Research Center
Finance & Information Management

Fraunhofer FIT
Project Group
Business & Information
Systems Engineering

Stop Disclosing Personal Data about Your Future Self

by

Christoph Buck

to be presented at: 23th Americas Conference on Information Systems (AMCIS),
Boston, USA, August 2017

University of Augsburg, D-86135 Augsburg
Visitors: Universitätsstr. 12, 86159 Augsburg
Phone: +49 821 598-4801 (Fax: -4899)

University of Bayreuth, D-95440 Bayreuth
Visitors: Wittelsbacherring 10, 95444 Bayreuth
Phone: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

WI-688

Stop Disclosing Personal Data about Your Future Self

Full Paper

Christoph Buck
University of Bayreuth
christoph.buck@uni-bayreuth.de

Abstract

Personal data is becoming more and more valuable because of new possibilities in gathering and analyzing data. Although, users integrate information systems in their most private spheres, they do not take adequate care of their privacy. In fact, they are becoming increasingly concerned about their information privacy, but act in a different way. This inconsistency in users' behavior is known as privacy paradox. This paper takes up the psychometric measurement of future self-continuity and investigates the relationship to selected constructs of information privacy research. The results show significant correlations to the concerns users have about their privacy – an increasing future self-continuity is related with higher concerns. Thus, users should be aware of the implications their current disclosure of personal data have on their future self.

Keywords

Information privacy, privacy paradox, future self-continuity, enhanced APCO model.

Introduction

Privacy and personal data are called the new oil of the 21st century. According to the World Economic Forum, plenty of researchers argue that personal data is becoming a commodity and is seen as a new asset class (Bennett 1995; Spiekermann et al. 2015; World Economic Forum 2011). The increasing valuation of personal data is associated with the mass adoption of private computing devices and the ongoing integration of information systems in users' everyday life. This everyday life integration leads to a paradox situation regarding the possibility to gather personal data and users' attention concerning the disclosure of personal data: the more useful information systems are integrated in everyday life, the more invisible they are. This implies that the most valuable data is achieved in the most private sphere. Consequently, "Cyberspace is invading private space" (Clarke 1999: 60). As the pocket knife of communication, smart mobile devices (SMD) possess a vast amount of connected sensors and functions. With about two billion smartphone users and more than 175 billion app downloads SMD and mobile applications (apps) are the most common user interface of information systems in mass markets (eMarketer 2016; Statistic Brain 2016). Apps are integral to the functioning of SMD like smartphones or tablets and are key elements for the interface design and functionality. Apps can be interpreted as the embodiment of ubiquitous computing, i.e. the creation of environments saturated with computing and communication capability, integrated with human users (Weiser 1991). Software in the form of apps diffused in the everyday life of users. Throughout these functions, the possibilities of gathering personal data are virtually endless.

With this mass adoption and the increasing possibilities of gathering personal information privacy concerns of users raised, too. This leads to inconsistencies in users' behavior, the so-called privacy paradox which gained broad attention in the literature (Norberg et al. 2007). The privacy paradox describes that individuals' actual information disclosure significantly exceeded the intention to disclose this information. Whereas extensive research was carried out in the field of the privacy paradox to date, no comprehensive explanation evolved (Kokolakis 2015).

Not at least because of a popular call for research from Dinev et al. (2015), IS scholars started to integrate the perspectives of behavioral economics and social psychology into their research. SMD and apps are a

broad field of research for the application, adaption and further development of insights of related domains due to their nature as socio-technical systems.

Therefore, this paper introduces a new perspective and psychometric measurement to the field of IS and information privacy. The presented study poses a first attempt to use the theory of future self-continuity in information privacy research. The model of Smith et al. (2011) and its enhanced version of Dinev et al. (2015) concerning Antecedents, Privacy Concerns, Outcomes (APCO) is extended with future self-continuity as an antecedent for privacy concerns, perceived risk and need for regulation. The results of the study show some significant correlations between the observed constructs, which reveals the approach as a valuable research instrument for further research in information privacy.

This paper is structured as follows. In the next section the theoretical foundations regarding information privacy, the privacy paradox, the enhanced APCO model, and the integration of future self-continuity are posed. The following section starts with the study design. Subsequently, the data collection and the results of the correlation analysis are presented. The paper ends with a conclusion and further research.

Theoretical Foundations

Information Privacy and its Value in the Context of Mobile Applications

Since privacy is addressed in many fields of social sciences and different definitions are used in various areas of everyday life, it lacks a holistic definition (Smith et al. 2011; Solove 2006). First, physical and information privacy have to be distinguished. Physical privacy relates to the "access to an individual and/or the individual's surroundings and private space" (Smith et al. 2011: 990). Contrary, information privacy only refers to information that is individually discernable 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: 990). Even though privacy has developed and changed drastically over the last decades, Westin's definition still holds true: he defines information privacy as "the claim of an individual to determine what information about himself or herself should be known to others" (Westin 2003: 431). Following Westin, 'control' is construed as an instrument of the protection of privacy. Privacy itself is often defined as the control over personal information (Solove 2006). Consequently, in this paper information privacy is defined as the ability to control the acquisition and use of one's personal information (Westin 1967).

Apps as the most common user interface of information systems are a suitable object of investigation because of their broad diffusion in the mass market and in users' everyday life. 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 like iOS and Android (Buck et al. 2014). Consequently, apps, as the most common user interface for digitized solutions (e.g. smart services, smart homes, wearables, etc.), layer everyday activities and lives in a digital way; or how Clarke rephrased it: "Cyberspace is invading private space" (Clarke 1999: 60). In app markets, users are able to control their privacy disclosure during the purchasing process. Thus, users can actively control their disclosure of personal data and the grasping of privacy from third parties (Chen and Chen 2015). This paper treats personal information and personal data as equal. I will keep the following principle throughout the remainder of this article: I will use the term privacy as a reference to information privacy, which is my immediate focus.

Dinev and Hart (2006: 61) stated that privacy "is a highly cherished value, few would argue that absolute privacy is unattainable." Privacy as digital personal information and highly personalized data collected via apps has a huge economic value (Acquisti et al. 2015). Derived from the perspective of personal data and privacy as a commodity, many researchers conceive privacy as a tradeable good or asset (Bennett 1995; Spiekermann et al. 2015). 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 society (Smith et al. 2011).

When the measurement of the (perceived) value of users' information privacy is observed, the theory of the privacy calculus has to be considered (Culnan and Armstrong 1999). Therefore, users are supposed to undertake an anticipatory, rational weighing of risks and benefits when confronted with the decision to disclose personal information or make transactions (Malhotra et al. 2004; Pavlou 2011; Xu et al. 2012).

The privacy calculus model assumes a correct and objectified understanding of the monetary value of privacy and therewith users' tangible willingness to pay for privacy (Dinev et al. 2015; Norberg and Horne 2007).

The Privacy Paradox

There are several explanations why it is difficult for individuals to assess privacy decisions according to the privacy calculus. Firstly, individuals suffer from uncertainty due to incomplete and asymmetric information. Taking the paradigm of experiential computing into account, the value of privacy increases with the (perceived) invisibility of the connected devices (Yoo 2010). With the increasing everyday life integration, devices and sensors become more and more invisible, but are an increasingly self-evident part of users' daily routine. Because of the establishment in users most intimate privacy sphere, users' awareness regarding their information privacy is affected in a paradox way. Consequently, individuals are frequently not aware of the information available to third parties, how that information is used and what consequences it might have (Acquisti et al. 2015). Secondly, to evaluate benefits and risks, individuals need to be aware of their preferences. However, research has shown that individuals are often not able to evaluate how much they like certain products or services and thus have little sense of their preferences (Slovic 1995). Privacy does not seem to be an exception for it as IS researchers have discovered a dichotomy between attitude towards privacy and privacy behavior (Chellappa and Sin 2005; Hann et al. 2007). Individuals who claim to have high privacy concerns and no intention to give away personal information, disclose it despite their attitude (Acquisti and Grossklags 2004). This inconsistency, the so-called privacy paradox (Norberg et al. 2007), received scholars' broad attention. To date, there is no comprehensive explanation for it (Kokolakis 2015).

In the literature, the privacy paradox is usually described by the dichotomy between privacy attitudes and privacy behavior. However, researchers often measure the differences between privacy concerns and privacy behavior (Kokolakis 2015). Nonetheless, the results on the privacy paradox are contradictory and several studies have shown the described dichotomy between privacy concerns and attitudes and privacy behaviors (Grossklags and Acquisti 2007; Hann et al. 2007; Norberg et al. 2007). Others did not support the dichotomy and argue that privacy behavior is in line with the overserved concerns and attitudes. This controversy is due to different interpretations, different research methodologies as well as the fact that the privacy paradox has been studied in various context (Kokolakis 2015). Owing to the fact that privacy behavior is a very contextual phenomenon (Morando et al. 2014).

Different theoretical backgrounds have been applied to investigate and to find explanations for the discovered gap between privacy attitudes and privacy behavior. Research from various disciplines including social theory, behavioral economics, psychology and quantum theory have contributed to the conceptualization of the phenomenon. The largest research part lies in the field of behavioral economics and the psychological perspective containing cognitive biases and heuristics (Acquisti et al. 2015; Acquisti and Grossklags 2005; Acquisti and Grossklags 2008; Brandimarte et al. 2012). Drawing from all findings from the various studies, the paradox should not be considered as paradox anymore. Due to uncertainties, individuals use heuristics and other cognitive cues when making privacy trade-offs to form their decision. Because of the contextual dependence of privacy preferences individuals show systematic inconsistencies, but no irrational behavior (Acquisti 2012; Acquisti et al. 2015). Thus, it is a complex phenomenon that yet has not been explained holistically and therefore needs further investigation (Kokolakis 2015).

Extending the APCO Model with Future Self-Continuity

So far, IS research, with the APCO model as a reflection of the majority of existing empirical privacy research, assumes that privacy-related behaviors are represented by deliberate, high effort processes (Bélanger and Crossler 2011; Li 2011; Smith et al. 2011).

The enhanced APCO model, shown in figure 1, is made up of three main components: the antecedents (A), the privacy concerns (PC), and the outcomes (O). The center of the model are privacy concerns which have emerged as a basic variable of measuring privacy in privacy research (Bélanger and Crossler 2011; Li 2011; Smith et al. 2011). 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 terms such as beliefs, attitudes and perceptions are used,

the underlying measurements are generally privacy concerns (Smith et al. 2011). There is no universal definition for privacy concerns. However, in general it refers to the "degree to which an individual perceived a potential loss associated with personal information" (Pavlou 2011: 981). There is a vast body of literature between privacy concerns and privacy outcomes, the right-hand side of the model. Outcomes represent the relationship between privacy concerns as independent variable and other constructs like behavioral reactions, trust, regulation, and the privacy calculus as dependent variables (Smith et al. 2011). The left-hand side of the model represents antecedents which have a direct impact on privacy concerns as dependent variable. Summarizing, there are antecedents that influence or shape individual's privacy concerns which in turn have impact on outcomes like trust and vice versa (Smith et al. 2011).

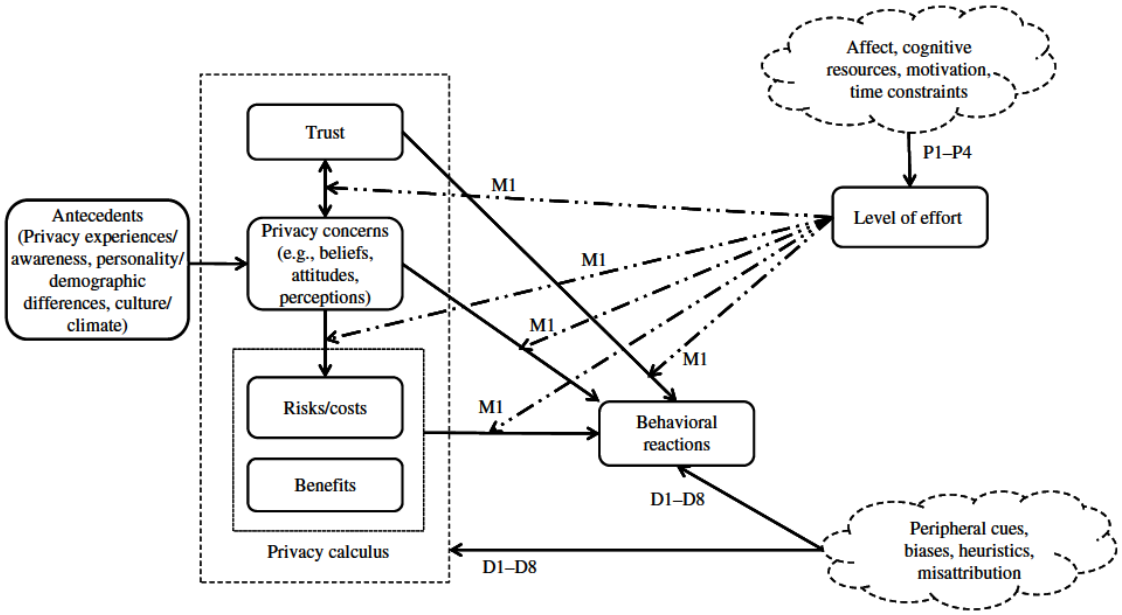

Figure 1. Enhanced APCO Model (Dinev et al. 2015)

Taking the mass adoption of modern IS as socio-technical systems and the new user in experiential computing into account, the current state of IS research does not sufficiently incorporate the existing knowledge of behavioral economics and social psychology. The existing models are overlooking the fact that individuals generally do not fully reflect their behavior regarding privacy options and therefore do not exhaustively reflect the status quo of information privacy research. Dinev et al. (2015) criticized this assumption of neo-classical theory and used the APCO model as a groundwork to proposed enhancements in privacy research. The main additions to the APCO model are two clouds which both influence privacy-related attitudes and behaviors (Dinev et al. 2015). The behavioral reactions are affected by extraneous influences represented by the lower cloud. Extraneous influences stand for peripheral cues, biases, heuristics, as well as misattributions. It has been found that those have a major impact on the privacy-related attitudes and behaviors lacking of cognitive effort (Dinev et al. 2015). The second cloud represents situational and cognitive limitations which do not have a direct influence on the model, but are moderated by the level of effort, which is determined by situational and cognitive limitations. Low-effort processing does not need to be determined by only one of the factors, it can also be a combination of them. It is proposed that low level processing does interfere with the linkages of the different constructs of the model.

However, existing literature and the model of Dinev et al. (2015) predominantly call attention to the PCO (Privacy Concerns and Outcomes) of the model - the middle and left part of figure 2. Only little attention has been paid on the insights of behavioral economics and social psychology regarding the left side (antecedents) of the APCO model. Taking into account that personal information, especially regarding the download and use of apps, on the one hand is a highly valuable asset, but on the other hand cannot be estimated by the users, it is questionable why users download (anonymous) apps in this vast amount.

Whereas researchers pointed out that users tend to hyperbolic discounting when weighing up todays consumptions against future losses (Acquisti and Grossklags 2004; Dasgupta and Maskin 2005; Rubinstein 2003), this paper suggests a new perspective and classification on users and their dealing with information privacy.

The careless disclosure of personal data today can have a huge negative impact for the situation of one's future self. Health insurances can be seen as an impressive example for the future impact of today's data disclosure. If a user tracks his data by health and fitness apps and shows up with unhealthy and unsustainable behavior for a long period, her future self could be charged by higher dues or even lose her insurance protection. Similar consequences can be assumed in various fields of users' everyday life. In an extreme case, data aggregators could publicly offer one's whole data history to the market: including all personal secrets and mysteries. To get back her privacy, she has to redeem the data history at potentially high costs.

In view of the fact that users' personal information can have impact on their future decisions and that users are not able to assess this circumstance in their current decision-making situations, the theory of future self-continuity is introduced. Future self-continuity is one of the most enduring mysteries regarding the personal identity which takes up the idea how users deal with their future self (Ersner-Hershfield et al. 2009a; Ersner-Hershfield et al. 2009b). According to the philosophical view, it is possible that users consider their future self as different people. If doing so, they "may have no more reason to reward the future self than to give resources to strangers" (Ersner-Hershfield et al. 2009a: 280). In other words: "the more connected you become with your future self, the more you will incorporate it into your present self-conception" (Mischel, 2014: 128-129). Assigned to the health insurance example, a user who is more emotionally in touch and identified with her future self, will carefully disclose personal data.

Therefore, Ersner-Hershfield et al. (2009a) developed a psychometric measure of future self-continuity which predicts "that people who experience no continuity with a future self should not save for that future self" (Ersner-Hershfield et al. 2009a: 280). Assigned to the domain of privacy and the ongoing discussion regarding the privacy paradox, the future self-continuity is an additional antecedent in the enhanced APCO model. Not disclosing or carefully disclosing personal data can be seen as caring for the future self of the user. Hence, the future self-continuity of app users represents an antecedent of the APCO model and should have impact on the dependent variables (see grey boxes in figure 2).

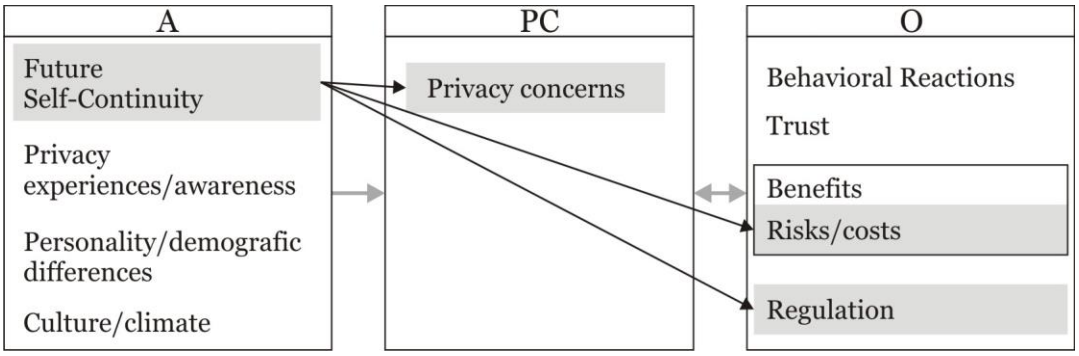

Figure 2. Simplified APCO Model with Future Self-Continuity (Smith et al. 2011).

More precisely, future self-continuity should have an impact on variables which are associated with the evaluation and disclosure of personal data. Following current literature, the privacy concerns should be directly affected by future self-continuity as an antecedent. The provided privacy concern is derived from existing research in privacy concerns. To acknowledge for the contextual dependence of privacy, the existing items of the Internet User Information Privacy Concern (IUIPC) and the Mobile Users Information Privacy Concern (MUIPC) which are based on the Concern for Information Privacy were developed for the field of smart mobile devices (SMD) and apps (Malhotra et al. 2004; Smith et al. 1996; Xu et al. 2012). A 17-item construct was developed which contains three second-order constructs: personal attitude, anxiety and requirements. Since the investigation was a first attempt in the field and

the concept of future self-continuity addresses the emotional connectedness of one's future self, the items requirement were not used. Nevertheless, the two first-order constructs anxiety and personal attitude with a total of 12 items were provided. Anxiety is defined as the degree to which a person is concerned about the usage and processing of the collected personal data via mobile apps. Personal attitude specifies how important it is for a person to protect her personal data and how much she is aware of it. Since privacy concerns are seen as a proxy for measuring privacy, it is hypothesized that a low future self-continuity is related to low privacy concerns.

Contrary to the supposed effects of the APCO model, the study additionally investigates direct effects of future self-continuity as antecedents on regulation and perceived risk as outcomes. Users of apps act in a system with very high information asymmetries. Viewing personal information as an economic good in app markets, it underlies asymmetric information and therefore relates to problems of adverse selection and moral hazard (Pavlou 2011). This means that ex ante individuals do not know who follows appropriate information protection and ex post if their personal information will be used in an appropriate manner (Acquisti and Grossklags 2008). This is highlighted by the different understanding of personal data which makes it non-transparent for the individual. Consequently, the perceived risk when downloading and using apps is a relevant construct. The construct was operationalized literature-driven. The three items product risk, financial risk, and overall risk were developed from existing literature (Jarvenpaa et al. 2000; Kim et al. 2008). One item regarding privacy risk was newly developed. Regarding the relationship towards future self-continuity, it is hypothesized that a low future self-continuity is related to low perceived risks.

In addition to privacy concerns and risk perception a handover of responsibility could be associated with the mental overload users are exposed when evaluating their privacy in mobile ecosystems. If users do not perceive the app provider as trustworthy, they will distrust self-regulation (Milberg et al. 2000). This can eventually lead to a regulatory response (Smith et al. 2011). Regarding the relationship towards future self-continuity it is hypothesized that a low future self-continuity is related to high needs for governmental regulation and low needs of app providers' self-regulation regarding the handling of personal data which represent the two provided items (Smith et al. 2011).

Investigating Future Self Continuity and Information Privacy

Study Design

An online survey was conducted to investigate the mentioned relationships. Undergraduates from a German university voluntarily participated via an online survey before the lecture started. After the welcome the participants were asked a filter question whether they own or do not own a smart mobile device (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, are essential for valid responses (Payne et al. 1999). Subsequently, the future self-continuity estimation by Ersner-Hershfield et al. (2009) took place which provides a high validity in predicting the valuation of future rewards (the extreme characteristics of the measurement are shown in figure 3).

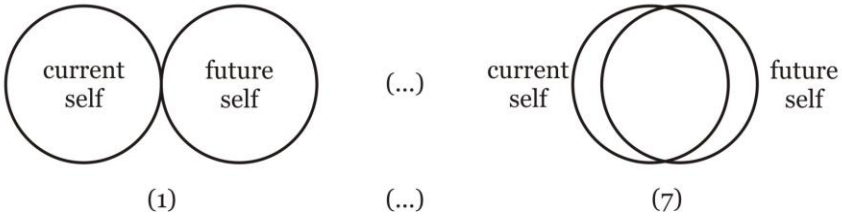

Figure 3. Extreme Characteristics of Scales for Measuring Future Self-Continuity

Therefore, the participants were subsequently asked to think about their current self, about a stranger, and about their future self (in ten years) (Ersner-Hershfield et al. 2009a). To ensure a minimum of attention, the screens were blocked for 15 seconds. After that the participants were asked to rate their future self-continuity. For that reason, the 7-point Lickert-scale from Ersner-Hershfield et al. (2009) was

applied. The seven scale points are represented by two overlapping circles. The overlap was designed with two circles from no overlap (1) up to a high level of overlap (7). Figure 3 provides the turning points of the given scale. Participants had to decide the correspondence of their current and future self by choosing the appropriate pair of circles. A "no opinion" option was available so that responses were not forced.

After the measurement of the future self-continuity the participants were randomly assigned to the three constructs: privacy concerns (12 items; 2 first-order constructs), perceived risk (4 items), and regulation (2 items). The survey ended with socio-technical questions (gender, age, profession, SMD-brand).

Data Collection and Results

The study was conducted as an online-based survey in the second week of February 2017 with business economics undergraduate students in an IS-related lecture. 168 (n=168) participants attended the study. After deleting questionnaires which contained non-smartphone users, incomplete questionnaires, and outliers, 144 (n=144) data sets were included in the subsequent analysis. The average age of participants was 20.4 years (SD=2.05). The age of participants' ranges from 18 to 28 years (M=20.15; SD=1.88). Of the remaining participants, 56.0% (n=84) were female and 44.0% were male (n=66). 80 (n=80) of the participants used Apples operating system (OS) iOS and 70 (n=70) used other operating systems. Bivariate correlation analysis was performed for the different groups. Every variable was normally distributed. Spearman's correlation coefficient was chosen because of the 7-point Likert-scale measurment. Bias corrected and accelerated bootstrap 95% CIs are reported in square brackets.

In the privacy-concern-group (n=52) the average age of these participants was 20.31 years (SD=1.93). The age of these participants ranges from 18 to 28 years (M=20.31; SD=1.93). Of the remaining participants, 53.8% (n=28) were female and 46.2% were male (n=24). 34 (n=34) of the participants used iOS and 18 (n=18) used non-iOS.

Privacy concerns were significantly correlated with future self-continuity, r_s = .255, 90% [.002, .501], p = .068. Personal attitude as first-order construct of privacy concerns were significantly correlated with future self-continuity, r_s = .361, 95% [.132, .571], p= .008. There was no significant relationship between anxiety as first-order construct of privacy concerns and future self-continuity, r_s = .180, 95% [-.108, .447], p= .202.

In the perceived-risk-group (n=42) the average age of these participants was 20.0 years (SD=1.64). The age of these participants ranges from 18 to 26 years (M=20.00; SD=1.64). Of the remaining participants, 55,6% (n=25) were female and 44.4% were male (n=20). 25 (n=25) of the participants used iOS and 20 (n=18) used non-iOS.

No significant relationship between perceived risk and future self-continuity could be found, r_s = -.079, 95% [-.425, .245], p = .606. In contrast, the overall perceived risk item was significantly correlated with future self-continuity, r =-.270, 95% [-.564, .070], p = .037.

In the regulation-group (n=50) the average age of these participants was 20.04 years (SD=2.03). The age of these participants ranges from 18 to 26 years (M=20.04; SD=2.03). Of the remaining participants, 56.0% (n=28) were female and 44.0% were male (n=22). 21 (n=21) of the participants used iOS and 29 (n=29) used non-iOS.

No significant relationship between regulation and future self-continuity could be found, r_s = .058, 95% [-.252, .375], p= .689.

Discussion, Conclusion and Further Research

The presented study is a first attempt in applying the psychometric measurement of future self-continuity in information privacy research. The paper shows the good fit of the approach to extend the enhanced APCO model.

The results show a significant correlation from privacy concerns and future self-continuity. This supports the assumption that users who feel emotionally connected to their future self on a higher level do care more about their privacy. Thus, users with higher future self-continuity are more concerned about their privacy because of possible implications for their future when disclosing personal information. Following

recent literature these higher privacy concerns lead to more privacy-aware behavioral reactions. The significant correlation of the first-order dimension "personal attitude" supports this interpretation. Consequently, the results show that even when the participants are in an early stage of their life, which implies that the likelihood of seeing their future self very different is high, they do connect the disclosure of personal data with their future. Thus, the primary objective of this study – to expose a positive relation between future self-continuity and privacy concerns – was successful which qualifies the introduced measurement for future investigations.

Contrary to the APCO model, the study investigated a direct effect between future self-continuity as an antecedent on regulation and perceived risk as outcomes. These assumptions could not be supported. No correlation of the need for governmental regulation or self-regulation could be interpreted by a missing trust or ability in the existing institutions to stand up for users' privacy. The negative correlation of the overall-perceived-risk item does not compulsively contradict these findings. Users are not able to assess the value and possibilities of gathering and analyzing their personal data. Consequently, they are not able to assess the risks involved. The non-findings regarding the perceived risk on a more granular level suggest that users are not able to conduct this valuation.

Nevertheless, this paper should be seen as a first attempt and is therefore afflicted with some limitations. Firstly, the sample size does not represent all age groups because of the focus on students. Moreover, I did not consider culture bound issues as the sample only consists of German users of SMD. For example, Krasnova and Veltri (2010) showed that Germans showed different attitudes when it comes to their level of privacy concerns compared to US users. In addition, the study provides only very general information on the demographic characteristics of the participants, which limits the ability to relate app users' information seeking behavior to demographic characteristics. The presented study is limited due to the three assumed associations of future self-continuity. Also the effects on other variables of the APCO model and other context-variables should be investigated. Consequently, I suggest future investigations in this area. Furthermore, the investigation is limited on privacy issues in the field of smart mobile devices and mobile applications. This leads to very limited generalizability of the presented results. Moreover, the assumed relationships are a first selection and should be extended. In addition, it can be scrutinized if the observed constructs, e.g. the privacy concern, are suitable measures. Therefore, one limitation lies in the multi-item constructs which might be too long and thus participants drift more towards a high-effort process which is not intended when low-effort processing should be measured. Furthermore, a limitation of the study is that the level of participants' literacy (specific knowledge in the field) is not known, 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. Generally, information privacy researchers should not automatically assume that intensions lead to behaviors (Bélanger and Crossler 2011). In the study I asked participants about their privacy concerns. Therefore, one limitation is that it is not possible to reflect actual behavior because I did not conduct a simulation with is a closer representation of the real world.

The significant correlations of privacy concerns and its first-order dimensions with future self-continuity indicate important relationships concerning how users deal with their information privacy and what could affect their behavior. Accordingly, the results indicate a contribution to the extensively discussed privacy paradox. The concept of future self-continuity can be incorporated as a part of the enhanced APCO model as an antecedent. Taking the difficulties of the users in estimating the value of the disclosure of personal information into account, the negative correlation of perceived-overall-risk and future self-continuity is no surprise. An overall-risk perception might not be a suitable measure.

The presented study and its results lead to the need of extensive research in the field of information privacy, behavioral economics and social psychology. Following this first attempt it appears as a promising approach to further investigate future self-continuity and its relationship on several constructs of information privacy and information privacy behavior. Furthermore, fundamental work should be done in the field of the value of personal data and on users' estimation of the implications the disclosure of personal data has on their future. Moreover, the role of privacy literacy should be investigated dependent on the prevailing context.

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 Gross, R. 2006. "Imagined communities: Awareness, information sharing, and privacy on the Facebook," International workshop on privacy enhancing technologies , pp. 36–58.

Acquisti, A., and Grossklags, J. 2004. "Chapter 1 PRIVACY ATTITUDES AND PRIVACY BEHAVIOR Losses , Gains , and Hyperbolic Discounting Personal Information Security and Privacy: Attitudes versus Behavior," , pp. 1–15.

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.

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.

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.

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.

Chellappa, R. K., and Sin, R. G. 2005. "Personalization versus privacy: An empirical examination of the online consumer's dilemma," Information Technology and Management (6:2-3), pp. 181–202.

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

Dasgupta, P., and Maskin, E. 2005. "Uncertainty and Hyperbolic Discounting," The American Economic Review (95:4), pp. 1290–1299.

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.

eMarketer 2016. Slowing Growth Ahead for Worldwide Internet Audience – eMarketer. https://www.emarketer.com/Article/Slowing-Growth-Ahead-Worldwide-Internet-Audience/1014045.

Ersner-Hershfield, H., Garton, M. T., Ballard, K., Samanez-Larkin, G. R., and Knutson, B. 2009a. "Don't stop thinking about tomorrow: Individual differences in future self-continuity account for saving," Judgment and Decision Making (4:4), pp. 280–286.

Ersner-Hershfield, H., Wimmer, G. E., and Knutson, B. 2009b. "Saving for the future self: Neural measures of future self-continuity predict temporal discounting," Social cognitive and affective neuroscience (4:1), pp. 85–92.

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.

Hann, I. H., Hui, K. L., Lee, S. Y. T., and Png, I. P. L. 2007. "Overcoming Online information privacy concerns: An information-processing theory approach," Journal of Management Information Systems (24:2), pp. 13–42.

Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. 2000. "Consumer Trust in an Internet Store: A Cross-Cultural Validation," Information Technology and Management (1:1), pp. 45–71.

Kim, D. J., Ferrin, D. L., and Rao, H. R. 2008. "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," Decision Support Systems (44:2), pp. 544–564.

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.

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.

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.

Milberg, S. J., Smith, H. J., and Burke, S. J. 2000. "Information Privacy: Corporate Management and National Regulation," Organization Science (11:1), pp. 35–57.

Mischel, W. 2014. "The Marshmallow Test: Understanding Self-control and How To Master It," Little Brown and Company, New York.

Morando, F., Iemma, R., and Raiteri, E. 2014. "Privacy evaluation: What empirical research on users' valuation of personal data tells us," Internet Policy Review (3:2), pp. 1–11.

Norberg, P. A., and Horne, D. R. 2007. "Privacy attitudes and privacy-related behavior," Psychology & Marketing (24:10), pp. 829–847.

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.

Pavlou, P. A. 2011. "State of the information privacy literature: Where are we now and where should we go?" Management information systems : mis quarterly (35:4), pp. 977–988.

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.

Rubinstein, A. 2003. ""Economics and Psychology"? The Case of Hyperbolic Discounting," International Economic Review (44:4), pp. 1207–1216.

Slovic, P. 1995. "The construction of preference," American Psycologist (50:5), p. 364.

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

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

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

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

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

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

Westin, A. F. 2003. "Social and Political Dimensions of Privacy," Journal of Social Issues (59:2), pp. 431–453.

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.