Low Effort and Privacy – How Textual Priming Affects Privacy Concerns of Email Service Users

Christoph Buck
Queensland University of Technology
Brisbane, Australia
christoph.buck@qut.edu.au

Tamara Dinev
Florida Atlantic University
Boca Raton, USA
tdinev@fau.edu

Abstract

The integration of digital applications and systems into the everyday routines of users is inevitably progressing. Ubiquitous and invisible computing requires the perspective of a new user and the inclusion of insights from related disciplines such as behavioral economics or social psychology. This paper takes up the call for research by Dinev et al. (2015) and examines the influence of textual priming elements on the privacy concerns of users of email accounts. The paper provides an operationalization of a privacy concern as a dependent variable, incorporated in an online experiment with 276 participants. The results show highly significant differences between the groups investigated by the experiment. Specifically, the users of different email providers show interesting results. While users of Gmail show no significant reaction in the experiment, users of other email providers show significant differences in the experimental setting.

1. Introduction

The average user of information systems (IS) has changed dramatically as a result of numerous technological innovations: the increasing performance of microprocessors, the progressive networking of products and platforms, the advent of the Internet of Things (IoT) and the worldwide adoption of smart mobile devices (SMD) such as smartphones and tablets. Disruptive innovations like the iPhone, the iPad, and software in form of mobile applications (apps), are diffused into the everyday life of users. This leads to fundamental changes concerning how users interact with computing devices and systems [43].

Numerous advantages for users have been realized through the adoption of IS by the average user and its integration into everyday live; however, this change has not taken place without consequences. Individuals' use of digital services poses multiple challenges for IS research, especially in privacy research. Privacy as digital personal information and highly personalized data collected via digital services has a huge economic value [2]. Most digital services are traded against privacy because of their valuable data. However, in contrast to most economic exchanges, individuals are usually not able to estimate the quality and performance characteristics of the digital services they download and use or the amount and economic value of privacy and personal data they disclose and pay with [37]. Nevertheless, research reveals that individuals are concerned about their privacy and that they are very sensitive regarding the collection and use of their personal data [29].

The traditional approach of information privacy research is in line with the neoclassical *homo oeconomicus* view that users make rational decisions when using IS, e.g. when actively using, downloading, or purchasing a digital service or good [11]. The so-called privacy calculus assumes that users consciously and rationally weigh up costs and risks as well as benefits and opportunities when using IS. Despite the everyday life integration and multiple recurring routine activities (e.g. the use of apps or email accounts), current research assumes a conscious consideration of the users in each individual decision situation in IS. This is supported by the common definition of privacy concerns which refers to a conscious perception of a potential loss associated with the disclosure of personal information [30]. Accordingly, it is assumed users calculate risks and benefits associated with the economic exchange situation when they are confronted with the disclosure of personal information [11].

As it is doubtful, however, that users make only conscious and rational decisions in IS, calls for a new user concept and an associated change in perspective on users of IS have become louder. This includes the

URI: https://hdl.handle.net/10125/64260
978-0-9981331-3-3

demand for the integration of research methods and findings from adjacent research domains such as behavioral economics, social psychology and consumer behavior [12]. This article takes up the call for research and investigates the influence of priming and message framing on users' privacy concerns.

Textual priming elements are omnipresent in everyday user life, especially in IS. Against this background, this paper examines the following research question: Do textual priming stimuli have an influence on the privacy concerns of users of information systems?

To address this research question, the remainder of this article is structured as follows. In the following section, relevant work in information privacy research and behavioral economics in the field of IS and digital services is reviewed. In the methodology section, we present the study design of our online experiment. Subsequently, we interpret and discuss our results and their implications for theory and practice. Finally, a conclusion is provided containing the limitations of our study and suggesting avenues of future research.

2. Relevant work

2.1. Information privacy research

Privacy encompasses several areas of human life and is used in numerous academic disciplines; therefore, it lacks a holistic definition [33, 35]. Consequently, different domains are subsumed under the umbrella term of privacy. Smit et al. (2011) divide privacy into physical privacy and informational privacy. Information privacy refers to information that is individually identifiable or describes the private informational spheres of an individual [33]. Within the scope of IS, personal information is gathered through the analysis of personal data. Thus, this article treats personal information and personal data as equal [7, 26]. Therefore, we will use the term privacy as a reference to information privacy throughout the remainder of this article.

One of the most discussed phenomenon in privacy literature is the so-called privacy paradox. Thus, users articulate high privacy concerns and do not intend to disclose data to IS that could violate their privacy, but behave in an opposite manner [28]. Accordingly, users have a high level of attention with regard to data misuse, but do not change their behavior with regard to data transmission and potential abuse. A consistent, theory-based model for explaining the dichotomy described by the privacy paradox is lacking so far [22].

Privacy has an enormous economic value due to the possibilities of collection, storage, linkage and analysis of data in IS [36, 37]. Regarding data quality, recent developments in mobile technology and an ever-increasing digitization of everyday tasks have led to an unprecedented precision of continuously updated and integrated personal data. Data generated through consumers' use of IS is of particular value. It offers extensive insights into consumers' digital lives, but also into their real lives. While data generated by a single IS contains only a tiny fraction of information about the consumer, the variety of data which can be created is extraordinary. This link to the individual identity creates a deep and holistic picture of the consumer.

Since privacy is seen as a commodity in IS, it is defined as an independent class of goods by the World Economic Forum [8, 36]. As a result, privacy is no longer seen as an absolute social value, but as part of an individual or social cost-benefit analysis [37]. This cost-benefit assessment is described in the literature by the privacy calculus [10, 11]. Users therefore weigh the risks of disclosing personal data against the economic or social benefits and decide according to their preferences. In line with the neoclassical *homo oeconomicus* view, users make this rational decision when downloading, purchasing, and using a digital service or good. The privacy calculus therefore assumes that the users in the decision-making situation rationally weight the aspect of privacy and thus the ability to objectively evaluate the disclosure of personal information and its consequences.

Privacy itself is based on insights, perceptions and experiences and cannot be rationally captured [33]. The measurement of privacy is therefore difficult to operationalize. Concerns about privacy have been established in the IS research domain as a central object of investigation and as a widely recognized proxy for privacy [19, 33]. Due to the broad application of privacy concerns, different perspectives and definitions of privacy concerns have developed in the scientific discourse. A very broad definitional approach of privacy concerns can be seen in the understanding that privacy is defined as the subjective view of users regarding fairness in the handling of personal data [26]. In this article, privacy concerns are defined as users concerns about a possible future loss of privacy as a result of voluntary or involuntary disclosure of personal data [11].

The neoclassic economic assumption of the rationally decisive user raises numerous questions against the background of decision-making in IS. According to economic theory, users do not disclose their data if they do not expect any added value from it [40]. In addition, markets with high information asymmetries inevitably fail [4, 18]. Since the emergence of the (monetary) value of personal data in

digital environments is complex and cannot be assessed by the user, the calculation of privacy, which is often examined in isolation in the literature, must be critically questioned. Taking this view into account, the average user of IS would not use any IS. The reality shows the opposite result.

Nevertheless, most of the existing privacy research in IS disregards 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 cited macro model and a reflection of the existing information privacy literature, has supposed that privacy-related behaviors are represented by deliberate, high-effort processes [7, 12, 25, 33]. Thus, the existing macro models make the critical assumption that "responses to external stimuli result in deliberate analyses, which lead to fully informed privacy-related attitudes and behaviors" [12]. Taking the mass adoption of modern IS and the 'new user' in experiential computing into account [43], the current state of IS research does not incorporate enough knowledge known from behavioral economics, social psychology, consumer behavior, and other related research domains.

2.2. Behavioral economics in IS

According to neoclassical economic theory, humans make rational decisions with regard to their preferences. However, drawing from the knowledge of psychology and economics, behavioral economics assumes that due to cognitive biases and peripheral cues individuals do not act in a consistently rational manner although they are making their best effort [5]. This is also true for personal information disclosure, as privacy is a complex dilemma resulting in different opinions, attitudes as well as behaviors which are noticeably different from one individual to another. Individuals are influenced by subjective threats, potential damages, psychological needs and actual personal economic returns that all shape their choices whether to protect or to disclose personal information [17]. However, this does not directly imply that individuals make irrational or wrong decisions. More subtly, the systematic inconsistencies and decision biases propose that richer theories are needed to understand how and which challenges and obstacles affect the way individuals make judgements about their information privacy [1].

Individuals face two major uncertainties when dealing with privacy decision problems: Firstly, they don't know what the relevant outcomes are under differently contexted situations. Secondly, they are not aware of the related consequences [17]. These uncertainties occur because individuals often do not have sufficient information and limited knowledge about the action that can be taken to protect (or give away) personal data and how third parties handle the data. Further, the consequences are generally hard to predict because it is difficult to find out whether the given information is used for e.g. unwanted communication or price discrimination strategies based on past consumption [17]. To summarize, not only limited cognitive effort restrict the ability to consider or reflect on the consequences of privacy-relevant actions. Inconsistent preferences due to opposing needs and incomplete or asymmetric information about the risks or consequences of disclosing personal information also lead to various systematic deviations from the standard rational decision-making process [1]. Thus, even if individuals would have complete information, they would not be able to process it and act optimally on large amounts of information.

There are first calls in the research community to reconsider the neoclassical principle of rational behavior by individuals and to draw attention to behavioral economics [5, 24]. However, IS research has not yet given much consideration to these calls. In 2015, Dinev et al. proposed an enhanced APCO model to overcome the questionable assumption of solely high-effort decisions in IS [12]. They came up with a set of related propositions deriving from the influences of extraneous factors. The propositions consider cognitive responses and low effort responses (which the current macro models neglect) inspired by research findings from (social) psychology and behavioral economics.

The first ideas of integration with these well-known effects of other research domains were published in the last few years. A distinction between objective and relative risks as well as the examination of limited cognitive resources was undertaken by some authors [3, 21]. Additionally, special attention in the area of "low effort" decisions was paid to affect heuristics and the influence of affect and affective commitment [21, 23, 41, 44]. Gerlach et al. (2018) investigated how users' stereotypical thinking can cause systematic judgment errors when individuals form their beliefs about an online service [13].

The aim of this study is to contribute to this gap in IS research in the field of possible priming effects. Generally, priming is described as a form of cognitive bias that influences individuals in how they perceive and process information [20, 38]. Furthermore, priming refers to the assumption that information is

not doubted and is directly classified as correct information when presented. Priming effects do occur in situations of low cognitive effort and are defined as misattributions that can influence actions as well as emotions [12, 38]. In this article, we focus on indirect priming (mostly denominated as associative or conceptual priming) [38]. Hence, it is a psychological technique and process that engages people in a task or exposes them to a stimulus [31]. A prime can occur or be implemented in different forms and in consequence activates associated memories (stereotypes, attitudes etc.). This cognitive, subconscious process may then affect individuals' attitude or performance on a subsequent task [38]. The findings of priming effects challenge the assumption that individuals make their decisions and judgments deliberately and independently [20].

3. Experimental study

3.1. Research design

In the present study, a textual priming stimulus was used as an independent variable. In order to carry out the experiment in a realistic and comprehensible context for the participants, the digital service email was chosen, since nowadays emails are used as the main communication medium, both privately and professionally. As a result, highly sensitive personal information is sent and received via email accounts. Since Google, as one of the largest providers of email accounts, has admitted that it is possible that Gmail's email accounts can be viewed by individuals from third parties, the privacy of users in this environment is at high risk. As this information was not made available to the general public or distributed proactively to all users of email accounts, this study examines whether the mere news of this privacy intrusion has an impact on the privacy concerns of the participants.

The aim of the chosen experimental research design is to answer cause and effect relations between two variables [16]. In the experiment, the independent variable is presented as a textual priming by showing the participants a sentence with regard to the possible privacy intrusion (third party access to their emails) of their email provider. The independent variable was varied by (I) a possible privacy intrusion and (II) by no privacy intrusion, according to the chosen definition of privacy concerns [11]. The textual priming was motivated by the confirmation of Google that emails can be read by third-party developers [14]. The textual priming and its operationalization are shown in Table 1.

Textual priming stimulus	Operationalization
Possible privacy intrusion (I)	Emails sent and received by PROVIDER users may sometimes be read by real people at third-party providers - not just machines.
No privacy intrusion (II)	Emails sent and received by PROVIDER users cannot be read by third parties.

Table 1. Operationalization of independent.

To investigate the causal relation between a textual priming stimuli and participants' privacy concerns we adapted the App Information Privacy Concern (AIPC), which is based on central measurement instruments for information privacy concerns in the existing literature [9]. It builds upon the Concern For Information Privacy (CFIP) [34], the Internet Users' Information Privacy Concerns (IUIPC) [26], the Mobile Users' Information Privacy Concerns (MUIPC) [42], and the Global Information Privacy Concern (GIPC) of Smith et al. (1996)) and is applied in the context of apps. Because 17 items are not appropriate for an experimental study, as answering that much questions somehow forces participants to high-effort processes, we reduced the items on a 3+1 item group. Drawing upon the results of previous investigations regarding the validation of the construct "privacy concerns", we established privacy concerns as a second-order latent reflective factor. Consequently, the first-order constructs (1) "awareness" and (2) "collection" from Malhotra et al. [26] and the variable (3) "perceived intrusion" from Xu et al. [42] reflect the users' privacy concerns. To measure the (4) "general information privacy concern" of users, we followed Smith et al. [34] and adapted the variable of Malhotra et al. [26, 34]. The items were translated to German and adapted for digital services and goods. Consequently, we propose that the consumer's privacy concerns regarding email services will be shaped by the variables "awareness", "collection", and "perceived intrusion".

No.	Items – 3-item privacy concern	Source
1	It is very important to me that I am aware and well informed about how my personal information is used.	[26]
2	Normally it annoys me when digital services ask me for personal information.	[26, 34, 42]
3	I feel that due to the use of digital services, personal information about me is on the market that, when used, invades my privacy.	[26, 42]
General Information Privacy Concern		
4	Compared to other people, I'm more sensitive to how digital service providers handle my personal information.	[26, 34]

Table 2. Operationalization of dependent variable.

To address the research question we conducted an online experiment using a one factorial-subject design. Participants were randomly assigned to either one of the treatment groups or the control group.

3.2. Data collection and descriptive results

The experiment was conducted as an online experiment from May 2019 to June 2019. The participants were students from a German university. The experiment was conducted by personally addressing students before their lectures. The (same) experimenter gave a short and always similar introduction about the conducted experiment. Following this, the experimenter encouraged the participants to enter a short-URL to get access to the study with their smartphone. Thus, we aimed to exclude the experimenter bias and to ensure independent samples.

After the personal introduction, the participants gained access via a short-URL and were forwarded to a website designed and provided with the software Qualtrics. When the participants were forwarded to the website, they were shown a short welcome site and after that asked which email provider they use. After the self-categorization by email provider, the participants were exposed to the textual priming stimulus, which they were asked to read. Subsequently, the participants were asked to answer the three items of the context adapted privacy concern and the additional item about their "general information privacy concerns". Accordingly, the experiment was conducted as an anonymous online experiment.

276 (n=276) participants were in the study. After deleting questionnaires which contained incomplete returns, 241 (n=241) data sets were included in the analysis. The participants were randomly distributed to the three groups: 88 participants (n=88) in treatment I (possible privacy intrusion), 70 participants (n=70) to the treatment II (no privacy intrusion) and 83 participants (n= 83) to the control group (no stimulus). The mean value (MV) of participants' age was 22.58 (SD=6.158). Of the remaining participants, 36.1% (n=87) were female, 62.2% were male (n=150), and 1.7% were non-binary (n=4). 67 (n=67) participants used Google mail and 172 (n=172) used other email accounts (2 missing values).

In this study we distinguish between users of Gmail and users of other email accounts based on one differentiation. Only Google has publicly admitted that emails sent and received by Googlemail users may sometimes be read by real people at third-party providers – not just machines; which corresponds to the textual priming stimulus used in this study for privacy intrusion. Due to this announcement, which attracted a lot of media attention, a different degree of sensitivity for privacy can be assumed between users of Googlemail and users of other email accounts.

The descriptive results of the study are shown in Table 3.

Participants	n=241
Female	n=87
Male	n=150
Non-binary	n=4
Users of Gmail	n=67
Users of other email accounts	n=172
Treatment I	n=88
Treatment II	n=70
Control Group	n=83
Age	MV 22.58 (SD=6.158)

Table 3. Descriptive results.

3.3. Group analysis and results

In order to evaluate the data according to the research question, different levels of analysis were chosen. We followed the classical experimental analysis [6, 32, 39]. We compared mean values (MV) by a one-way ANOVA of the treatment group I, the treatment group II and the control group regarding their 3-item privacy concerns and their General Information Privacy Concern. Furthermore, we compared mean values (MV) by t-test of the experimental group (exposed to a stimulus) and the

control group regarding their 3-item privacy concerns and their general information privacy concern. To get a deeper understanding of the underlying effects, we additionally analyzed the data on a single-item level. The analysis was done for the complete data set, for the sub-group of Gmail users, and the sub-group of users of other email accounts. Differences on a 95% confidence interval were reported as significant results. Differences on a 90% confidence interval were characterized as not significant (n.s.). We also reported their values as these results can serve as interesting tendencies.

Complete data set

From a perspective of the whole data set, no significant differences (n.s.) between the two treatment groups and the control group could be identified, neither for the 3-item privacy concerns [$F(2, 238) = 2.824$, $p = .061$], nor for the general information privacy concern [$F(2, 238) = .9$, $p = .408$].

In a grouping of the data into the distinction between treatment group and control group, differences on a 90% confidence interval show both at the level of the 3-item concern and at the level of the single-item perceived intrusion (item no. 3). The results regarding the complete data set are shown in Table 3.

Complete data set	Experimental vs. control
3-item privacy concern	(n.s.); $p<0.1$; $t(241)=1.865$; $p=.064$
1	(n.s.)
2	(n.s.)
3	(n.s.); $p<0.1$; $t(241)=1.702$; $p=.091$
4	(n.s.)

Table 3. Results of complete data set (experimental vs. control).

When considering the female participants in the experiment, no significant differences between the three groups can be identified, neither for the 3-item privacy concerns [$F(2, 84) = 2.974$, $p = .057$], nor for the general information privacy concern [$F(2, 84) = 1.544$, $p = .220$].

Significant differences, however, can be detected in the women subgroup when comparing the experimental group and the control group. Both the 3-item concern and the single-item perceived intrusion show significant differences (see Table 4).

Complete data set	Female Experimental vs. control
3-item privacy concern	$p<0.05$; $t(87)=2.393$; $p=.020$
1	(n.s.)
2	(n.s.)
3	$p<0.01$; $t(87)=3.157$; $p=.002$
4	(n.s.); $p<0.1$; $t(87)=1.947$; $p=.055$

Table 4. Results of complete data set (experimental vs. control) for female.

No significant differences between the three groups could be observed in the subgroup of male, neither for the 3-item privacy concerns [$F(2, 147) = 1.396$, $p = .251$], nor for the general information privacy concern [$F(2, 147) = .502$, $p = .606$]..

In the differentiation between the experimental group and the control group, the 3-item-concern shows results on a 90% confidence interval (see Table 5).

Complete data set	Male Experimental vs. control
3-item privacy concern	(n.s.); $p<0.1$;$t(99)=1.783$; $p=.078$
1	(n.s.)
2	(n.s.)
3	(n.s.)
4	(n.s.)

Table 5. Results of complete data set (experimental vs. control) for male.

Users of Gmail

When considering the group of Gmail users, no significant differences can be detected between the three groups, neither for the 3-item privacy concerns [$F(2, 64) = .193$, $p = .825$], nor for the general information privacy concern [$F(2, 64) = .368$, $p = .694$]. No significant differences could be identified when isolating genders, either.

Users of other email accounts

When considering the group of users of other email accounts, significant differences can be observed. With regard to the group comparison, significant differences can be identified on the level of the 3-item concern as well as on the level of the single-items collection and perceived intrusion (see Table 6).

Other email acc.	Female & Male
3-item privacy concern	F(2, 169) = 4.708, p = .010
1	(n.s.)
2	F(2, 169) = 3.421, p = .035
3	F(2, 169) = 3.197, p = .043
4	(n.s.)

Table 6. Results of users of other email accounts.

A comparison of the results between the experimental group and the control group reveals considerable differences, as shown in Table 7. Significant differences can be identified at the 3-item privacy concern, as well as for the single-item perceived intrusion.

Other mail-acc.	Female & Male Experimental vs. control
3-item privacy concern	p<0.05;t(113)=2.422; p=.017
1	(n.s.); p<0.1;t(113)=1.804; p=.074
2	(n.s.)
3	p<0.05;t(113)=2.342; p=.021
4	(n.s.); p<0.1;t(113)=1.758; p=.081

Table 7. Results of users of other email accounts (experimental vs. control).

Looking at the female participants in the study from the subgroup of users of other email accounts, an interesting picture emerges. Differences between the three groups appear for the 3-item privacy concern and the single-items collection and perceived intrusion, as shown in Table 8.

Other email acc.	Female
3-item privacy concern	F(2, 68) = 4.152, p = .020
1	(n.s.)
2	(n.s.)
3	F(2, 68) = 6.501, p = .003
4	(n.s.); F(2, 68) = 2.859, p = .064

Table 8. Results of female users of other email accounts.

Furthermore, significant and highly significant differences can be identified in the distinction between the experimental group and the control group (see Table 9).

Other mail-acc.	Female Experimental vs. control
3-item privacy concern	p<0.01;t(71)=2.806; p=.007
1	(n.s.); p<0.1;t(71)=1.692; p=.099
2	(n.s.)
3	p<0.01;t(71)=3.830; p=.000
4	p<0.05;t(71)=2.590; p=.012

Table 9. Results of female users of other email accounts (experimental vs. control).

A contrasting picture emerges when looking at the male study participants in the subgroup of users of other email accounts. No significant differences between the three groups can be identified, neither for the 3-item privacy concerns [F(2, 97) = 1.560, p = .215], nor for the general information privacy concern [F(2, 97) = .300, p = .741]. No significant differences were found in the differentiation between experimental group and control group.

4. Interpretation and discussion

In the introduction we posed the research question: Do textual priming stimuli have an influence on the privacy concerns of users of information systems?

To answer this question, we presented an online experiment providing the influence of textual stimuli on information privacy concerns. With the experiment we provide both an independent variable derived from what we observed in the context of private email accounts and a shortened privacy concern as a dependent variable which is appropriate for low effort driven experimental research.

An interesting result is the massively different reaction of users of the Gmail service and users of other email services. Users of Gmail, for example, do not show any significant differences between the different groups - neither in the differentiation of the three main groups nor in the discrimination of the gender. However, users of other email services show a completely opposite picture. They show significant and sometimes highly significant differences between the different groups.

A possible explanation of these interesting results can be derived on several levels. For one thing, users of Google's services may have lower privacy expectations – especially about Google's services – and may therefore not respond to the stimuli presented. They may be more accustomed to exchanging data for

digital services. In addition, users of other email services may have greater confidence in their provider and therefore react more sensitively to the stimuli.

This can lead to two perspectives for explaining the results. On the one hand, users of Google services may be more digital per se. They are used to navigating in digital environments and have a higher awareness of their privacy calculus. On the other hand, a higher degree of resignation can also explain the results. For example, it is conceivable that users of Google services have already resigned and see no real chance of protecting their privacy in digital systems. They may therefore have already surrendered more to their fate of losing privacy, since the only alternative is not to use the digital services.

Another interesting result is the more pronounced effect in the group differentiation between the experimental group and the control group. Thus, the variation of the stimulus in the treatment group leads to a weaker effect than the differentiation between experimental group and control group. This can be interpreted by the fact that the mere idea that third parties read the email account leads to higher data protection concerns. Consequently, the mere discussion of the issue leads to an increase in data protection concerns.

5. Limitations and further research

The experiment is subject to several limitations due to the nature of our research. Firstly, the sample is not representative for Germany, nor the worldwide users of email accounts. Furthermore, it does not consider culturally bound issues. By addressing specific lectures for the data collection, we also limited our validity in terms of a deficit of randomization. An additional limitation lies in the field of the context of email accounts, which also limits the generalizability of the findings for the use of IS. Beyond that, we do not know much about the predispositions of our participants, e.g. their relationship to the provider, their level of integration of their provider, or their personal dispositions like their level of literacy or their previous experiences with privacy-related decision situations. Further, 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. It has been taken into account that privacy concerns do not necessarily lead to actual behaviors. Moreover, the contextual dependence is an important factor when it comes to information privacy [7, 27, 33]. Therefore, it is likely that individuals have divergent privacy concerns depending on which apps they use. They might have high concerns regarding health and banking apps but could have lower concerns while using gaming or news apps. In addition, we query privacy concerns directly with the dependent variable. This can lead to socially desirable answers and distort the results.

This experiment represents a first step towards the experimental investigation of privacy-related questions and thus directly takes up the call for research by Dinev et al. (2015 and Goes (2013) [12, 15]. Already at a low-threshold level of priming stimuli, significant and sometimes highly significant effects on privacy concerns can be identified. This leads to the assumption that numerous cause-effect mechanisms, which may be based on behavioral economics and social psychology, influence the behavior of individuals in IS.

From the perspective of a new user of information systems, the insights of related disciplines must also enter the domain of IS. With the increasing integration of IS in the everyday life of users, it is essential to research and understand digital consumer behavior. Only in this way can new applications and systems be developed and effective consumer protection achieved.

6. References

[1] Acquisti, A., "Nudging Privacy: The Behavioral Economics of Personal Information", IEEE Security and Privacy Magazine, 7(6), 2009, pp. 82–85.

[2] Acquisti, A., L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information", Science (New York, N.Y.), 347(6221), 2015, pp. 509–514.

[3] Adjerid, I., E. Peer, and A. Acquisti, "Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making", 2016/04/16.

[4] Akerlof, G.A., "The market for "lemons": Quality uncertainty and the market mechanism", The quarterly journal of economics, 84(3), 1970, pp. 488–500.

[5] Ariely, D., "The End of Rational Econonmics", Harvard business review, 87(7/8), 2009, pp. 78–84.

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

[7] Bélanger, F. and R.E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems", MIS Quarterly, 35(4), 2011, 1017-A36.

[8] Bennett, C.J., "The political economy of privacy: a review of the literature", Center for Social and Legal Research, 1995.

[9] Buck, C. and S. Burster, "App Informations Privacy Concerns", AMCIS 2017 proceedings, 2017.

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

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

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

[13] Gerlach, J., T. Widjaja, and P. Buxmann, "Handle with care: How online social network providers' privacy policies impact users' information sharing behavior", The Journal of Strategic Information Systems, 24(1), 2015, pp. 33–43.

[14] https://www.bbc.com/news/technology-44699263.

[15] Goes, P.B., "Editor's comments: information systems research and behavioral economics", MIS Quarterly, 37(3), 2013, pp. iii–viii.

[16] Gravetter, F.J. and L.-A.B. Forzano, Research methods for the behavioral sciences, 5th edn., Cengage Learning, Stamford, CT, 2016.

[17] Grossklags, J. and A. Acquisti, "What Can Behavioral Economics Teach Us about Privacy?", 2, pp. 363–377.

[18] Hirshleifer, J., "Where Are We in the Theory of Information?", The American Economic Review, 63(2), 1963, pp. 31–39.

[19] Hong, W. and J.Y.L. Thong, "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies", MIS Quarterly, 37(1), 2013, pp. 275–298.

[20] Kahneman, D., Thinking, fast and slow, Penguin Books, London, 2012.

[21] Kehr, F., T. Kowatsch, D. Wentzel, and E. Fleisch, "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus", Information Systems Journal, 25(6), 2015, pp. 607–635.

[22] Kokolakis, S., "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", Computers & Security, 64, 2017, pp. 122–134.

[23] Kordzadeh, N. and J. Warren, "Communicating Personal Health Information in Virtual Health Communities: A Theoretical Framework", in IEEE 8th International Symposium on Service-Oriented System Engineering (SOSE), 2014: 7 - 11 April 2014, Oxford, United Kingdom ; [including workshop/simposium papers, 2014 47th Hawaii International Conference on System Sciences (HICSS), Waikoloa, HI, 1/6/2014 - 1/9/2014. 2014. IEEE: Piscataway, NJ.

[24] Lee, L., O. Amir, and D. Ariely, "In Search of Homo Economicus: Cognitive Noise and the Role of Emotion in Preference Consistency", Journal of Consumer Research, 36(2), 2009, pp. 173–187.

[25] Li, Y., "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework", Communications of the Association for Information Systems, 28, 2011.

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

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

[28] Norberg, P.A., D.R. Horne, and D.A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", Journal of Consumer Affairs, 41(1), 2007, pp. 100–126.

[29] Ozdemir, Z. d., H. Jeff Smith, and J.H. Benamati, "Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study", European Journal of Information Systems, 26(6), 2017, pp. 642–660.

[30] Pavlou, P.A., "State of the information privacy literature: Where are we now and where should we go?", MIS Quarterly, 35(4), 2011, pp. 977–988.

[31] Samson, A. and G. Loewenstein, The Behavioral Economics Guide, 2014.

[32] Schwarz, N., H. Bless, F. Strack, G. Klumpp, and al et, "Ease of retrieval as information: Another look at the availability heuristic", Journal of Personality and Social Psychology, 61(2), 1991, pp. 195–202.

[33] Smith, H.J., T. Dinev, and H. Xu, "Information Privacy Research: An Interdisziplinary Review", MIS Quarterly, 35(4), 2011, pp. 989–1015.

[34] Smith, H.J., S.J. Milberg, and S.J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", MIS Quarterly, 20(2), 1996, p. 167.

[35] Solove, D.J., "A taxonomy of privacy", University of Pennsylvania Law Review, 154(3), 2006, pp. 477–564.

[36] Spiekermann, S., A. Acquisti, R. Böhme, and K.-L. Hui, "The challenges of personal data markets and privacy", Electronic Markets, 25(2), 2015, pp. 161–167.

[37] Spiekermann, S. and J. Korunovska, "Towards a value theory for personal data", Journal of Information Technology, 32(1), 2017, pp. 62–84.

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

[39] Tversky, A. and D. Kahneman, "The framing of decisions and the psychology of choice", Science, 211(4481), 1981, pp. 453–458.

[40] Varian, H.R., "Economic Aspects of Personal Privacy", in Internet Policy and Economics, L.M. Pupillo and W.H. Lehr, Editors. 2009. Springer: Dordrecht.

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

[42] Xu, H., S. Gupta, M. Rosson, and J. Carroll, "Measuring Mobile Users' Concerns for Information Privacy", ICIS 2012 Proceedings, 2012.

[43] Yoo, "Computing in Everyday Life: A Call for Research on Experiential Computing", MIS Quarterly, 34(2), 2010, p. 213.

[44] Yu, J., P.J.-H. Hu, and T.-H. Cheng, "Role of Affect in Self-Disclosure on Social Network Websites: A Test of Two Competing Models", Journal of Management Information Systems, 32(2), 2015, pp. 239–277.