Summer 6-15-2016

AN EMPIRICAL ANALYSIS OF PRIVACY DASHBOARD ACCEPTANCE: THE GOOGLE CASE

Johana Cabinakova
University of Freiburg, johana.cabinakova@jupiter.uni-freiburg.de

Christian Zimmermann
University of Freiburg, zimmermann@iig.unifreiburg.de

Guenter Mueller
University of Freiburg, mueller@iig.uni-freiburg.de

AN EMPIRICAL ANALYSIS OF PRIVACY DASHBOARD ACCEPTANCE: THE GOOGLE CASE

Research

Cabinakova, Johana, University of Freiburg, Freiburg, Germany, johana.cabinakova@jupiter.uni-freiburg.de

Zimmermann, Christian, University of Freiburg, Freiburg, Germany, zimmermann@iig.uni-freiburg.de

Müller, Günter, University of Freiburg, Freiburg, Germany, mueller@iig.uni-freiburg.de

Abstract

Over the last decades, personal data has become a crucial asset for digital services. The exploitation of this asset, however, entails severe threats to privacy. Recently, so-called Privacy Dashboards have been presented, which are tools that allow users to gain insight and exercise control over data that a digital service provider has accumulated about them. This innovation enables not only privacy protection but also new ways of collaboration of users and providers of digital services. Privacy Dashboards have the potential to allow users to participate in the generation of user profiles for personalized services, thereby contributing to improved services. However, while a variety of Privacy Dashboards has been presented, factors leading to their actual adoption by users are largely unexplored. To fill this research gap, this paper provides an empirical analysis of antecedents of users' adoption of Privacy Dashboards, in that focusing in particular on the currently most-prominent Privacy Dashboard "Google My Account". Integrating the Technology Acceptance Model and the Privacy Calculus, our analysis shows that trust is the crucial factor in users' adoption of the examined Privacy Dashboard and that Privacy Dashboards can both support users in protecting their privacy but also induce them to disclose personal data and thereby contribute to more precise user profiles.

Keywords: Privacy Dashboards, Technology Acceptance, Collaborative Data Mining, Privacy

1 Privacy Dashboards

Personal data has emerged as one of the core assets of the digital economy (World Economic Forum, 2011). Providers of online services such as Google or Facebook rely almost exclusively on the analysis of their users' data in order to generate revenue through targeted advertising (Enders et al., 2008). However, the collection and analysis of user data not only benefits the providers of these services but also their users (Franke, 2009). For example, personalized services allow for reduction of transaction cost on the side of the user (Varian, 2002). However, ubiquitous data collection and analysis for user profiling obviously threatens users' privacy, autonomy and freedom (Schermer, 2011; Hildebrandt, 2009; Weitzner, 2007).

Privacy Dashboards, a specific class of Transparency-Enhancing Technologies (TETs) (Hansen, 2008), have recently gained increased attention as instruments for not only supporting privacy protection in the digital economy but also for including users as active parts in the value creation of digital services. In contrast to Privacy-Enhancing Technologies, Transparency-Enhancing Technologies aim not at the prevention of data disclosure but at "provid[ing] to the individual concerned clear visibility of aspects relevant to [its personal] data and the individual's privacy" (Hansen, 2008, p. 205). Privacy Dashboards (PDBs), which are defined by Zimmermann et al. (2014) as "transparency tools to provide data subjects with a clear and easily understandable overview over data a data controller has accumulated about them, and [to] empower data subjects to control processing or usage of that data, as well as

future collection of data by the data controller" (Zimmermann et al., 2014, p. 153) go further than that and aim, among others, at "provid[ing] data subjects with mechanisms to control data about them stored by a data controller" (Zimmermann et al., 2014, p. 153). This allows for completely new ways of generating user profiles for personalized digital services. On the one hand, Privacy Dashboards have the potential to decrease user's privacy concerns and, on the other hand, they can facilitate collaborative approaches towards data collection and analysis of providers of digital services. Several privacy dashboards have been present during the last years, both in academia and in practice. Valuable research towards privacy dashboards has been conducted, e.g., by Fischer-Hübner et al. (2011) who developed the "DataTrack" within the Prime and PrimeLife projects or by Buchmann et al. (2013) who presented the "Personal Information Dashboard". Several providers of online services also provide privacy dashboards, e.g., Acxiom (2015) or Google (2015). With its "Google My Account" (GMA) launched in 2015, Google provides the currently most prominent privacy dashboard (Google Inc., 2015). The GMA provides Google's users with functionality for gaining insight into personal data collected by Google and, to some extent, for exercising control over that data through deletion and modification. For example, users can gain insight into location data stored about them by Google, into their search history or into advertising categories they are associated with. However, despite users' concerns for transparency and control with respect to their personal data (Acquisti et al., 2013; Steward and Segars, 2002) and coverage of privacy dashboards in the media (e.g. Handelsblatt, 2015; Spiegel Online, 2015), factors influencing the adoption of Privacy Dashboards by users of online services are currently unexplored.

Consequently, in this paper, we examine key determinants influencing users' attitude to adopt privacy dashboards, in that drawing from the Technology Acceptance Model and the Privacy Calculus. We focus our examination on the Google My Account, because of its wide-ranging functionality and prominent status and on the group of "digital natives" (Prensky, 2001).

The remainder of this paper is structured as follows: the next section presents and elaborates on our research model and hypotheses. Section 3 discusses our methodology and presents the results of our empirical analysis. In Section 4, the analysis, its limitations and our results are critically discusses in detail. Section 5 concludes the paper and provides an outlook on future research.

2 Framework for Online Users Intentions to use Privacy Dashboards

In order to develop a thorough understanding of online users' attitudes toward Privacy Dashboards and their intentions to use them, we constructed a model based on recent research on privacy and technology adoption and diffusion. As defined before, Privacy Dashboards are new technological tools that provide data subjects with an overview over their collected data on the one hand, and the possibility to control and modify this data on the other. Privacy dashboards can be provided either by the data-controller regarding whose data handling behavior they provide transparency or by third parties (Zimmermann et al., 2014). In the case of the Google My Account, the former is the case and, hence, in the following we do not distinguish between Privacy Dashboard provider and data-controller.

Considering the overall novelty of Privacy Dashboards and the very limited understanding of their adoption and usage by online users, the core constructs of our research model are adapted from the Technology Acceptance Model (TAM) (Davis, 1989; Davis et al. 1989), the most successful model in the information systems adoption field (Williams et al. 2009). Despite the fact that the TAM was originally constructed for the purposes of investigating the adoption of computer-based technologies in the working environment (Davis, 1989) many studies show that TAM is likewise suitable as theoretical foundation for the adoption of other online services such as e-commerce (Dinev and Hart, 2006; Gefen et al. 2003; Lee et al., 2001), online banking (Pikkarainen et al., 2004) or electronic health records (Angst and Agarwal, 2009) which focus inter alia on privacy aspects as well. Arguing on this wide-ranging and successful deployment of TAM, we use the TAM constructs "intention" and "attitude" as a basis for our research model. A broad number of researchers examined the relationship between atti-

tudes and intentions and found this relationship to be positive (Ajzen 1985, 1991; Ajzen and Madden 1986; Fishbein and Ajzen, 1974, 1975) meaning, in the field of information systems, that a positive attitude towards a new technology has a positive impact on users intention to use and adopt this technology (Venkatesh et al. 2003; Agarwal and Prasad 1998; Taylor and Todd 1995; Davis and Warshaw 1992; Davis et al. 1989). Therefore, considering attitude as a crucial factor for information systems adoption, we centralize this factor in our research model and focus our primary interest on its determinants with respect to Privacy Dashboards adoption. The main idea underlying this paper is to examine two kinds of factors. Those, which we assume to have an impact on users' attitude towards Privacy Dashboards and which can, to some extent, be influenced by Privacy Dashboards providers and factors that result solely from the already existing user behavior.

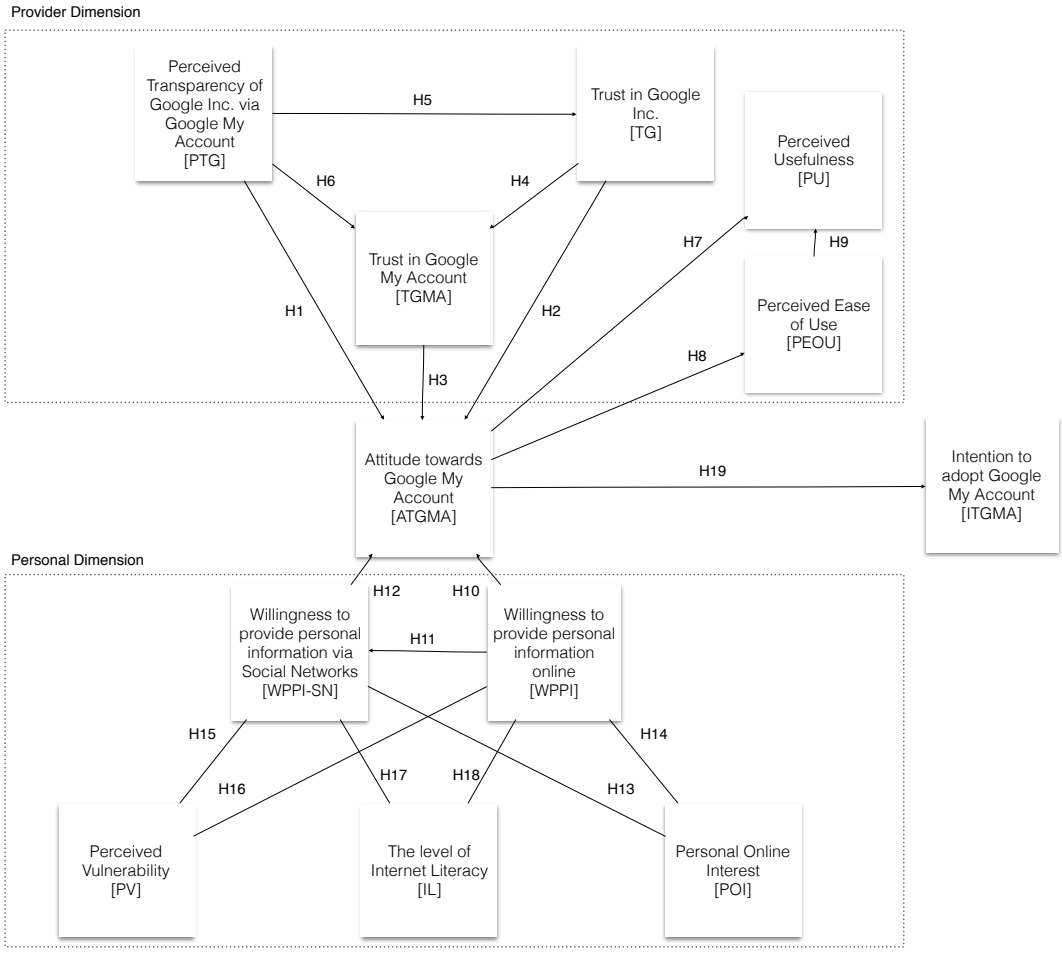

Figure 1: The Research Model

In particular, we build upon the approach by Gefen et al. (2003) and extend and integrate it with the Privacy Calculus approach by Dinev and Hart (2005, 2006), which constitutes "a common approach to analyzing individuals' information disclose behavior, suggesting that an individual's intention to disclose information is based on the comparison of expected benefits and perceived risks in a given context" (Li, 2012). On the example of online shopping, Gefen (2003) confirms that the concept of trust in combination with the traditional TAM constructs including the factors *Perceived Ease of Use* (PEOU) and *Perceived Usefulness* (PU) explain a considerable proportion of variance in intended behavior. Considering the results of Dinev and Hart (2005, 2006) who examined the relationship between *Perceived Vulnerability*, *Internet Literacy* and *Personal Online Interest* on users' *Willingness to Disclose*

Personal Information Online, which is a classic construct of privacy concerns-related research, we likewise incorporate these constructs into our research model.

Drawing from these approaches, we build a two-dimensional research model on Privacy Dashboard adoption while centralizing the two core factors of TAM, attitude and intention and analyzing their determining factors. Figure 1 depicts our research model. We subsume factors that the provider has direct influence over to some extent, such as the *Users Trust in the Privacy Dashboard* (here "GMA"), *Trust in the Privacy Dashboard Provider* (here "Google") and the *Perceived Transparency of the Privacy Dashboard Provider via the Privacy Dashboard* under the term *Provider Dimension.* Here, the term dimension is to be understood as an aspect or feature of situation. On the other hand, the *Personal Dimension* of our model consists of factors that antecede or result from online users already existing privacy concerns, namely *Willingness to Disclose Information Online* and their influential factors *Perceived Vulnerability*, *Internet Literacy* and *Personal Online Interest*. In the following, we introduce our research model and elaborate on its dimensions.

2.1 Provider Dimension – Perceived Transparency and Trust

In order to examine how transparency and trust are related in the context of Privacy Dashboards and how they might influence users' attitude towards Google My Account, a clear definition of both terms is required. Transparency is often defined as "letting the truth be available for others to see if they so choose" (Oliver, 2004) and, hence, with an underlying notion of passivity of the observed (Oliver, 2004). In contrast to this notion, transparency is understood in this paper as active disclosure (Oliver. 2004), e.g., as in the definition by Rawlins (2006), who defines transparency as "the deliberate attempt to make available all legally releasable information […] in a manner that is accurate, timely, balanced, and unequivocal, for the purpose of enhancing the reasoning ability of publics and holding organizations accountable for their actions, policies, and practices". Other than simple disclosure of vast amount of information, transparency means that an organization provides the public with information that is truthful, substantial and useful while allowing holding organization accountable for its actions (Rawlins, 2008). As too much information often leads to less understanding and subsequently to less trust (Strathern, 2000) the extent of information shared should be balanced and determined by demands of customers (Rawlins, 2008). The Google My Account falls under the definition of Privacy Dashboards provided above and is used by Google for "active disclosure" (Oliver, 2004) of information on its handling of its users' data. However, it is not clear for the user whether the data observable within Google My Account is in fact truthful and complete. At the same time, Privacy Dashboard users do not know exactly how their personal data has been collected. Nevertheless we argue that providing a Privacy Dashboard that provides a credible perception of the provider's transparency as active disclosure of information is an important determinant in Privacy Dashboard adoption. More precisely we argue that online users value the information provided via current Privacy Dashboards although it they can not conclusively determine whether the information provided is in fact completely truthful.

Within our research example, users using the Privacy Dashboard Google My Account are provided with insight into some of the personal data Google has stored about them and functionality for, among others, management of their advertisement settings, searching and browsing activity, location history obtained via Google Maps, watched or uploaded videos on YouTube or others. This includes functionality for modification and deletion of some of this data. We assume that, given this information, users are able to form a personal perception of the transparency of the Privacy Dashboard provider (who is, in our case, also the data-collector, viz. Google), which positively affects their attitude towards the adoption of Privacy Dashboards. Therefore the following hypothesis was tested:

H1: Perceived Transparency of Google Inc. via Google My Account positively influences user's attitude towards Google My Account.

The literature shows that the concept of trust is closely related to the concept of transparency (Cramer et al. 2008; Rawlins 2008; Akkermans et al. 2004; Welch and Hinnant, 2003). Lack of trust, both in

the properties of online vendors (service provider) and in the overall web environment, has been repeatedly identified as one of the major barriers for people to engage in services involving submission of personal information online (Aldridge et al. 1997; Wang and Emurian, 2005). As an ambiguous concept studied in number of disciplinary fields, trust covers a wide range of relationships. For the purposes of our research we stick to the definition of Gefen (2000) who defined trust as the belief that the other party will behave as expected in a socially responsible manner, and in doing so, it will fulfill the trusting party's expectations. In order to receive more precise and meaningful results we apply the construct of trust both to the Privacy Dashboard and Privacy Dashboard provider.

Trust in a service provider (here, the Privacy Dashboard provider) determines if a client (here: the user) will maintain the relationship with provider in the future (Doney and Cannon, 1997) and what will be the value of the relationship (Gounaris, 2005). As users are interested the information stored by a provider as well as the data's confidentiality, a trusting behavior towards a service provider is indispensable (Morgan and Hunt, 1994; Sharma and Pattersson, 1999; Liljander and Roos, 2002). Similarly, trust in the particular e-service (or privacy dashboard) is defined as a "quantified belief by a trustor, with respect to the competence, honesty, security and dependability of a trustee within a specified context" (Grandison and Sloman, 2003, p.2) and indicates a positive impact on adoption of e-services. Therefore, with respect to our research example, we assume that the extent to which users are willing to trust in a Privacy Dashboard provider and in the Privacy Dashboard itself is positively related to their attitude towards Privacy Dashboard Adoption:

H2: Trust in Google Inc. will positively influence user's attitude towards Google My Account

H3: Trust in Google My Account will positively influence user's attitude towards Google My Account

In the e-commerce context, empirical research has shown that trust in online vendors increases people's intention to use the vendors' web site (Mukherjee and Nath, 2007; Bhattacherjee, 2002; George, 2002). More precisely, Bhattacherjee (2002) found that trust has a positive effect on an individual's willingness to conduct transactions with an online bank, i.e., to participate in the provided online service. Considering Privacy Dashboard an e-service we hence estimate the following hypothesis:

H4: Trust in Google Inc. will positively influence user's trust in Google My Account

In line with existing research (see above), we argue that the construct of transparency and the constructs of trust are interconnected. Investigating this relationship, Rawlins (2008) showed that as employee perceptions of organizational transparency increased so did trust in the organization. In the context of online privacy, it has repeatedly been shown that providing data-subjects with transparency and control increases their trust in the data-controller (Schnorf et al., 2014; Krasnova et al., 2010; Dinev and Hart, 2006). Transferring these results to our research field and based on the above-mentioned definitions we expect that the same holds in the online context as well:

H5: Perceived Transparency of Google via Google My Account positively influences user's trust in Google Inc.

H6: Perceived Transparency of Google via Google My Account positively influences user's trust in Google My Account.

Finally, considering the previously mentioned decision to build our research model upon the TAM together with studies that describe a significant relationship between attitude and intention we argue that *Perceived Usefulness* (PU) and *Perceived Ease of Use* (PEOU) are significant predictors of attitude (Karahanna and Straub, 1999;Venkatesh, 2000; Gefen, 2000), we assume that the following hypotheses hold:

H7: Perceived Usefulness of Google My Account positively influences user's attitude towards Google My Account.

H8: Perceived Ease of Use of Google My Account positively influences user's attitude towards Google My Account.

H9: Perceived Ease of Use of Google My Account positively influences Perceived Usefulness of Google My Account.

2.2 Personal Dimension - Willingness to disclose information online

The second dimension of our research model focuses on factors that have an effect on user's attitude towards Privacy Dashboards, but in contrast to those in the *Provider Dimension*, can not be as directly influenced by the provider. All of these factors are closely interconnected and result in, or originate from, users' privacy concerns. The factors in the Personal Dimension are adapted from Dinev and Hart (2004; 2005; 2006).

Referring to Westin's definition of privacy "as the claim of individuals to determine for themselves, when, how and to what extent information about them is communicated to others" (Westin, 1967, p. 7), privacy dashboards aim at providing online users with control over the use of the information they have disclosed to a service provider. However the more information disclosed by online users, the more information there is to be controlled and the more challenging it becomes without the availability of a proper tool. Results by Culnan and Armstrong (1999) confirm that the availability of fair information practices, e.g., provision of Privacy Dashboards, can elicit disclosure and build trust relationships. Similarly, previous studies indicate that privacy concerns can be addressed through the use of fair information practices, by providing consumers with more control over their information (Phelps et al. 2000; Culnan and Armstrong, 1999; Milne and Boza, 1999; Foxman and Kilcoyne, 1993). Brandimarte et al. (2013), Xu et al. (2011) or Krasnova et al. (2010) show that users' trust and willingness to disclose personal data can be increased by providing them with control over collection and usage of their personal data.

We assume that this relationship is bidirectional. As the provision of a Privacy Dashboard might increase users' willingness to disclose, a user's general willingness to disclose personal data might positively affect her attitude towards privacy dashboards, which enable her to gain insight into the disclosed data and exercise some extent of control over it and its usage. Hence, we assume the following hypothesis to hold:

H10: Users Willingness to provide personal information online has a positive impact on their attitude towards privacy dashboards.

Especially within the field of online social networks, the amount of disclosed information has dramatically increased in recent years (Gross and Acquisti, 2005). The participation in social networks is inevitably connected with information disclosure, be it through "likes", browsing behavior or simply through one's circle of friends. Hence, we assume that user of online social networks are users that are generally relatively willing to provide personal data online. Thus, the following hypothesis was tested:

H11: Users overall Willingness to provide personal information online positively influences users Willingness to provide personal information online via Social Networks.

Obviously, Privacy Dashboards can not only be provided by search engine providers, but also by providers of online social networking services or chat services. As these services are widely used, especially among digital natives, we were also interested in the question whether users of online social networks and chat services have a particularly positive attitude towards Privacy Dashboards. The following hypothesis was therefore formulated:

H12: Willingness to participate in social networks and chat services (that encourage users to disclose (and) or interchange personal data) has a positive impact on online users attitude towards Privacy Dashboards.

In order to fully understand online users' motivations to adopt Privacy Dashboards, the factors that antecede users' willingness to disclose personal information online have to be taken into account as well. A wide variety of these aspects can moderate the relationship between willingness to disclose information and users' attitude towards Privacy Dashboards, but for the purpose of this paper only the

most relevant also utilized by Dinev and Hart (2004; 2005; 2006) are discussed: *Perceived Vulnerability* (PV), *Personal Online Interest* (POI) and the *Level of Internet Literacy* (LIL).

Personal Online Interest. For the receiving of information online, data disclosure by the users is often unavoidable. This might include situations such as disclosure of credit card information for successful completion of purchases within the field of e-commerce, the disclosure of socio-demographic information for generating an account within a social network service or the disclosure of phone number as required precondition for the usage of chat or messaging services. Users' disclosure of personal data in order to receive some information online in exchange is, in particular, driven by the *Personal Online Interest*, i.e., a construct that reflects users' level of enticement to transact online (Dinev and Hart, 2006). *Personal Online interest* is defined as "the degree of cognitive attraction to Internet interactions" (Dinev and Hart, 2006). Dinev and Hart (2006) confirm that interest to obtain a particular information positively influences the willingness to disclose personal information for being able to access information, goods, and services that might otherwise not be available to users (Dinev and Hart, 2006). We argue that this effect is observable not only in case of the overall information disclosure but also in the field of social networks where information disclosure is always a necessary prerequisite for successful functionality, e.g., when a user is requested to disclose her email address in order to gain access to Facebook. Hence, the following hypotheses were tested:

H13: Personal Online Interest positively influences user's Willingness to disclose personal information via Social Networks

H14: Personal Online Interest positively influences user's overall Willingness to disclose personal information

Perceived Vulnerability. Other than the personal online interest, *Perceived Vulnerability*, defined as the perceived risk of misuse of personal information obtained online (Dinev and Hart, 2004), was examined as a major antecedent of online privacy concerns. It described the potential risk perceived by user when personal information is revealed (Raab, 1998). Similarly as in the case of *Personal Online Interest*, we argue that an impact of perceived vulnerability of disclosed information on the willingness to disclose information is observable as well in its general form as in the case of social networks and that this impact is negative. Therefore the following hypotheses were tested:

H15: Perceived Vulnerability negatively influences user's Willingness to provide personal information online via Social Networks

H16: Perceived Vulnerability negatively influences user's overall Willingness to provide personal information online

Level of Internet Literacy. The third factor related to users online privacy concerns is the *Level of Internet Literacy* measured as the level of skill and knowledge possessed by consumers in using the Internet (Dinev and Hart, 2006). With this the capability to establish an Internet connection, navigating the Web, completing e-commerce transactions, protecting the computer from viruses and spyware, setting the browser's privacy and security options appropriately, and protecting one's privacy by employing adequate measures before disclosing information online is meant (Bandyopadhyay, 2009; Dinev and Hart, 2006; Spiekermann at al. 2001). Previous research confirmed, that a high level of Internet literacy is negatively related to privacy concerns (Dinev and Hart, 2006). However some researcher argue, that the impact of Internet literacy might be double-sided. Based on an approach by Dinev and Hart (2006), Bandyopadhyay (2009) proposes two effects of Online Literacy on privacy concern – positive and negative, depending on the specific skills and knowledge gained through such literacy. Integrating this assumption into our model, we argue that Online Literacy might have two effects on users' willingness to disclose personal information. We distinguish between effects of Internet Literacy on willingness to disclose personal information in general and with respect to online social networks. It might be that online users, who exhibit a high level of Internet literacy and are knowledgeable of the ways their online privacy might be violated, feel more vulnerable regarding their online privacy and, thus, decide not to disclose or to disclose only small amounts of their information. On the other hand, a high degree of Internet literacy might also result in more confident behavior and

ensure online users that they are qualified enough to protect their privacy, e.g., by setting firewalls or using security software which will reduce their perceived vulnerability and thus foster their willingness to disclose information (Bellman et al., 2004). Considering the target group of our research study, i.e., digital natives (cf. Section 3), we expect a high level of Internet Literacy and, similarly to findings by Bellman et al. (2004), a positive impact on users' willingness to disclose information online. Hence the following hypotheses are formulated:

H17: The Level of Internet Literacy positively influences user's Willingness to provide personal information online via Social Networks

H18: The Level of Internet Literacy positively influences user's Willingness to provide personal information online.

3 Methodology and Results

The survey was conducted using a standardized questionnaire both in paper form and online. The first section of the questionnaire contained construct questions referring to the *Provider Dimension* of our research model to measure online users' perceptions on three different attributes of Privacy Dashboards*: Perceived Transparency of Service Provider via Privacy Dashboard*, *Trust in Privacy Dashboard Provider* and *Trust in Privacy Dashboard*. The constructs used to test the proposed research model are based on existing literature and are available in the appendix, along with the list of asked questions. In the second part, questions to measure online users' *Willingness to Provide Information Online*, online users' *Willingness to Provide Information Online Via Social Networks* as well as the three antecedents of privacy concerns (*Perceived Vulnerability*, *Level of Internet Literacy* and *Personal Online Interest*) building up the *Personal Dimension* were asked. The third section consisted of questions related to demographics, namely to age, gender, nationality, marital status, highest educational achievement, current position, average gross yearly income and residence.

In order to provide participants unfamiliar with Google My Account with enough information to be able to competently answer the questionnaire, a detailed description of the examined tool, its structure and functionality was offered at the beginning of the questionnaire. Additionally, participants of the online survey had the possibility to gain this information not only in written form but also in an optional short video tutorial. The invitation to answer the questions in online form was distributed via social networks, whereas the paper form questionnaire were answered by soon-to-be students participating in the preliminary courses of two German universities at the beginning of the 2015/2016 winter term. The approximate time needed to answer the questionnaire amounted to 18 minutes. Data collection took place between August and October 2015. In total, 478 completed surveys were received; 161 from the online survey and 317 from the paper version. In order to make our sample homogenous with respect to our research target, in the point that computer self-efficacy due to age is minimal we focused our analysis only on digital natives. The term *Digital Native* was originally introduced by Prensky in 2001 and refers to those young people who have grown up with digital technology (Prensky, 2001). More precisely, digital natives are all people born after 1980, when social technologies came online (Palfrey and Gasser, 2008). Therefore as we measured age by mean of categories, all participants above the category 21-30 years were excluded from our sample. Also out of the initial set a few subjects needed to be deleted because of irregularities in answer behavior. The final number of people whose answers were adequate to be examined and fulfilled the digital natives condition, amounts to 432. Out of these 432 respondents, 49.4% were female and 50.6% male. Most of the participants were between 17-20 (53.1%) and 21-30 (46.2%) years old. The group is dominated by students (77.7%) and workers (21%), which was to be expected regarding our pre-selection based on age. The educational level of 71.7% of all respondents was the high school diploma and 21.6% held a university degree. 36.8% of all participants reported an average yearly gross income no higher than 5000 euros. The second income group, 9%, didn't exceed a yearly income of 10000 euros. Interestingly, almost 40% of all participants decided not to disclose information about their income.

In order to examine the presented research model and to validate the proposed hypotheses, the model has been transferred into a structural equation model (Chin, 1998). For this analysis the software SmartPLS was used to determined path influences. The results of the path coefficients and t-test are depicted in Figure 2. The R^2 of attitude and intention were satisfying with 0.445 and 0.254, respectively. To test the significance, we used the bootstrapping procedure incorporated in SmartPLS.

As discussed in Section 2, the basis of the Technology Acceptance Model suggests that attitude towards a new technology determines users' behavioral intention to adopt this technology. The results of our examination support this. In our examination, 25.4 % of the variance of behavioral intention is explained by attitude. Considering the results of the *Provider Dimension* with respect to hypotheses H1 – H9 we can draw the conclusion that all hypotheses hold, and, except for H2 and H8, even to a significance level of 0.001.

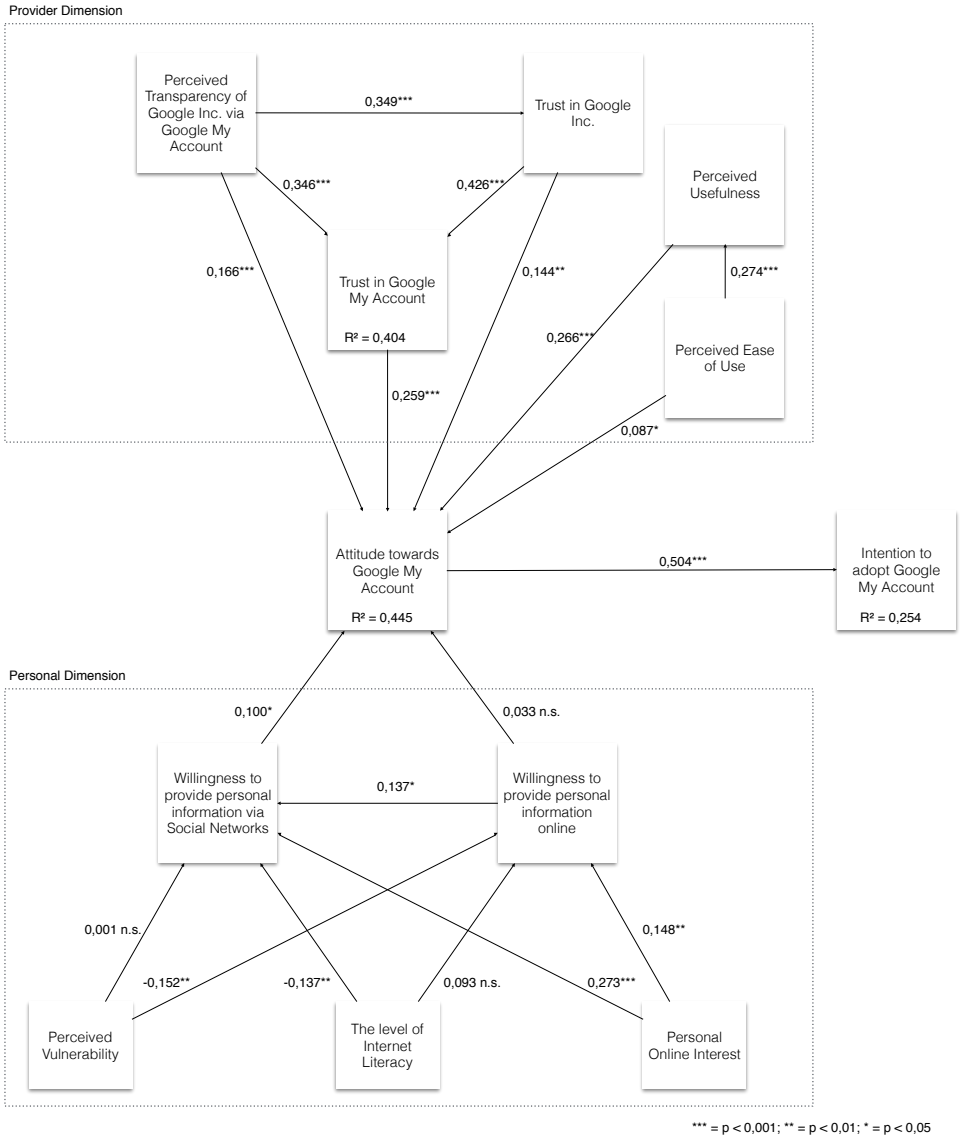

Figure 2. The Results of Structural Model

More diverse results can be found in *Personal Dimension* of our research model. Both, *Willingness to Provide Personal Information via Social Networks* and the overall *Willingness to Provide Personal Information Online* show to have a positive impact on users' attitude towards privacy dashboards,

whereby only in the field of social networks with a satisfying significance level (0.05). Considering the observed antecedents of online information disclosure, the *Personal Online Interest* (H13 and H14) shows strong and positive impact on both willingness to disclose information online via social networks and the overall willingness of information disclosure. Surprisingly the impact of users level of *Internet Literacy* is negative and not positive as anticipated and only in case of the willingness to disclose personal information via social networks significant (H17). Finally, the Perceived Vulnerability shows almost no impact on users willingness to disclose personal information via social networks (not significant), but has a negative, significant effect on general willingness to disclosure information online ($p < 0.01$).

Items		LDNG	CR	AVE	PEOU	PTG	PU	ATGMA	IT-GMA	POI	IL	WPPI-SN	T-GMA	TG	PV	WPPI
PEOU	v_4 v_5 v_6	**0,886 0,749 0,916**	0,889	0,728	0,854											
PTG	v_14 v_15 v_16 v_17	**0,705 0,706 0,761 0,762**	0,824	0,539	0,211	0,734										
PU	v_1 v_2 v_3	**0,774 0,909 0,874**	0,890	0,729	0,274	0,284	0,854									
AT-GMA	v_29 v_30 v_31 v_32	**0,841 0,813 0,882 0,833**	0,907	0,710	0,283	0,447	0,448	0,843								
IT-GMA	v_33 v_34 v_35	**0,847 0,898 0,843**	0,898	0,745	0,124	0,257	0,281	0,504	0,863							
POI	v_20 v_21 v_22	**0,753 0,836 0,850**	0,855	0,663	0,167	0,092	0,094	0,228	0,118	0,814						
IL	v_18 v_19	**0,917 0,922**	0,916	0,845	0,181	0,032	0,044	0,078	0,039	0,063	0,919					
WPPI-SN	v_27 v_28	**0,902 0,906**	0,900	0,818	0,069	0,085	0,072	0,212	0,022	0,287	-0,105	0,904				
T-GMA	v_10 v_11 v_12 v_13	**0,775 0,795 0,835 0,889**	0,895	0,680	0,212	0,494	0,329	0,553	0,262	0,038	0,023	0,205	0,825			
TG	v_7 v_8 v_9	**0,923 0,912 0,923**	0,942	0,845	0,150	0,349	0,107	0,400	0,152	0,014	0,070	0,103	0,547	0,919		
PV	v_23 v_24	**0,928 0,855**	0,887	0,797	0,052	0,111	0,193	0,067	0,230	-0,091	-0,051	-0,041	-0,057	-0,113	0,893	
WPPI	v_25 v_26	**0,865 0,700**	0,763	0,620	0,164	0,023	0,096	0,171	0,094	0,168	0,110	0,168	0,222	0,140	-0,171	0,787

Table 1. The Results of Measurement Model

As to the measurement model, we tested for construct validity, convergent and discriminant validity. In order to validate the construct validity the Composite Reliability (CR) of the constructs was estimated. In order to ensure the construct reliability CR-values exceeding the threshold of 0.7 are recommended which is fulfilled at this place (see Table 1). For convergent validity we estimated the average variance extracted (AVE) which also exceeded the threshold of 0.5 in all cases in our sample (Fornell and Larcker, 1981). In order to justify the different interpretations concerning the test-findings the discriminant validity is used. Due to discriminant validity one can indicate to what extent the measurement of a particular construct distinguish themselves from measures of other constructs in the used model, and ensuring that there are theoretically unequal. To test the discriminant validity the Fornell Larcker Criterion (Fornell and Larcker, 1981) was used, implying that the square root of the AVE should be higher than the correlation with other latent variables. This criterion was also fulfilled

in this sample. Table 1 summarizes the results of the measurement model in a detailed overview. Beside the loadings, the AVE and the CR, the square root of the corresponding AVE is provided (last number in each line). The different correlations are listed below this value in order to verify the discriminant validity.

4 Discussion

With reference to our research objectives, the results of our study hold the following implications. First of all our findings show that the perceived transparency of Google via the GMA significantly increases not only users' trust in the GMA itself but also their trust in Google and has a positive impact on their attitude towards the GMA. In fact, all trust-related factors in the *Provider Dimension* of our research model have a significantly positive effect on users' attitude towards the GMA.

Our findings also show, that users' willingness to disclose information in SNS has a significantly positive effect on their attitude towards the GMA. This seems natural, as users who are willing to engage in data disclosure in an interactive environment such as an SNS would also have a positive attitude towards the GMA, which aims at enabling users' to not only gain insight into the data Google has stored about the user and its data handling behavior but also at interacting with this data, i.e., at deleting or modifying this data. To our surprise, the users' general willingness to disclose information online did not have a significant effect on their attitude towards the GMA. One possible explanation for this result would be the fact that the queried items within the contract willingness to disclose information online focused explicitly on highly sensitive personal information such as credit card number, social security number or annual income, which do not necessarily reflect the content of information provided by GMA and are therefore in a little or no relation to GMA.

Our findings with respect to the effect of users' personal online interest confirm findings by Dinev and Hart (2006). The same holds for users' perceived vulnerability, although only for general willingness to disclose personal information online. It has, to our surprise, almost no effect on the users' willingness to disclose personal information in SNS. While we did not find a significant effect of users' Internet literacy on their general willingness to disclose information online, we did find it to have a negative effect on their willingness to disclose information in SNS. While we can not be sure of the reason for this negative effect, it might be that users in our sample with a high Internet literacy were more aware of recent scandals and developments with respect to SNS and, hence, less wiling to disclose information there. While events such as the CJEU's recent judgement concerning the Safe Harbor Agreement (Court of Justice of the European Union, 2015) or the revelation of the connection of Facebook and US intelligence agencies (Simpson and Brown, 2013) which resonated heavily in Germany might have had an effect on Internet literate German users, we have no conclusive evidence for such a connection.

Some general conclusions on the effects of PDBs on users and providers of online service can be drawn from our findings regarding the GMA although these findings are not necessarily transferrable straightforward. From the above-provided definition of Privacy Dashboards itself, it can be derived that PDBs can be used not only to support users in protecting their privacy but also for actively including them in the generation of the provider's data sets and profile generation. Hence, from a provider-perspective, providing or supporting PDBs can serve primarily three purposes. First, providers can provide PDBs with the goal to increase users' trust and willingness to disclose information or to interact. Second, providers of digital services can utilize PDBs to enhance their data sets and profiles by allowing users to actively modify the data stored about them. Finally, providers of online services can provide privacy dashboard in order to comply with current and future legal requirements such as providing users with an easy to use instrument to exercise their rights to access and rectification (European Commission, 1995, Art. 12). As can be seen, Privacy Dashboards have the potential to constitute valuable instruments for innovative approaches towards data mining in digital services where the service users are not solely providers of data but active party of the value chain. Their active involvement can benefit both parties, e.g., through more precise personalization and less violations of privacy.

From a privacy protection perspective, however, PDBs are Transparency-Enhancing Technologies that aim at supporting in exercising control over their personal data (Hansen, 2008). This aspect is not always necessarily compatible with the above-described application of PDBs for collaborative generation of user profiles. As described above, our analysis shows that the perceived transparency of the provider Google has significantly positive effect not only on the users' trust in the GMA but also in Google itself. Further, all of these three factors have, in our analysis, a significantly positive effect on user' attitude towards the GMA. From a privacy-perspective, this finding constitutes a double-sided sword. It has repeatedly been shown, however, that increased trust in a provider increases users willingness to disclose personal information to the provider Culnan and Armstrong, 1999; Krasnova et al., 2010; Olivero and Lunt, 2004; Stewart and Segars, 2002; Xu et al., 2011) and to interact with the provider (Dinev and Hart, 2006; Kobsa and Teltzrow, 2005; Malhotra et al., 2004; McKnight et al., 2002; Xu et al., 2008). Hence, there is a risk, that PDBs can be misused by providers of online services to pry more data out of their users than would be possible without a PDB. Still, whether PDBs constitute a means for establishing a justifiably trustworthy relation between users and providers of digital services depends heavily on their design and implementation and no general conclusions regarding their benefits and threats can be drawn here.

Last but not least, our analysis obviously has some limitations. The specific focus on the Google My Account makes it difficult to derive general results applying to privacy dashboards in general. However, we decided to specifically examine the GMA because of its prominent status among existing and actually used privacy dashboards and because of its wide-ranging functionality. Further, other existing privacy dashboards such as the "AboutTheData" portal by Acxiom are, with respect to their fundamental scope and functionality, very similar to the GMA. Hence, while our results might not be transferrable to other privacy dashboards straightforward, we still can derive and discuss general conclusion with respect to privacy dashboards. A further limitation of our analysis is its focus on mostly German Digital Natives. Further considering younger and older populations might lead to differing result although we could not find evidence for that in our data set. Nonetheless, further investigations with a broader scope with respect to age are necessary in order to test our results. Despite these limitations, our analysis yield interesting results that can guide future research into privacy dashboards and Transparency-Enhancing Technologies in general.

5 Conclusion and Outlook

In this paper, we examined antecedents for users' adoption of the Google My Account, in that providing the first empirical analysis of users' adoption of a Privacy Dashboard. For our analysis, we extended and integrated existing approaches towards analysis of users' technology acceptance and of users' behavior with respect to privacy and disclosure of personal data. We found out that trust-related factors play a crucial role with respect to users' attitude towards the Google My Account, which we have shown to have a significantly positive effect on their intention to use the technology. We have also shown that users' intention to use the examined Privacy Dashboard is positively effected by their willingness to disclose personal information in online social network services.

From our analysis we draw the conclusion that Privacy Dashboards have the potential to serve as instruments for not only supporting users in protecting their privacy but also for new, collaborative approaches towards digital services and online personalization that do not violate users' privacy but actively include them in the value creation process in the digital economy. For that, however, providers of digital services need to foster users' trust and to design Privacy Dashboards such as to attract users willing to disclose personal information as early adopters. Further research into trust-fostering instruments is necessary, as is research into instruments and mechanism for preventing misuse of disclosed information and Privacy Dashboards. These can include, e.g., accountability-enabling mechanisms and institutions. Future research into Privacy Dashboard adoption should also empirically evaluate this paper's results with respect to broader user groups.

References

Acquisti, A., Adjerid, I., and Brandimarte, L. (2013). „Gone in 15 Seconds: The Limits of Privacy Transparency and Control.“ *IEEE Security and Privacy 11*, 72–74.

Acxiom Corporation (2015). “Acxiom AboutTheData.” URL: https://www.aboutthedata.com (visited on 11/24/2015)

Agarwal, R., and Prasad, J. (1998). “A conceptual and operational definition of personal innovativeness in the domain of information technology.” *Information systems research*, *9*(2), 204-215.

Ajzen, I. (1985). “From Intentions to Actions: A Theory of Planned Behavior.” In: *Action Control.* P.D.J. Kuhl, and D.J. Beckmann, eds. (Springer Berlin Heidelberg), pp. 11–39.

Ajzen, I. (1991). “The theory of planned behavior.” *Organizational behavior and human decision processes*, *50*(2), 179-211.

Ajzen, I., and Madden, T. J. (1986). “Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control.” *Journal of experimental social psychology*, 22(5), 453-474.

Akkermans, H., Bogerd, P., and Van Doremalen, J. (2004).” Travail, transparency and trust: A case study of computer-supported collaborative supply chain planning in high-tech electronics.” *European Journal of Operational Research*, 153(2), 445-456.

Aldridge, A., Forcht, K., and Pierson, J. (1997). „Get linked or get lost: marketing strategy for the Internet.“ *Internet Research 7(3)*, 161–169.

Angst, C. M., and Agarwal, R. (2009). “Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion.” *MIS quarterly*, *33*(2), 339-370.

Bandyopadhyay, S. (2011). “Antecedents and consequences of consumers’ online privacy concerns.” *Journal of Business and Economics Research* 7(3).

Bellman, S., Johnson, E.J., Kobrin, S.J., and Lohse, G.L. (2004). “International Differences in Information Privacy Concerns: A Global Survey of Consumers.” *The Information Society 20*, 313–324.

Bhattacherjee, A. (2002), “Individual trust in online firms: scale development and initial test”, *Journal of Management Information Systems*, Vol. 19 No. 1, pp. 211-41.

Brandimarte, L., Acquisti, A., and Loewenstein, G. (2013). “Misplaced Confidences Privacy and the Control Paradox.” *Social Psychological and Personality Science* 4, 340–347

Buchmann, J., Nebel, M., Rossnagel, A., Shirazi, F., Simo Fhom, H., and Waidner, M. (2013). “Personal Information Dashboard: Putting the Individual Back in Control.” *In Digital Enlightenment Yearbook 2013: The Value of Personal Data*, M. Hildebrandt, K. O’Hara, and M. Waidner, eds. (Amsterdam: IOS Press), pp. 139–164.

Casalo, L.V., Flavia n, C. and Guinaliıu, M. (2007), “The role of security, privacy, usability and reputation in the development of online banking”, *Online Information Review*, Vol. 31 No. 5, pp. 583-603.

Chin, W. W. (1998). “The partial least squares approach to structural equation modeling.” *Modern methods for business research*, *295*(2), 295-336.

Coulter, K.S., Coulter, R.A. (2002). “Determinats of trust in a service provider: the moderating role of length of relationship.” *Journal of Service Marketing*, 16(1), 35-50.

Court of Justice of the European Union (2015). “Judgment in Case C-362/14.” URL: http://curia.europa.eu/juris/documents.jsf?num=C-362/14# (visited on 11/18/2015).

Cramer, H., Evers, V., Ramlal, S., Van Someren, M., Rutledge, L., et al.. (2008). “The effects of transparency on trust in and acceptance of a content-based art recommender.” *User Modeling and User-Adapted Interaction*, 18(5), 455-496.

Culnan, M. J., and Armstrong, P. K. (1999). “Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation.” *Organization Science*, 10(1), 104-115.

Davis, F. D., and Warshaw, P. R. (1992). “What do intention scales measure?”. *The Journal of General Psychology*, *119*(4), 391-407.

Davis, F.D. (1989). "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology." *MIS Quarterly*. 3, pp.319-340.
Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. (1989). "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models." *Management Science*. 8, pp. 982-1003.
Dinev, T., and Hart, P. (2005). „Internet privacy concerns and social awareness as determinants of intention to transact." *International Journal of Electronic Commerce 10*, 7–29.
Dinev, T., and Hart, P. (2006). "An extended privacy calculus model for e-commerce transactions." *Information Systems Research*, *17*(1), 61-80.
Doney, P.M., and Cannon, J.P. (1997)." An examination of the nature of trust in buyer-seller relationships." *The Journal of Marketing* 35–51.
Enders, A., Hungenberg, H., Denker, H.-P., and Mauch, S. (2008). "The long tail of social networking." Revenue models of social networking sites." *European Management Journal* 26, 199–211.
European Commission (1995). "Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." *Official Journal of the European Communities* L281:38, 31–50.
Fischer-Hübner, S., Hedbom, H., and Wästlund, E. (2011). "Trust and Assurance HCI." In *Privacy and Identity Management for Life*, J. Camenisch, S. Fischer-Hübner, and K. Rannenberg, eds. (Springer Berlin Heidelberg), pp. 245–260.
Fishbein, M., and Ajzen, I. (1974). "Attitudes towards objects as predictors of single and multiple behavioral criteria." *Psychological review*, *81*(1), 59.
Fishbein, M., and Ajzen, I. (1975). "Belief, attitude, intention and behavior: An introduction to theory and research". *Reading, MA: Addison, Wesley*.
Fornell, C., and Larcker, D.F. (1981). „Evaluating structural equation models with unobservable variables and measurement error." *Journal of Marketing Research 18*, 39–50.
Foxman, E.R., and Kilcoyne, P. (1993). "Information technology, marketing practice, and consumer privacy: Ethical issues." *Journal of Public Policy and Marketing* 106–119.
Franke, N., Keinz, P., and Steger, C.J. (2009). "Testing the Value of Customization: When Do Customers Really Prefer Products Tailored to Their Preferences?" *Journal of Marketing 73*, 103–121.
Gefen, D. (2000). "E-commerce: the role of familiarity and trust." *Omega*, *28*(6), 725-737.
Gefen, D., Karahanna, E., and Straub, D. W. (2003). "Trust and TAM in online shopping: an integrated model." *MIS Quarterly*, 27(1), 51-90.
George, J.F. (2002), "Influences on the intent to make internet purchases", *Internet Research*, Vol. 12 No. 2, pp. 165-80.
Google, Inc. (2015). "Google My Account." URL: https://myaccount.google.com/ (visited on 2015//11/24)
Gounaris, S.P. (2005). „Trust and commitment influences on customer retention: insights from business-to-business services." *Journal of Business Research 58*, 126–140.
Grandison, T., and Sloman, M. (2003). "Trust management tools for internet applications." In *Trust Management*, (Springer), pp. 91–107.
Gross, R., and Acquisti, A. (2005). "Information revelation and privacy in online social networks." In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, (ACM), pp. 71–80.
Hansen, M. (2008). „Marrying Transparency Tools with User-Controlled Identity Management." In: *The Future of Identity in the Information Society*, S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci, eds. (Springer US), pp. 199–220.
Hildebrandt, M. (2009). "Profiling and AmI." In: *The Future of Identity in the Information* Society, K. Rannenberg, D. Royer, and A. Deuker, eds. (Springer Berlin Heidelberg), pp. 273–310.
Karahanna, E., and Straub, D.W. (1999). "The psychological origins of perceived usefulness and ease-of-use." *Information and Management 35*, 237–250.
Kerkmann, C. (2015). Google will erwachsen werden. Handesblatt. URL: http://www.handelsblatt.com/my/unternehmen/it-medien/zugestaendnisse-beim-datenschutz-

google-will-erwachsen-werden/12471656.html?ticket=ST-169407-z7LTofdzdWZucwBY5kfj-s02lcgiacc01.vhb.de (visited on 2015/11/26)
Kobsa, A., and Teltzrow, M. (2005). "Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior." In: *Privacy Enhancing Technologies*, D. Martin, and A. Serjantov, eds. (Springer Berlin Heidelberg), pp. 329–343.
Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). "Online social networks: why we disclose*." Journal of Information Technology* 25(2), 109–125.
Lee, D., Park, J., and Ahn, J. H. (2001). "On the explanation of factors affecting e-commerce adoption." *ICIS 2001 Proceedings*, 14.
Li, Y. (2012). "Theories in online information privacy research: A critical review and an integrated framework." *Decision Support Systems* 54, 471–481.
Liljander, V., and Roos, I. (2002). "Customer-relationship levels-from spurious to true relationships." *Journal of Services Marketing 16*, 593–614.
Malhotra, N.K., Kim, S.S., and Agarwal, J. (2004). "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15(4), 336–355.
McKnight, D.H., Choudhury, V., and Kacmar, C. (2002). "The impact of initial consumer trust on intentions to transact with a web site: a trust building model." *The Journal of Strategic Information Systems* 11(3), 297–323.
Meinert, D.B., Peterson, D.K., Criswell, J.R., Crossland, M.D. (2006). "Privacy Policy Statements and Consumer Willingness to Provide Personal Information." In: *Journal of Electronic Commerce in Organizations*, 4(1), 1-17.
Milne, G.R., and Boza, M.-E. (1999). "Trust and concern in consumers' perceptions of marketing information management practices." *Journal of Interactive Marketing 13*, 5–24.
Morgan, R.M., and Hunt, S.D. (1994). "The commitment-trust theory of relationship marketing." *The Journal of Marketing* 20–38.
Mukherjee, A. and Nath, P. (2007), "Role of electronic trust in online retailing: a re-examination of the commitment-trust theory", *European Journal of Marketing*, Vol. 41 Nos 9/10, pp. 1173-202.
Oliver, R.W. (2004). *What is Transparency?* McGraw-Hill.
Olivero, N., and Lunt, P. (2004). "Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control." *Journal of Economic Psychology*, *25*(2), 243-262.
Palfrey, J. and Gasser, U. (2008) *Born Digital: Understanding the First Generation of Digital Natives*. (Basic Books)
Parasuraman, A., Zeithaml, V.A. and Berry, L.L. (1985). "A conceptual model of service quality and its implications for future research." *Journal of Marketing*, 49(4), 41-50.
Phelps, J., Nowak, G., and Ferrell, E. (2000). "Privacy Concerns and Consumer Willingness to Provide Personal Information." *Journal of Public Policy and Marketing* 19(1), 27–41.
Pikkarainen, T., Pikkarainen, K., Karjaluoto, H. and Pahnila, S. (2004), "Consumer acceptance of online banking: an extension of the technology acceptance model", *Internet Research*, Vol. 14 No. 3, pp. 224-35.
Prensky, M. (2001). "Digital natives, digital immigrants part 1." *On the Horizon 9*, 1–6.
Raab, C.D. (1998). "The distribution of privacy risks: Who needs protection?" *The Information Society 14*, 263–274.
Rawlins, B. (2006). "Give the Emperor a Mirror: Toward Developing a Stakeholder Measurement of Organizational Transparency." *Paper presented at Educators Academy, Public Relations Society of America International Conference*, Salt Lake City, UT.
Rawlins, B. (2008). "Measuring the relationship between organizational transparency and employee trust." *Public Relations Journal*, 2(2), 1-21.

Schermer, B.W. (2011). "The limits of privacy in automated profiling and data mining." *Computer Law and Security Review* 27(1), 45–52.
Schnorf, S., Ortlieb, M., and Sharma, N. (2014). "Trust, Transparency and Control in Inferred User Interest Models." In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, (New York, NY, USA: ACM), pp. 2449–2454.
Sharma, N., and Patterson, P.G. (1999). „The impact of communication effectiveness and service quality on relationship commitment in consumer, professional services." *Journal of Services Marketing 13*, 151–170.
Simpson, D., and Brown, P. (2013). „NSA mines Facebook for connections, including Americans' profiles." URL: http://edition.cnn.com/2013/09/30/us/nsa-social-networks/ (visited on 2015/11/26)
Spiegel Online (2015). Datensammlung zum Nachschauen: Google macht transparent, wie nackt seine Nutzer sind. URL: http://www.spiegel.de/netzwelt/netzpolitik/privacy-dashboard-google-buendelt-privatsphaere-einstellungen-a-1036634.html (visited on 2015/11/26)
Spiekermann, S., Grossklags, J., and Berendt, B. (2001). "E-privacy in 2Nd Generation E-commerce: Privacy Preferences Versus Actual Behavior". In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, (New York, NY, USA: ACM), pp. 38–47.
Stewart, K.A., and Segars, A.H. (2002). "An empirical examination of the concern for information privacy instrument." *Information Systems Research* 13(1), 36–49.
Strathern, M. (2000). "The tyranny of transparency." *British Educational Research Journal*, 26(3), 309-321.
Taylor, S., and Todd, P. A. (1995). "Understanding information technology usage: A test of competing models." *Information systems research*, *6*(2), 144-176.
Varian, H.R. (2002). "Economic Aspects of Personal Privacy." In *Cyber Policy and Economics in an Internet* Age, W.H. Lehr, and L.M. Pupillo, eds. (Springer US), pp. 127–137.
Venkatesh, V. (2000). "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model." *Information Systems Research 11*, 342–365.
Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). "User acceptance of information technology: Toward a unified view." *MIS Quarterly*, 425-478.
Wang, Y. D., and Emurian, H. H. (2005). "An overview of online trust: Concepts, elements, and implications." *Computers in human behavior*, *21*(1), 105-125.
Weitzner, D.J. (2007). "Google, Profiling, and Privacy." *IEEE Internet Computing* 11(6), 95–97.
Welch, E. W., and Hinnant, C. C. (2003, January). "Internet use, transparency, and interactivity effects on trust in government." In *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on* (pp. 7-pp). IEEE.
Westin, A. (1967). *Privacy and Freedon* (New York, USA: Atheneum).
Williams, M.D., Dwivedi, Y.K., Lal, B and Schwarz, A. (2009). "Contemporary trends and issues in IT adoption and diffusion research." *Journal of Information Technology*. 1, pp. 1-10.
World Economic Forum (2011). "Personal Data: The Emergence of a New Asset Class." URL: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (visited on 11/25/2015)
Xu, H., Dinev, T., Smith, H.J., and Hart, P. (2011). "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances." *Journal of the Association for Information Systems* 12(12), 798 – –824.
Xu, H., Dinev, T., Smith, H.J., and Hart, P. (2008). "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View." In: *Proceedings of ICIS 2008*.
Zimmermann, C., Accorsi, R., Müller, G. (2014). "Privacy Dashboards: Reconciling data-driven business models and privacy." In: *Proceedings of the 9th International Conference on Availability, Reliability and Security*. (IEEE)

Appendix

Construct	Item	Scale	Source
Perceived Usefulness [PU]	The Google My Account is useful for me, because: v_1: using this service enables me to see what kind of data has been accumulated about me by Google v_2: using this service enables me to control the information about me saved by Google v_3: using this service enables me to change the information about me saved by Google	Strongly disagree–Strongly agree	Davis, 1989 Davis et al. 1989
Perceived Ease of Use [PEOU]	v_4: I think Google My Account is easy to use. v_5: Learning how to use Google My Account would be easy for me. v_6: My interaction with Google My Account would be clear and understandable	Strongly disagree–Strongly agree	Davis, 1989 Davis et al. 1989
Trust in Google Inc. [TG]	v_7: All in all I have trust in Google. v_8: I think I can trust Google with respect to what it does with my data provided online. v_9: I think that Google is a trustworthy company.	Strongly disagree–Strongly agree	* self developed
Trust in Google My Account [TGMA]	v_10: I think that Google My Account doesn't follow the interest of Google Company but mine. v_11: I trust Google My Account that it shows all information saved about me. v_12: I trust Google My Account that all information I delete is really deleted. v_13: All in all I have trust in Google My Account.	Strongly disagree–Strongly agree	* self developed
Perceived Transparency of Google Inc. via Google My Account [PTG]	v_14: I think that Google My Account is a tool that helps to understand how Google's decisions affect people like me. v_15: I think that Google My Account provides information that is useful to people like me for making informed decisions. v_16: I think that Google My Account contributes to make Google accountable to people like me for its actions. v_17: I think that Google My Account lets people like me know what is Google doing with the collected information and why it is doing it.	Strongly disagree–Strongly agree	Rawlins (2006)
Internet Literacy [IL]	Rate the extent to which you are able to do the following tasks: v_18: Identify and delete a program which you consider intrusive (spyware) and which was installed through the Internet without your knowledge and permission. v_19: Manage virus attacks by using antivirus software.	Not at all-Very much	Dinev and Hart (2006)
Personal Online Interest [POI]	Rate the extent to which you agree with the following statements: v_20: I find that personal interest in the information that I want to obtain from the Internet overrides my concerns of possible risk or vulnerability that I may have regarding my privacy. v_21:The greater my interest to obtain a certain information or service from the Internet, the more I tend to suppress my privacy concerns. v_22:In general, my need to obtain certain information or services from the Internet is greater than my concern about privacy.	Strongly disagree–Strongly agree	Dinev and Hart (2006)
Perceived Online Vulnerability [PV]	Indicate the extent to which you are concerned about the following: v_23:Records of online transactions could be sold to third parties v_24:Personal information submitted online could be misused	Not at all concerned–Very concerned	Dinev and Hart (2004)
Willingness to provide personal information online [WPPI]	To what extent are you willing to use the Internet to do the following activities? v_25: Purchase goods or services from websites that require me to submit accurate and identifiable information such as telephone number, social security number or credit card number. v_26: Provide financial information about e.g. my annual income.	Not at all-Very much	Dinev and Hart (2006) Phelps et al. (2000)
Willingness to provide personal information online via social networks [WPPI-SN]	To what extent are you willing to use the Internet to do the following activities? v_27: Use free social networks such as Facebook that require me to submit accurate and identifiable information. v_28: Use free chat services such as WhatsApp by means of which I interchange accurate and identifiable information about me.	Not at all-Very much	*self developed
Attitude towards Google My Account [ATGMA]	v_29: In my opinion, Google My Account is a useful tool. v_30: I think it is a good idea, that Google launched Google My Account. v_31: I think I would feel positive about using Google My Account. v_32: Using Google My Account gives me a good feeling.	Strongly disagree–Strongly agree	Davis et al. 1989; Fishbein and Ajzen 1975 Taylor andTodd 1995a, 1995b
Intention to use Google My Account [ITGMA]	v_33: I intend to use Google My Account in the future in order to solely see the data Google Inc. have saved about me. v_34: I intend to actively use Google My Account in the future in order to modify and/or delete the data Google Inc. have saved about me. v_35: I intend to use Google My Account regularly in the future.	Strongly disagree–Strongly agree	Venkatesh et al 2003, Davis et al.1989,;Fishbein and Ajzen 1975;Taylor and Todd 1995a,1995b