious, share, abuse etc. The control group did also get a scrambled sentence test, however, there was no prime involved therefore they got displayed neutral sets of five-word elements in scrambled order such as "I apple eating like cutting ". We hypothesize that participants in the treatment condition have higher AIPC due to the subconscious priming compared to the control group.

The experiment was conducted as an online experiment in the fourth week of November 2016 with students from faculty of law and economics. 205 participants (n=205) attended to the study. After deleting questionnaires which contained no-smartphone users, incomplete questionnaires and ineffective stimuli (negative manipulation check) 143 (n=143) data sets were included in the analysis. The participants were randomly distributed to the two groups: 70 participants (n=70) in treatment I and 73 participants (n=73) to the control group. The MV of participants' age was 23.34 (SD=3.23). Of the remaining participants, 37.1% (n=53) were female and 62.9% were male (n=90). 66 (n=66) participants used iOS and 77 (n=77) used non-iOS.

Major results of the third experiment are as follows. Following the classical experimental analysis (Bargh et al. 1996; Tversky and Kahneman 1981; Schwarz 1990), we compared MVs (t-test) of the experimental group (exposed to stimulus) and the control group regarding their overall AIPC and its three dimensions "anxiety", "personal attitude" and "requirements". An independent sample t-test indicated that there was a significant difference between treatment group I and the control group t(141)=-2.247, p=.026, for overall AIPC, and t(141)=-2.153, p=.033, for "anxiety" on a 5%-level. Further, there was a significant difference t(141)=-3.090, p=.002, for "personal attitude" at a 1%-level. No significant difference was found t(141)=-.465, p=.642, for "requirements". For female ($n_{treat}$=26; $n_{con}$=27) an independent sample t-test indicated that there was no significant difference between treatment group I and the control group, t(51)=-.306, p=.761, for overall AIPC, t(51)=-.709, p=.482, for "anxiety", t(51)=-.457, p=.650, for "personal attitude", and t(51)=.804, p=.425, for "requirements". For male ($n_{treat}$=44; $n_{con}$=46) an independent sample t-test showed that there was a significant difference between treatment group I and the control group, t(88)=-2.657, p=.009, for overall AIPC and t(88)=-3.461, p=.001, for "personal attitude" at a 1% level. At a 5%-level there was a significant difference t(88)=-2.245, p=.0270, for "anxiety". No significant difference was found t(88)=-1.159, p=.250, for "requirements". For iOS users ($n_{treat}$=34; $n_{con}$=32) an independent sample t-test indicated that there was no significant difference between treatment group I and the control group, t(64)=-1.183, p=.241, for overall AIPC, t(64)=-1.245, p=.218, for "personal attitude", and t(64)=.415, p=.680, for "requirements". However, there was a significant difference t(64)=-1.704, p=.093 for "anxiety" at a 10%-level. For non-iOS users ($n_{treat}$=36; $n_{con}$=41) an showed sample t-test showed that there was a significant difference between treatment group I and the control group, t(75)=-2.252, p=.027, for overall AIPC at a 5%-level. Moreover, there was a significant difference t(75)=-3.540, p=.001, for "personal attitude" at a 1%-level. No significant difference were found t(75)=-1.538, p=.128 for "anxiety", and t(75)=-1.393, p=.168, for "requirements".

The experiment shows that the scrambled sentence exercise leads to higher AIPC. Significant differences in "personal attitude" and "anxiety" were found. However, this is only confirmed on a gender level for male for the AIPC, "personal attitude" and "anxiety". For OS-affiliation the prime was confirmed for iOS for "anxiety" and for the AIPC and "personal attitude" for non-iOS.

### *Experiment 4: Framing*

The fourth experiment is testing a peripheral cue known as framing. The effect aims to give the same information framed in a positive and negative formulation (McNeil et al. 1982; Tversky and Kahneman 1981). Different representations of the same information evoke different emotions and determine how an information is perceived (Goes 2013). The idea of formulating the same information in two different ways can be transferred to the field of information privacy as IS research has already emphasized the possible influence of message framing on privacy and trust (Angst and Agarwal 2009; Lowry et al. 2012). Thus, experiment four aims to examine the influence of this framing effect towards AIPC. It was designed with two treatment groups, which got the same pie-chart displayed. The difference between the treatment groups was the formulation of the message beside the pie-chart: "94% of all apps in the App Store are uncritical" vs. "6% of all apps in the App Store are critical" (Bruce Snell 2016). Before the participants were exposed to the stimulus, they got a description of what we understand critical/uncritical apps are, to ensure all participants will have the same understanding of the term. The control group was exposed to no stimulus. We hypothesize that the stimulus of treatment group I (negative frame: 6% critical apps) will cause a negative effect leading to a higher AIPC compared to the control group and the treatment group II (positive frame: 94% uncritical apps).

The experiment was conducted as an online experiment in the third week of November 2016 with undergraduate students in business studies in an IS-related lecture. 266 participants (n=266) attended to the study. After deleting questionnaires which contained non-smartphone users, incomplete questionnaires and ineffective stimuli (negative manipulation check) 207 (n=207) data sets were included in the analysis. The participants were randomly distributed to the three groups: 55 participants (n=55) in treatment I (negative stimulus), 58 participants (n=58) in treatment II (positive stimulus) and 95 participants (n= 95) to the control group. The mean value (MV) of participants' age was 20.44 (SD=2.05). Of the remaining participants, 58.9% (n=122) were female and 41.1% were male (n=85). 96 participants (n=96) used iOS and 111 (n=111) used non-iOS.

Major results of experiment four are as follows. After conducting a one-factorial analysis of variance (ANOVA) to test the three groups on significant differences regarding their overall AIPC and its three dimensions "anxiety", "personal attitude" and "requirements" using Gabriel as a Post-Hoc-Test (Field 2013), there are no significant differences on a 5% level between the experimental groups. Also, no significant differences could be found on the level of gender and OS-affiliation. Following the classical experimental analysis (Bargh et al. 1996; Tversky and Kahneman 1981; Schwarz 1990), we also compared mean values by conducting an independent t-test of the two treatment groups (exposed to reversed stimuli). The major results are as follows. An independent sample t-test indicated that there was no significant difference between treatment group I (negative stimulus) and the treatment group II (positive stimulus), t(110)=-.131, p=.896, for overall AIPC, t(110)=-.335, p=.739, for "anxiety", t(110)=.331, p=.742, for "personal attitude" and t(110)=.096, p=.932 for "requirements". For female ($n_{treatI}$=33; $n_{treatII}$=33) an independent sample t-test indicated that there was no significant difference between the treatment groups, t(64)=.557, p=.579, for overall AIPC, t(64)=.044, p=.965, for "anxiety", t(64)=1.475, p=.145, for "personal attitude" and t(64)=.387, p=.700 for "requirements". An independent sample t-test for male ($n_{treatI}$=22; $n_{treatII}$=24) showed that there was no significant difference between the treatment groups, t(44)=-.829, p=0.412, for overall AIPC, t(44)=-.619, p=.539, for "anxiety", t(44)=-1.252, p=.217, for "personal attitude" and t(44)=-.313, p=.756, for "requirements". For iOS users ($n_{treatI}$=22; $n_{treatII}$=35) an independent sample t-test indicated that there was no significant difference between the treatment groups, t(55)=.539, p=.592, for overall AIPC, t(55)=.300, p=.765, for "anxiety", t(55)=.958, p=.342 for "personal attitude" and t(55)=.210, p=.834, for "requirements". For non-iOS users (ntreat1=33; n treat2=22) an independent sample t-test showed that there was no significant difference between the treatment groups, t(53)=-0.043, p=.966, for overall AIPC, t(53)=-.123, p=.903, for "anxiety", t(53)=-.093, p=.926, "personal attitude" and t(53)=.371, p=.712, for "requirements".

No significant differences were found. Thus, the experiment did not confirm that the framing effect leads to higher privacy concerns.

### *Experiment 5: Order of Information*

The idea of this experiment is to examine if the halo effect holds for attributes of apps and thus influences the individual's AIPC. In theory, the halo effect is a cognitive bias which results in a more coherent picture of people and situations (Asch 1946; Nisbett and Wilson 1977). The effect can be described as the tendency to like or dislike all attributes of an object without knowing it in detail and being able to judge all its attributes (Nisbett and Wilson 1977). The order of the sequence of attributes can lead to different impression about the same object, person, or situation because the first attributes in the list override the meaning of the subsequent attributes due to the halo effect (Asch 1946). To set up the experiment, a list of app attributes was presented in different orders to the two treatment groups. The participants were randomly assigned to one of the three experimental groups. The difference between the two treatment groups was the order (positive to negative) of five given attributes. Treatment group I was exposed to the positive (descending) sequence: very good evaluations; cost-free app; attainment of an aim; function abuse; unauthorized data transfer. Treatment group II was exposed to the list of attributes in the reverse order (negative to positive). For the control group the stimulus was absent. We hypothesize that the positive sequence of attributes will cause a positive effect on the AIPC leading to a lower information privacy concern and vice versa to the reversed sequence.

The experiment was conducted as an online experiment in the fourth and last week of November 2016 with students from the faculty of law and economics. 301 participants (n=301) attended to the study. After deleting questionnaires which contained no-smartphone users, incomplete questionnaires and ineffective stimuli (negative manipulation check) 181 (n=181) data sets were included in the analysis. The participants were randomly distributed to the three groups: 41 participants (n=41) in treatment I (positive stimulus), 54 participants (n=54) in treatment II (negative stimulus) and 96 participants (n=96) to the control group. The MV of participants' age was 23.28 (SD=3.88). Of the remaining participants, 39.2% (n=71) were female and 60.8% were male (n=110). 81 (n=81) participants used iOS and 100 (n=100) used non-iOS.

Major results of experiment five are as follows. After conducting a one-factorial analysis of variance (ANOVA) to test the groups on significant differences regarding their overall AIPC and its three dimensions "anxiety", "personal attitude" and "requirements" using Gabriel as a Post-Hoc-Test (Field 2013), there are no significant differences on a 5% level between the experimental groups. Also, no significant differences could be found on the level of gender and OS-affiliation. Following the classical experimental analysis (Bargh et al. 1996; Tversky and Kahneman 1981; Schwarz 1990), we also compared MVs (t-test) of the two treatment groups (exposed to reversed stimuli). An independent sample t-test indicated that there was a significant difference between treatment group I (positive stimulus) and the treatment group II (negative stimulus), t(90)= -1.662, p=.100, for overall AIPC and t(90)=- 1.675, p=.097, for "personal attitude", at a 10%-level. No significant differences were found t(90)=-1.352, p=.180, for "anxiety", and t(90)=-1.110, p=.270 for "requirements". For female ($n_{treatI}$=15; $n_{treatII}$=21) an independent sample t-test indicated that there was no significant difference between the treatment groups, t(34)=-.612, p=.544, for overall AIPC , t(34)=-.415, p=.681, for "anxiety", t(34)=-.663, p=.512, for "personal attitude", and t(34)=-.581, p=.565, for "requirements". For male ($n_{treatI}$=25; $n_{treatII}$=30) an independent sample t-test showed that there was a significant difference between the treatment groups, t(53)=-1,778, p=.081, for overall AIPC at a 10%-level. No significant differences were found t(53)=-1.495, p=.141, for "anxiety", t(53)=-1.609, p=.114, for "personal attitude", and t(53)=-1.088, p=0.282 for "requirements". For iOS users ($n_{treatI}$=24; $n_{treatII}$=25) an independent sample t-test indicated that there was no significant difference between the treatment groups, t(47)=-.614, p=.542, for overall AIPC, t(47)=-.349, p=.729, for "anxiety", t(47)=-.624, p=.536 for "personal attitude", and t(47)=-.748, p=.458 for "requirements". For non-iOS users ($n_{treatI}$=16; $n_{treatII}$=26) an independent sample t-test showed that there was a significant difference between the treatment groups, t(40)=-2.170, p=0.036, for overall AIPC and t(40)=-2.222, p=.320, for "personal attitude" at a 5%-level. Further, there was a significant difference t(40)=-1.906, p=.064, for "anxiety" at a 10%-level. No significant differences was found t(40)=-1.078, p=.288, for "requirements".

The experiment shows that order of information leads to higher AIPC and shows significant differences in "personal attitude". However, this is only confirmed on a gender level for male for the AIPC. For OS-affiliation the prime was confirmed for non-iOS for the AIPC, "anxiety" and "personal attitude".

### *Experiment 6: Availability*

Experiment six aims to prime the influence by naming critical or uncritical apps. In situations of uncertainty individuals use simplifying strategies, such as heuristics, to make decisions (Tversky and Kahneman 1973). The experimental setting is based on the work of Schwarz et al. (1990), who requested subjects to estimate their assertiveness. Participants were asked to describe only few or many examples of being assertive or unassertive (Schwarz 1990). If the recall process was easy, the subjects judged themselves according to the recalled behavior. When the recall process was difficult, the corresponding recall affected self-judgement was the opposite to the implications of the recalled behavior (Schwarz 1990).

Besides a control group, we arranged two main treatments in which participants were asked to name either critical or uncritical apps (free fields; no force to respond). According to Schwarz (1990) we set up two sub-groups (name three or six apps) for each main treatment to test for the implications of the ease or difficulty of recall on the AIPC. Before the participants were exposed to the stimuli, they got a description of what we understand as critical/uncritical apps to ensure all participants will have the same understanding of the term. We hypothesize that individuals are primed by naming critical/uncritical apps. Further we hypothesize that individuals have a lower AIPC if they cannot easily recall any negative experience regarding the usage of personal data by apps. The fluency with which the individuals are recalling examples to judge the frequency of critical apps is relatively low and in consequence they have a lower AIPC. Contrary, if individuals are not able to list uncritical apps their AIPC is rather high. This leads to a bias that is due to the retrieval of examples.

The experiment was conducted as an online experiment in the fourth week of November 2016 until the last week of December with undergraduate students from the law and economics faculty as well as with participants reached via social media and email. 494 participants (n=494) attended to the study. After deleting questionnaires which contained no-smartphone users, incomplete questionnaires and ineffective stimuli (negative manipulation check) 323 (n=323) data sets were included in the analysis. The participants were randomly distributed to five groups: 57 participants (n=57) in treatment I (naming 3 uncritical apps), 55 participants (n=55) in treatment II (naming six uncritical apps), 56 participants (n=56) in treatment III (naming three critical apps), 67 participants (n=67) in treatment IV (naming six critical apps), and 88 participants (n=88) to the control group. The MV of participants' age was 26.07 (SD=6.68). Of the remaining participants, 47.4% 153 (n=153) were female and 52.6% were male 170 (n=170). 163 (n=163) participants used iOS and 160 (n=160) used non-iOS.

Major results of experiment six are as follows. After conducting a one-factorial analysis of variance (ANOVA) to test the groups on significant differences regarding their overall AIPC and its three dimensions "anxiety", "personal attitude" and "requirements" using Gabriel as a Post-Hoc-Test (Field, 2013), there are no significant differences on a 5% level between the experimental groups. Also, no significant differences could be found on the level of gender and OS-affiliation.

Following the classical experimental analysis (Bargh et al. 1996; Tversky and Kahneman 1981; Schwarz 1990), we also compared MVs (t-test) of the four treatment groups (critical & uncritical apps). An independent sample t-test indicated that there was a significant difference between treatment group I (naming three uncritical apps) and the treatment group II (naming six uncritical apps), t(110)= -1.862, p=.065, for "anxiety", at a 10%-level. No significant differences were found t(110)= -1.466 p=.146, for overall AIPC, t(110)=-1.200, p=.233, for "personal attitude", and t(110)=-0.071, p=.943 for "requirements". An independent sample t-test indicated that there was a no significant difference between treatment group III (naming three critical apps) and the treatment group VI (naming six critical apps), t(121)=.466, p=.642 for overall AIPC, t(121)=.301, p=.764, for "anxiety", t(121)=.229, p=.820, for "personal attitude", and t(121)=.872, p=.385, for "requirements". For female for the positive treatments (I & II) ($n_{pos3}$=26; $n_{pos6}$=31) an independent sample t-test indicated that there was no significant difference between the treatment groups for overall AIPC and neither for "anxiety", "personal attitude", and "requirements". The same is true for the negative treatments (III & IV) ($n_{neg3}$=32; $n_{neg6}$=22). Interestingly, in contrast to women, there are significant differences for men for the positive treatments (I & II) ($n_{pos3}$=31; $n_{pos6}$=24) t(53)= -1.712, p=.093, for "anxiety" at a 10% level of significance. No significant differences were found t(53)= -1.370, p=.176, for overall AIPC, t(53)=- 1.008, p=.318, for "personal attitude", and t(53)=-.341, p=.734 for "requirements". Further, an independent sample t-test indicated that there was no significant difference between the negative treatments (III & IV) ($n_{neg3}$=24; $n_{neg}$=54) for overall AIPC and neither for "anxiety", "personal attitude",and "requirements". For iOS users for the positive treatments ($n_{pos3}$=33; $n_{pos6}$=30) an independent sample t-test indicated that there was no significant difference between the treatment groups for overall AIPC and neither for one of the different levels. The same is true for iOS users for the negative treatments ($n_{neg3}$=28; $n_{neg6}$=28). However, for non-iOS users for the positive treatments (I & II) ($n_{pos3}$=24; $n_{pos6}$=25) an independent sample t-test showed that there was a significant difference between the treatment groups, t(47)=-1.788, p=.080, for overall AIPC at a 10% level and t(47)=-2.423, p=.019, for "anxiety" at a 1%-level. Further, there was a no significant difference for the positive treatment groups t(47)=-1.008, p=.319, for "personal attitude", and t(47)=-.504, p=.617 for "requirements". Moreover, there was no significant difference between the negative treatments (III & IV) ($n_{neg3}$=28; $n_{neg6}$=39), for overall AIPC and neither for "anxiety", "personal attitude", and "requirements".

The experiment shows that the prime was only confirmed for the different positive treatments (naming three or six uncritical apps) for "anxiety". This is also true for men. However, for female no significant differences could be found. For OS-affiliation the prime was confirmed for non-iOS for the AIPC, as well as "anxiety".

## Interpretation and Limitations

In the introduction we posed the research question "Which priming stimuli influence app information privacy concerns?" To answer this question we presented six experiments providing the influence of several stimuli on app information privacy concerns. These results show that WYSIATI, prior experience, scrambled sentences, order of information, and availability have a significant impact on app information privacy concerns or second order constructs of the measurement (see table 1).

This findings support the propositions of Dinev et al. (2015) that peripheral cues, heuristics, biases, and misattributions do have an impact on information privacy concerns, and subsequently on privacy behaviors. The results emphasize the classification of users' behavior in mobile ecosystems as low-effort processes. Although the experiments represent a low-threshold attempt to the field, the results of the experiments show the relevance of such investigations to understand users' behavior in information systems.

| Exp. 1:WYSIATI | AIPC | Anxiety | Personal Attitude | Requirements |
|---|---|---|---|---|
| Overall | x | x | Sig. (5%) | x |
| Female | x | x | x | x |
| Male | Sig. (10%) | x | Sig. (1%) | x |
| iOS | x | x | x | x |
| non-iOS | Sig. (10%) | Sig. (10%) | x | x |
| Exp. 2:Prior Experience | | | | |
| Overall | Sig. (10%) | x | x | x |
| Female | x | x | x | x |
| Male | Sig. (5%) | Sig. (5%)x | Sig. (5%) | x |
| iOS | x | x | Sig. (10%) | x |
| Non-iOS | x | x | x | x |
| Exp. 3: Scrambled Sentences | | | | |
| Overall | Sig. (5%) | Sig. (5%) | Sig. (1%) | x |
| Female | x | x | x | x |
| Male | Sig. (1%) | Sig. (5%) | Sig. (5%) | x |
| iOS | x | Sig. (10%) | x | x |
| Non-iOS | Sig. (5%) | x | Sig. (1%) | x |
| Exp. 4: Framing | | | | |
| Overall | x | x | x | x |
| Female | x | x | x | x |
| Male | x | x | x | x |
| iOS | x | x | x | x |
| Exp. 5: Order of Information | | | | |
| Overall | Sig. (10%) | x | Sig. (10%) | x |
| Female | x | x | x | x |
| Male | Sig. (10%) | x | x | x |
| iOS | x | x | x | x |
| Non-iOS | Sig. (5%) | Sig. (10%) | Sig. (5%) | x |
| Exp. 6: Availability | | | | |
| Overall | x | Sig. (10%) (uncritical apps) | x | x |
| Female | x | x | x | x |
| Male | x | Sig. (10%) (uncritical apps) | x | x |
| iOS | x | x | x | x |
| Non-iOS | Sig. (10%) (uncritical apps) | Sig. (1%) (uncritical apps) | x | x |

**Table 1. Table of Results**

Thus, it can be deduced that antecedence and the personal approach towards personal information d have an important influence on privacy concerns. Looking at the single experiments, the comparison of iOS and non-iOS show interesting results. Compared to iOS users, non-iOS users seem to be more anxious and concerned when being exposed to a prime. This is probably due to the fact that individuals who are using iOS, are feeling more protected within the used ecosystem. Whereas non-iOS users are more often confronted with malicious apps, Apple claims a stricter control process for accredited apps in their AppStore. Regarding gender, significant differences could be found. This results are supported by general research on the differences between female and male, which provide evidence for a higher risk aversion of women (Eckel and Grossman 2008).

The experiments are subject to several limitations due to the nature of our research. Firstly, the sample size does not represent all age groups because of the large number of students. Moreover, we did not consider culture bound issues as the sample only consists of German users of SMDs (Krasnova and Veltri 2010). In addition, we only have very general information on the demographic characteristics of our respondents, which limits the ability to relate app consumers' information seeking behavior to demographic characteristics. With addressing specific lectures, we also limited our validity in terms of a deficit of randomization. An additional limitation lies in the field of application, which also limits the generalizability of the findings for the use of IS. A further limitation is, that we do not know the level of literacy (specific knowledge in the field) the participants had, e.g. regarding the functionality of apps and the processing of personal information. It is possible that with more elucidation and knowledge transfer in the area of digital ecosystems individuals are more conscious and reflecting, when they are disclosing personal information. Further, when we asked about critical/uncritical apps in our experiments (four and six), we gave the participants a description of what we understand as critical/uncritical apps to ensure everyone will have the same understanding of the term. However, as there were only slight differences in those experiments it is possible that this was too much information influencing the low effort process. Additionally, we asked in experiment two participants how often they were exposed to negative privacy incidents. If they did not (consciously) experience privacy abuse, the prime could mislead. In experiment four it is possible that the pie-chart overshadowed the actual prime (frame of information). According to the enhanced APCO model, we did not bear related constructs (e.g. privacy calculus and trust) in mind which could affect the privacy concern and its liability to the exposed stimuli. Due to the fact that we provide a series of experiments with an overview of the results, we did not analyze underlying more in-depth effects of the experiments.

## Conclusion and Further Research

Our paper deals with the question whether individuals react on exposed primes with a change in the app information privacy concern (AIPC). To investigate the research question developed an AIPC and we conducted six independent experiments with altogether 1954 participants. Even though the results of the experiments were not highly significant in all experimental settings, there is an overall tendency that the chosen primes do affect individuals in mobile ecosystems. This leads to possible implications for practice and research (Acquisti 2012). In practice we see app providers and governmental regulation as two sides of the same coin. Whereas app provider could use results from the experiments to further develop apps in terms of data disclosure, policy-making could start to protect consumers by intervening and bursting low effort processing in digital ecosystems. App providers could try to mislead users by e.g. providing optimized orders of information. While policy makers could force app providers to e.g. incorporate questions or tests which arouse attention to the privacy-related action the users wants to undertake with the proposed download. This could lead to a governmental action plan by introducing the concept of 'digital nudging'. The idea is to design IS that offer individuals more informed choices and thus increasing individual and societal welfare by nudging them towards a more sensible handling of their data (Acquisti 2012).

Further research should investigate particularly privacy awareness, attitudes, concerns and behavior in app markets due to the increasing relevance of app usage as the most common user interface to merge smart environments with connected sensors and devices. Moreover, it is important to conduct more research in finding a suitable instrument for measuring information privacy concern, especially while conducting experiments. Only with a suitable measurement, conclusions on the causal relationship between the independent and the dependent variable can be drawn. We made an attempt to come up with a reliable and valid measurement, however, it is important to replicate these findings to increase validity (e.g. lab experiment) and to further develop the construct. Researchers should investigate other factors (antecedence, trust, risk, regulations) of the enhanced APCO model and their linkages with privacy behavior. Therefore, it might be helpful to not only consider privacy concerns as measurement for privacy behavior. It is also important to consider other constructs (e.g. attitudes) which are common in marketing and consumer behavior research.

## References


Acquisti, A. 2012. “Nudging privacy: The behavioral economics of personal information,” in *Digital Enlightenment Yearbook 2012*, pp. 193–197.

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. “Privacy and human behavior in the age of information,” *Science (New York, N.Y.)* (347:6221), pp. 509–514.

Acquisti, A., and Grossklags, J. 2005. “Privacy and Rationality in Decision Making,” *IEEE Security and Privacy* , pp. 24–30.

Acquisti, A., and Grossklags, J. 2008. “What can behavioral economics teach us about privacy,” *Digital Privacy: Theory, Technologies, and Practices* , pp. 363–377.

Akerlof, G. A. 1970. “The Market for "Lemons": Quality Uncertainty and the Market Mechanism,” *The Quarterly Journal of Economics* (84:3), p. 488.

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,” *Management information systems : mis quarterly* (33:2), pp. 339–370.

Apple Inc. 2017. *Apple Trademark List*. http://https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html.

Ariely, D. 2009. *Predictably irrational*: *The hidden forces that shape our decisions*, New York, NY: Harper Collins Publ.

Asch, S. E. 1946. “Forming impressions of personalities,” *Journal of Abnormal and Social Psychology* (41), pp. 258–290.

Bargh, J. A., Chen, M., and Burrows, L. 1996. “Automaticity of social behavior: Direct effects of trait construct and stereotype-activation on action,” *Journal of Personality and Social Psychology* (71:2), pp. 230–244.

Bélanger, F., and Crossler, R. E. 2011. “Privacy in the Digital Age: A Review of Infomation Privacy Research in Information Systems,” *MIS Quarterly* (35:4), pp. 1017–1041.

Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. 2004. “International differences in information privacy concerns: A global survey of consumers,” *Information Society* (20:5), pp. 313–324.

Bem, D. J. 1967. “Self-perception: An alternative interpretation of cognitive dissonance phenomena,” *Psychological Review* (74:3), pp. 183–200.

Bennett, C. J. 1995. “The political economy of privacy: a review of the literature,” *center for social and legal research, DOE genome project (Final draft), University of Victoria, Department of Political Science, Victoria* .

Brandimarte, L., Acquisti, A., and Loewenstein, G. 2012. “Misplaced Confidences: Privacy and the Control Paradox,” *Social Psychological and Personality Science* (4:3), pp. 340–347.

Brenner, L. A., Koehler, D. J., and Tversky, A. 1996. “On the evaluation of one-sided evidence,” *Journal of Behavioral Decision Making* (9:1), pp. 59–70.

Bruce Snell 2016. “Mobile Threat Report: What's on the Horizon for 2016,” *Intel Security* , pp. 1–12.

Buck, C., Horbel, C., Germelmann, C. C., and Eymann, T. 2014. “The Unconscious App Consumer: Discovering and Comparing the Information - Seeking Patterns,” *Twenty Second European Conference on Information Systems* , pp. 1–14.

Buck, C., Stadler, F., Eymann, T., and Suckau, K. 2017. “Privacy as a Part of the Preference Structure of Users App Buying Decision.,” *Leimeister, Jan Marco ; Brenner, Walter (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)* , pp. 792–806.

Chen, H.-T., and Chen, W. 2015. “Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection,” *Cyberpsychology, behavior and social networking* (18:1), pp. 13–19.

Clarke, R. 1999. “Internet privacy concerns confirm the case for intervention,” *Communications of the ACM* (42:2), pp. 60–67.

Culnan, M. J. 1993. “"How Did They Get My Name?: ": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use,” *MIS Quarterly* (17:3), p. 341.

Dinev, T., and Hart, P. 2006. “An extended privacy calculus model for e-commerce transactions,” *Psychology & Marketing* (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.

Eckel, C. C., and Grossman, P. J. 2008. “Men, women and risk aversion: Experiment evidence,” in *Handbook of experimental economics results,* Amsterdam [u.a.]: North-Holland, pp. 1061–1073.

Field, A. 2013. *Discovering statistics using IBM SPSS statistics*: *And sex and drugs and rock 'n' roll,* Los Angeles, London, New Delhi: Sage.

Fox, Z. 2013. *The Average Smartphone User Downloads 25 Apps*. http://mashable.com/2013/09/05/most-apps-download-countries/#eT9lIhcICOqQ.

Goes, P. B. 2013. “Editor’s ’ Comments Information Systems Research and Behavioral Economics,” *MIS Quarterly* (37:3).

Grossklags, J., and Acquisti, A. 2007. “When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information,” *Information Security* , pp. 7–8.

Hirshleifer, J. 1973. “Where are we in the theory of information?” *The American Economic Review* (63:2), pp. 31–39.

Kahneman, D. 2013. *Thinking, fast and slow,* New York: Farrar Straus and Giroux.

Kahneman, D., and Frederick, S. 2002. “Representativeness Revisited: Attribute Substitution in Intuitive Judgment,” in *Heuristics and biases: The psychology of intuitive judgement*, T. Gilovich, D. W. Griffin and D. Kahneman (eds.), Cambridge, U.K., New York: Cambridge University Press, pp. 49–81.

Kokolakis, S. 2015. “Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon,” *Computers & Security* .

Krasnova, H., and Veltri, N. F. 2010. “Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA,” in *43rd Hawaii International Conference on System Sciences (HICSS), 2010 ; Honolulu, Hawaii, 5 - 8 Jan. 2010*, R. H. Sprague (ed.), Honolulu, Hawaii, USA. 5/1/2010 - 8/1/2010, Piscataway, NJ: IEEE, pp. 1–10.

Lamb, R., and Kling Rob 2003. “Reconceptualizing Users as Social Actors in Information Systems Research,” *MIS Quarterly* (27:2), pp. 197–236.

Li, Y. 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.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., and Wells, T. 2012. “Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers,” *Journal of the American Society for Information Science and Technology* (63:4), pp. 755–776.

Malhotra, N. K., Kim, S. S., Agarwal, J., Tech, G., and Peachtree, W. 2004. “Internet Users ’ The Information the Scale , and a Causal (IUIPC ),” *Psychology & Marketing* (15:4), pp. 336–355.

McNeil, B. J., Pauker, S. G., Sox, H. C., and Tversky, A. 1982. “On the elicitation of preferences for alternative therapies,” *New England Journal of Medicine* (306:21), pp. 1259–1262.

Nisbett, R. E., and Wilson, T. D. 1977. “The Halo Effect: Evidence for Unconscious Alteration of Judgments,” *Journal of Personality and Social Psychology* (35:4), pp. 250–256.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. “The Privacy Paradox: Personal Information Disclosure Intentions vers us Behaviors,” *The Journal of Consumer Affairs* (41:1), pp. 100–126.

Payne, J. W., Bettman, J. R., and Schkade, D. A. 1999. “Measuring Constructed Preferences: Towards a Building Code,” *Journal of Risk & Uncertainty* (19:1-3), pp. 243–270.

Polites, G. L., and Karahanna, E. 2013. “The embeddedness of information systems habits in organizational and individual level routines: Development and disruption,” *Management information systems : mis quarterly* (37:1), pp. 221–246.

Samson, A., and Loewenstein, G. 2014. *The Behavioral Economics Guide 2014* .

Schwarz, N. 1990. *Ease of retrieval as information*: *Another look at the availability heuristic*, Mannheim: ZUMA.

Skinner, G., Han, S., and Chang, E. 2006. *An introduction to a taxonomy of information privacy in collaborative environments:* World Scientific and Engineering Academy and Society (WSEAS) .

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

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. “Information Privacy: Measuring Individuals’ Concerns about Organizational Practices,” *Management Information Systems Quarterly* (20:2), p. 167.

Solove, D. J. 2006. “A taxonomy of privacy,” *University of Pennsylvania Law Review* (154:3), pp. 477–560.

Spiekermann, S., Acquisti, A., Böhme, R., and Hui, K.-L. 2015a. “The challenges of personal data markets and privacy,” *Electronic Markets* (25:2), pp. 161–167.

Spiekermann, S., Böhme, R., Acquisti, A., and Hui, K.-L. 2015b. “Personal Data Markets,” *Electronic Markets* (25), pp. 91–93.

Srull, T. K., and Wyer, R. S. 1979. “The role of category accessibility in the interpretation of information about persons: Some determinants and implications,” *Journal of Personality and Social Psychology* (37:10), pp. 1660–1672.

Statista 2014. *Mobile Sicherheit: Apps greifen auf sensible Daten zu*: *3/4 aller Apps können auf sensible Funktionen zugreifen*. https://www.securepim.com/mobile-sicherheit-34-aller-apps-koennen-auf-sensible-funktionen-zugreifen/. Accessed 3 December 2016.

Statista 2017. *Number of free mobile app downloads worldwide from 2012 to 2017 (in billions)*. https://www.statista.com/statistics/241587/number-of-free-mobile-app-downloads-worldwide/.

Statistic Brain 2016. *Mobile Phone App Store Statistics*. http://www.statisticbrain.com/mobile-phone-app-store-statistics/.

Stone, E. F., Gueutal, H. G., Gradner, D. G., and McClure, S. 1983. “A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations,” .

Stone, E. F., and Stone, D. L. 1990. “Privacy in organizations: Theoretical issues, research findings, and protection mechanisms,” *Personnel and Human Resources Management,* (8:3), 349-411.

Tulving, E., Schacter, D. L., and Stark, H. A. 1982. “Priming effects in word-fragment completion are independent of recognition memory,” *Journal of Experimental Psychology: Learning, Memory, and Cognition* (8:4), pp. 336–342.

Tversky, A., and Kahneman, D. 1973. “Availability: A heuristic for judging frequency and probability,” *Cognitive Psychology* (5:2), pp. 207–232.

Tversky, A., and Kahneman, D. 1981. “The framing of decisions and the psychology of choice,” *Science* (211:4481), pp. 453–458.

Vaidya, C. J., Gabrieli, J. D., Monti, L. A., Tinklenberg, J. R., and Yesavage, J. A. 1999. “Dissociation between two forms of conceptual priming in Alzheimer’s disease,” *Neuropsychology* (13:4), pp. 516–524.

Venkatesh, V., Thong, J. Y. L., and Xu, 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.

Watson-Manheim, M.-B., and Belanger, F. 2002. “Support for Communication-Based Work Processes in Virtual Work,” *e-Service Journal* (1:3), pp. 61–82.

Weinberg, P. 1995. “Emotional Aspects of Decision Behavior. a Comparison of Explanation Concepts,” *European Advances in Consumer Research* (2), 246-250.

Weiser, M. 1991. “The computer for the 21st century,” *Scientific american* (265:3), pp. 94–104.

Wellman, B. 2010. “The Reconstruction of Space and Time: Mobile Communication Practices,” *Contemporary Sociology: A Journal of Reviews* (39:2), pp. 179–181.

Westin, A. F. 1967. “Privacy and freedom,” (25:1).

World Economic Forum 2011. *Personal Data: The Emergence of a New Asset Class*. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

Xu, H., Gupta, S., Rosson, M., and Carroll, J. 2012. “Measuring Mobile Users' Concerns for Information Privacy,” *ICIS 2012 Proceedings* .

Yoo, Y. 2010. “Computing in everyday life: a call for research on experiential computing,” *MIS Quarterly* (34:2), pp. 213–231.