Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization

SABRINA KARWATZKI, OLGA DYTYNKO, MANUEL TRENZ, AND DANIEL VEIT

SABRINA KARWATZKI (sabrina.karwatzki@wiwi.uni-augsburg.de; corresponding author) is a Ph.D. candidate in the Faculty of Business and Economics of the University of Augsburg, Germany. Her research focuses on the impact of information privacy on individuals and organizations. Her work has been published in the *Journal of Business Economics*, as well as in the proceedings of conferences such as the European Conference on Information Systems and Hawaii International Conference on System Sciences.

OLGA DYTYNKO (olga.dytynko@student.uni-augsburg.de) is affiliated with the Faculty of Business and Economics of the University of Augsburg, Germany. Her research focuses on the impact of personalization-privacy trade-offs on adoption of personalized services. Her research has been published in the proceedings of Hawaii International Conference on System Sciences.

MANUEL TRENZ (manuel.trenz@wiwi.uni-augsburg.de) is an assistant professor in the Faculty of Business and Economics of the University of Augsburg, Germany, and a research associate in the Research Department for Information and Communication Technologies of the Centre for European Economic Research. He holds a Ph.D. from the Business School of the University of Mannheim, Germany. His research focuses on the implications of IT innovations on individuals' perceptions and behavior, including innovative digital services, channel convergence in retailing, and social issues arising in the areas of privacy or the sharing economy. His work has been published in *Managerial and Decision Economics*, as well as in the proceedings of conferences such as the International Conference on Information Systems and the European Conference on Information Systems.

DANIEL VEIT (veit@wiwi.uni-augsburg.de) is a professor of Information Systems and Management in the Faculty of Business and Economics of the University of Augsburg, Germany. His interests focus on market mechanisms, sustainability-related research, and business models and entrepreneurship, including questions regarding multichannel commerce, privacy, health, and sharing economy. Among others, his work has been accepted for publication in the *Journal of Service Research* and the *European Journal of Operational Research* as well as published in the proceedings of the International Conference on Information Systems and the European Conference on Information Systems.

ABSTRACT: Digital services need access to consumers' data to improve service quality and to generate revenues. However, it remains unclear how such services should be configured to facilitate consumers' willingness to share personal information. Prior studies discuss an influence of selected individual traits or service configurations, including transparency features and service personalization. This study aims at uncovering how interactions among individuals' privacy valuation, transparency features, and service personalization influence their willingness to disclose information. Building on *information boundary theory*, we conducted an experimental study with 286 participants on a data-intense digital service. In contrast to our expectation, we found no indication that providing transparency features facilitates individuals' information disclosure. Relative to the personalization–privacy paradox, individuals' privacy valuation is a strong inhibitor of information provision in general, not only for personalized services. Personalization benefits only convince consumers who exhibit little focus on privacy. Thus, service providers need to align their service designs with consumers' privacy preferences.

KEY WORDS AND PHRASES: digital services, information boundary theory, information disclosure, information privacy, information-use transparency, personalization, privacy, transparency features, valuation of privacy.

The personal data of consumers allow digital businesses to improve or monetize their services. Marketers worldwide collect and analyze identity-related consumer data, such as e-mail addresses, location, demographics, or lifestyle details [36]. Such data can be used for personalization of products and services to deliver additional value to consumers by better targeting their needs and interests. Thus, personalization is a potential source of competitive advantage [58, 62]. The data can also be leveraged for other beneficial use cases (e.g., overall service improvement) by learning about consumers' usage patterns and issues. However, it can be exploited to realize direct monetary benefits—either via targeted advertisement or by selling information to third parties. More often than not, services lack transparency features, and consumers are not well-informed about which data are collected and how they will be used [4, 59]. As a direct result of many cases where firms gather data without explanation or recognizable necessity, some consumers preserve information boundaries and are resistant to sharing their data.

According to the latest TRUSTe Privacy Index 2016, 92 percent of U.S. Internet users have privacy-related concerns, while 45 percent of respondents are more worried about their online privacy than they were one year ago [60]. Nevertheless, consumers may give up personal information to businesses in exchange for promised benefits [16] and trade the benefits of using superior or free services against the associated risks [12, 54]. This evaluation of benefits and risks depends on the privacy valuation of each individual [30, 59]. Since digital services are highly dependent on consumers' data, it is crucial to uncover how this disposition interacts with service characteristics such as transparency or personalization.

Surveys typically find that consumers wish to have more transparency regarding the collection and use of their personal data [60]. *Information-use transparency* *features* allow consumers to access the data collected about them and inform them about how and for what purposes the acquired information is used [6].[1] Previous research highlights that the implementation of transparency-enhancing mechanisms could be one way to overcome privacy concerns [32, 59], because it increases perceived procedural fairness and fosters reciprocity [68, 70]. It also increases people's willingness to spend money on websites that communicate their privacy practices in an easily accessible and understandable way [61]. Yet, there might also be a contrary effect of transparency: if consumers understand how much information is collected and how it is used, their fears may increase [35].

At the same time, the situational trade-off may be positively influenced by personalization features [58]. While there is a general consensus on the positive impact of personalization [7], the joint investigation of personalization and privacy valuation resulted in an interesting discovery: the *personalization–privacy paradox* [6], which states that people who value privacy features most have a low willingness to be profiled for personalization purposes. We challenge and extend this finding by combining it with the situational benefits of information-use transparency based on the assumption that those benefits may satisfy certain consumers' needs for privacy feedback, and thus facilitate their interactions with personalized services. We aim to disentangle the interactions between privacy valuation, personalization, and information-use transparency. Overall, we pose the following research question: *How do consumers' dispositions to value privacy, service personalization, and transparency features influence their willingness to disclose information?*

Theoretical Foundations and Development of Hypotheses

Prior Research on Personalization, Transparency Features, and Privacy Valuation

Personalization is "the ability to proactively tailor products and ... experiences to tastes of individual consumers based upon their personal and preference information" [12, p. 181]. It mostly appears in two forms: *personalized advertising* and *personalized services* (e.g., product recommendations) [6]. For both kinds of personalization, firms build consumer profiles based on data that users provide voluntarily or via information acquired through observation of users' online behaviors [11, 12]. We focus on personalized services.

Information systems (IS) researchers have investigated both benefits and risks of personalization. For instance, personalized services can reduce information overload and thereby increase the satisfaction of users [41]. If personalization increases the sense of control and freedom of consumers—for example, through personalized order tracking, purchase histories, or e-mail notification of new products and special deals—it will be appreciated by many consumers. Furthermore, web personalization that includes relevant content is valued by consumers as a decision aid because it reduces cognitive efforts in their decision-making processes [33].

However, some consumers may refuse to use offered services, even if they value personalization, as they are concerned about their information privacy due to potential commercial misuse of their data [6, 12]. *Information privacy* reflects the extent to which individuals are able to control how, when, and what amount of personal information is revealed to others [64]. *Privacy concerns* are individuals' concerns related to opportunistic behavior with regard to personal data submitted over the Internet. These concerns represent the degree to which individuals consider a potential privacy loss through the disclosure of personal information [18, 19] and arise as "personalization is not feasible without sharing personal information, and free allowance of services is not feasible without some exploitation of this information by the vendor" [11, p. 196]. Thus, while some consumers are willing to sacrifice their privacy to some extent in exchange for benefits (e.g., personalization), others protect their privacy as a fundamental right [56]. The resulting *personalization–privacy trade-off* suggests that consumers will likely use personalization services if they obtain a certain value that overrides existing privacy concerns [12, 38]. In Table 1, we summarize the existing knowledge about the personalization–privacy trade-off in IS research.

Further investigation of the tension between personalization and privacy revealed that people's perception of the benefits and costs of personalized communication depends on their general attitude toward revealing personal data [59]. Thus, consumers' privacy preferences are heterogeneous, and they experience the trade-off between information disclosure benefits and privacy concerns in distinct ways [30, 59]. One concept that depicts people's general privacy preferences, in particular, is their *disposition to value privacy* (DTVP) [40, 66]. DTVP is a personality attribute that represents a person's general need to preserve specific information boundaries in order to frame their personal space in different situations and contexts. Prior research found that DTVP influences individuals' assessment of privacy risks [66]. It follows that individuals who generally value privacy more may also perceive risks of information disclosure for personalization differently than people with a lower DTVP, and their resulting information disclosure behavior may vary as well. Yet, to the best of our knowledge, the impact of privacy valuation on information disclosure and its interactions with personalization have yet to be studied. Table 2 presents an overview of previous research on individuals' privacy valuation.

To reduce privacy concerns and thereby increase service usage, previous research has investigated transparency-enhancing mechanisms [6, 34, 61], including privacy assurances [44] and control features [42].[2] *Information-use transparency* is the extent to which an online firm provides features that allow consumers to access the data collected about them and informs them about how and for what purposes the acquired information is used [6]. From a consumer's perspective, privacy policies and transparency features are not the same [6]: transparency features give an overview and thus enhance the sense of which information is collected and how it could be used by organizations in an accessible and understandable way. In combination, privacy policies and transparency features can facilitate the understanding of a company's data usage policy for consumers. If such information is absent, or if

Table 1. Summary of Previous Research on the Personalization–Privacy Trade-Off

Authors	Understanding of personalization	Context	Theory	Method	Main findings
Chellappa and Sin (2005) [12]	Ability to tailor products and purchasing experiences to individuals' needs based on personal and preference information	Online personalization service	Privacy calculus	Survey	Consumers' value of personalization positively affects usage of personalization, while privacy concerns have a negative impact.
Awad and Krishnan (2006) [6]	Ability to collect, analyze, and use consumers' information to offer personalized services or advertising	Personalized advertising, personalized news, and financial services	Utility maximization theory	Survey	Personalization–privacy paradox: consumers who value transparency features are less willing to be profiled for personalization purposes. Consumers value personalized online services more than ads.
Treiblmaier and Pollach (2007) [59]	Consumer profiles derived from (un-) consciously provided consumer data are used to provide personalized services or advertising	Personalization for purposes such as purchase decisions, advertisements	—	Qualitative interviews, survey	Peoples' perception of benefits and costs of personalization depends on their privacy valuation and the context.
Sheng et al. (2008) [54]	Personalization in u-commerce can be based on individuals' identity, time, and location	Personalized location-aware notifications (weather service)	Privacy calculus	Experiment	Impact of personalization on privacy concerns is context-dependent: In an emergency situation, individuals are more willing to adopt personalized services than in nonemergency situations.
Xu et al. (2009) [68]	Extent to which a location-based service can be tailored to consumers' preferences, needs, and context	Location-based services (mobile coupons)	Privacy calculus	Experiment	Personalization positively influences consumers' information disclosure decisions, while perceived risks have a negative impact. Privacy-related interventions can influence this trade-off.

(continues)

Table 1. Continued

Authors	Understanding of personalization	Context	Theory	Method	Main findings
Ho (2009) [32]	Collect and analyze consumers' preferences and behavior to tailor content to consumers' needs	Personalized mobile services	—	Focus group, survey	Consumers value highly personalized mobile services, but are also concerned about privacy and spam. They hesitate to share some information with such service providers.
Xu et al. (2011) [66]	Ability to provide content or services based on individuals' behavior and preferences to meet the needs of an individual	Location-aware marketing (mobile coupons)	Privacy calculus	Experiment	The perception of personalization as something positive or negative depends on how personalized content is delivered (covert vs. overt).
Li and Unger (2012) [38]	Personalization of product or service recommendations based on previously collected information such as past purchases or browsing behavior	Personalized news and financial services	Privacy calculus	Experiment	The quality of personalization offerings can outweigh the negative impact of privacy concerns on individuals' likelihood of service usage.
Sutanto et al. (2013) [57]	Usage of consumers' information to deliver personalized advertising messages to meet their preferences more effectively	Personalized mobile advertising (mobile coupons)	Information boundary theory, gratification theory	Experiment	Personalization and privacy produce a tension. If a privacy-safe solution is provided that prevents transmission of personal information while still offering a personalized service, individuals' concerns can be mitigated.

Table 2. Summary of Previous Research on Individuals' General Valuation of Privacy

Authors	Context	Theory	Method	Main findings
Ackerman et al. (1999) [1]	General	—	Survey	Individuals differ in how they perceive disclosures of personal data and information practices. Based on those differences, they can be segmented into marginally concerned individuals, pragmatic majority, and privacy fundamentalists.
Harris Interactive (2002) [31]	General	—	Survey	Consumers can be segmented into privacy fundamentalists, privacy pragmatists, and privacy unconcerned. The majority of individuals are pragmatists.
Sheehan (2002) [53]	Various online communication-related scenarios	—	Survey	Individuals can be segmented into four groups based on their level of privacy concerns: the unconcerned, circumspect, wary, and alarmed users. The groups differ in terms of age and education.
Berendt et al. (2005) [8]	Personalized online shopping recommendations	—	Experiment	Individuals differ in their willingness to reveal personal information and can be categorized into marginally concerned, identity concerned, profiling averse, and privacy fundamentalists. Yet, individuals may easily neglect their privacy concerns and disclose personal information in case there are appropriate benefits offered in return.
Treiblmaier and Pollach (2007) [59]	Personalization purposes such as purchase decisions or advertisements	—	Survey	People's perception of benefits and costs of personalization depends on their privacy valuation and the context.
Hann et al. (2007) [30]	Registration at a financial portal	Expectancy theory of motivation	Experiment	Internet users can be categorized into privacy guardians, information sellers, and convenience seekers. Those groups significantly differ in their trade-off between benefits and privacy concerns, in particular in their value of monetary rewards, convenience, and privacy protection.
Xu et al. (2011) [66]	E-commerce, social networking, financial, health-care sites	Information boundary theory	Survey	Disposition to value privacy positively influences individuals' privacy concerns and risks, but is an underdeveloped construct that needs further attention.
Li (2014) [40]	Websites in general	Information boundary theory	Survey	Disposition to value privacy positively influences situational privacy concerns, independent of contextual factors such as reputation or familiarity.

consumers cannot easily grasp its nature, they will likely hesitate to share requested information [38]. In addition, Tsai et al. [61] found that individuals are willing to pay more on websites that display privacy information in a more obvious and intuitive manner. Table 3 presents a summary of previous studies that address the notion of information-use transparency features.

Awad and Krishnan [6] also discovered the personalization–privacy paradox: consumers who value transparency features are less willing to be profiled for personalized offerings, however. They speculated that these people might be so-called privacy fundamentalists who have a high disposition to value privacy, and are thus less willing to disclose information in general and for personalized offerings in particular. Nonetheless, they argued that high-quality transparency features combined with a clear privacy policy in a privacy-safe environment may persuade these consumers to provide information for personalization. Yet, to the best of our knowledge, the usefulness of transparency mechanisms with respect to individuals' DTVP and service personalization has not been studied. It is an interesting avenue as it not only can add to our theoretical understanding but could also inform practitioners about how to design personalized services.

In summary, previous studies of the impact of personalization, DTVP, and transparency features on consumers' willingness to disclose information have found that personalizing a service offering often leads to a more positive valuation of services but may depend on situational factors such as how the personalized content is delivered and the immediacy of the benefits that a service delivers. Also, individuals largely differ in how they value privacy. Moreover, investigations of the impact of transparency features are limited in that many authors only speculate that such features may help to ease individuals' privacy concerns, but few studies have empirically tested those suggestions. Current insights on the role of individuals' DTVP and transparency features in the consumers' personalization–privacy dilemma are also scarce. We address this shortfall and improve the understanding of the trade-off between personalization and privacy. Based on information boundary theory, we expect that individuals' behavioral intentions to disclose information to services with differing levels of personalization vary depending on personal factors, namely, individuals' DTVP and situational factors such as the availability of transparency features; we test those interactions with the help of an experimental setup.

Information Boundary Theory

A broad range of established theories such as expectancy-value theory, protection motivation theory, and social response theory have been used in information privacy research [39]. This study draws on *information boundary theory* (also called *communication privacy management theory*), which explains how individuals decide what kind of personal information should be disclosed when and to whom [51, 66]. The theory, which was developed by Petronio [50, 51] and has its origin in interpersonal communication research, suggests that individuals have an informational

Table 3. Summary of Previous Research Related to Information-Use Transparency Features

Authors	Understanding of information-use transparency features	Context	Theory	Method	Main findings
Treiblmaier and Pollach (2007) [59]	Informing consumers about how personal information is used and providing mechanisms for users to change or delete it	Personalization for different purposes such as purchase decisions or advertisement	—	Interviews, survey	Consumers feel poorly informed about the actual usage of their personal information collected by organizations. Transparently communicating how consumer data are handled and how they can be changed or deleted may help to build trust and ease individuals' privacy concerns.
Tsai et al. (2011) [61]	Intuitive and accessible presentation of privacy information	Online shopping	Utility maximization theory	Experiment	In case privacy information is presented in a more salient and accessible manner (i.e., privacy icons), some consumers are willing to pay a premium to purchase from privacy protective websites.
Adjerid et al. (2013) [5]	Informing consumers about firm's data handling practices in a simple and easily accessible way	Survey about ethical questions	Cognitive biases	Experiment	The impact of privacy notices is sensitive to reference dependence and can be reduced by misdirection.

space with defined boundaries that they try to manage and control. Therefore, individuals form rules to determine which information they are willing to disclose. Those rules depend on the nature of the information to be shared, the individual's personality, environmental factors, and an interrelated risk–benefit assessment. For example, an individual may feel uncomfortable about sharing health-related information with an event recommendation service because the individual has high privacy concerns and does not see how this information could lead to a better event recommendation. At the same time, sharing information about personal recreational activities may not be seen as risky. However, when asked by a doctor, an individual might be very willing to disclose health information because of the associated benefits (i.e., a suitable treatment and cure). Individuals' boundaries can thus differ in their permeability (i.e., how thin or thick they are and which information is shared with whom), in their linkage (i.e., how strong the connection between the involved parties is), and in their ownership, which reflects the responsibilities and rights regarding the spread of information. If external parties, such as a service provider, attempt to cross those information boundaries and access information that individuals do not want to share, they may perceive this behavior as an invasion of privacy [51].

Previous research has used information boundary theory to explain the disclosure of personal information between partners in marital couples [50]. It has also been adopted by various IS researchers to study the formation of privacy concerns of website users [66] and to explain the tension between information disclosure and privacy in online commercial transactions [47], in social media [13], and in the mobile context [57].

Information boundary theory is suitable for our study for several reasons. First, it considers interrelations between benefits and risks of information disclosure that have been discovered in the context of personalized services [38, 54]. Taking into account these interrelations differentiates the theory from the often-used privacy calculus, in which risks and benefits are independently assessed and then weighted against each other [17, 18]. Second, information boundary theory illustrates the rise of an individual's privacy concerns depending on an individual's personality and related disposition to value privacy [39, 66]. Finally, the theory explains how an individual's privacy concerns and the evaluation of associated risks depend on situational factors. Such situational factors include, for example, the extent of personalization and transparency offered to a consumer [51].

Hypotheses Development

Information boundary theory acknowledges the important role of individuals' personalities in managing their information boundaries and the resulting information disclosure [51]. While individuals' previous experiences or demographic factors have been studied [66], we focus on the influence of DTVP as another facet of individuals' personalities. The literature shows that individuals differ with respect to their DTVP: while some individuals attribute high value to their privacy and thus are also highly concerned about privacy invasions, others may be more pragmatic and easily trade their privacy for benefits or may even be unconcerned about their privacy in general [40, 64]. If individuals have a general tendency to highly value their privacy, this valuation has been shown to impact how individuals evaluate different situations.

Individuals with a high DTVP are more likely to expect higher risks and thus negative outcomes associated with information disclosure [40, 66]. Therefore, we formulate our first hypothesis:

> *Hypothesis 1 (The Disposition to Value Privacy Hypothesis): Consumers who have a high disposition to value privacy are more wary of sharing personal information with an online service.*

In addition to personal factors, information boundary theory also posits that environmental factors influence individuals' decisions about how to manage their informational boundaries [51]. The personalization of a service offering is such an environmental factor. Based on the collection and analysis of information (e.g., individuals' interests and previous behavior), service providers can personalize services by preselecting what is offered to a specific user. This service personalization aims at more effectively targeting the needs of an individual and is generally perceived positively by consumers [12, 67]. Thus, in line with our theoretical perspective, we argue that the availability of personalization increases consumers' willingness to disclose information compared to an impersonalized service offering that collects the same personal information. In this case, the risks are the same but the availability of a personalized service offering increases the perceived benefit. Thus, we offer the following hypothesis:

> *Hypothesis 2 (The Personalized Service Hypothesis): Consumers are more willing to share information with an online service if the service is highly personalized.*

Providing transparency features represents another environmental factor that may influence the risk–benefit assessment of individuals when having to decide about the management of their information boundaries. Transparency features inform consumers about which information is collected and how it is used, to whom it may be passed on, and how information can be removed [6]. If individuals get to know how their information is treated, they gain a feeling of not only trust but also control [47, 59]. Drawing on information boundary theory, we argue that those perceptions make an individual more confident in being able to preserve one's information boundaries [51]. Thus, we hypothesize:

> *Hypothesis 3 (The Information-Use Transparency Features Hypothesis): Consumers are more willing to share personal information with an online service if the service exhibits transparency features.*

In the following, we take a closer look at a possible interaction between DTVP and the different levels of service personalization. As discussed above, an individual with higher DTVP will more likely expect negative outcomes associated with the disclosure of personal information (e.g., the loss of privacy) than someone with lower DTVP [66]. If we compare the risk perceptions of consumers with distinct DTVP levels but with identical information boundary penetration in a given situation (e.g., a particular personalized service offering that collects certain personal information), their perceptions of risks will differ: consumers with high DTVP will feel less in control of their information and thus have higher concerns [6, 40]. Offering personalized services to such individuals with high DTVP may even provoke not only a perception of benefits but also a stronger perception of privacy risks related to a service [6, 54, 57, 68] because consumers become more aware that their personal information is collected and analyzed to provide this service. Thus, individuals perceive stronger information boundary penetration involved in the process of personalization; and people with high DTVP who generally have great worries about their privacy are reluctant to share personal information with any service, whether it is personalized or not.

The opposite holds for consumers with low DTVP and weaker risk perceptions [66]. In this case, individuals are more willing to trade their personal information but only if substantial benefits of personalization are offered. Even more, for highly personalized services, individuals with low DTVP have higher intentions to disclose information than people with high DTVP. This relationship can be expressed as a two-way interaction between privacy valuation and personalization:

> *Hypothesis 4 (The Disposition to Value Privacy Personalization Hypothesis): For individuals with high disposition to value privacy, personalization features will have a lower influence on the willingness to share personal information with an online service than for individuals with low disposition to value privacy.*

To shed more light on the effect of transparency features and to reduce the reluctance to share personal information, we differentiate between individuals with low and high DTVP in the following. As those individuals assess risks and benefits differently [66], combined effects of transparency and personalization may differ between the two groups of individuals. Following information boundary theory, individuals with low DTVP have a generally lower tendency to preserve their private information space and are thus more willing to share information [66]. If they are in a situation with low personalization and low transparency, they see low benefits for themselves, but due to their low DTVP, they are less likely to further investigate which information might be collected. However, if low personalization is combined with high transparency, it becomes obvious that a lot of information is collected about the individual that is not used for personal advantage. Thus, they might perceive this situation as unfair because the service only offers low personalization yet unnecessarily intrudes upon their privacy boundaries and we expect them to share less information than if the level of transparency is low. If highly personalized services are offered, then individuals with a low DTVP are particularly interested in the benefits, and transparency features might even foster a feeling of fairness, as *reciprocity* (e.g., telling consumers why their data are needed and how they will be used) has been shown to increase the probability of disclosing information and thus enhances users' perceptions of justice [70].

In contrast, individuals with high DTVP have a high inherent need to maintain their information boundaries [66]. They are generally skeptical about information disclosure and have low intentions to do so, in particular for a weakly personalized service no matter the level of information-use transparency. When facing highly personalized services, however, they also see some benefits in addition to the high risks of information disclosure. Yet, attempting to establish a reciprocal relationship through transparency features might have counterproductive effects when dealing with individuals with high DTVP [70]. As such individuals focus strongly on potential losses that are associated with information disclosure, transparently communicating which information is collected and how all this information may be used can even inflate their perceived privacy risks and lead to higher privacy concerns by strengthening their perception of boundary intrusion. We hypothesize:

> *Hypothesis 5 (The Disposition-Specific Transparency Personalization Hypothesis): For individuals with high disposition to value privacy, the availability of transparency features will reduce the impact of personalization on the willingness to share personal information with a service, whereas for individuals with low disposition to value privacy, the availability of transparency features will increase the impact of personalization on information disclosure intentions.*

Methodology

Experimental Scenarios and Procedure

To make our experiment as realistic as possible, participants were presented with a cover story about a new online service supporting users in finding relevant events that match their preferences. According to the scenario, the new website was under construction and would be launched shortly. The participants were encouraged to evaluate the service based on website screenshots. To obtain an authentic setting for our experiment, we designed the service description in line with existing event recommendation services (such as eventim.de, eventbrite.com, eventempfehlung.de) that allow individuals to browse upcoming events and book them via the website. To do so, individuals have to enter event preferences and create a user account storing their name, date of birth, contact details such as e-mail and physical address, and payment details. The service also tries to collect additional information such as event category preferences, education, current occupation, income, lifestyle, and family details and to connect to social media data to further improve event recommendations. After the service description that differed between subjects as described below, participants were asked to complete a questionnaire about their perception of the service.

An experimental 2 × 2 factorial design was chosen. This choice allowed us to design and control the independent variables of personalization and transparency features, combine it with the personality trait of DTVP, and to include several potential covariates. At the same time, this setup enabled the conduct of our online experiment within the natural Internet environment for users of personalized services. Moreover, the scenario-based method facilitated the investigation of future states from the respondents' contemporary perspectives [54]. Participants were randomly assigned to four distinct scenarios. As we employed a between-subject design, each subject was exposed to only one experimental condition. This design allowed us to prevent any carryover effects that are likely to occur in within-subject designs [23].

The experimental treatments were personalization (low versus high) and information-use transparency (low versus high). The distinct levels of personalization in this experiment were determined by the extent to which the service is able to find relevant events, provide recommendations, and tailor its newsletter to consumers' actual preferences and online behavior. In the low personalization condition, users were able to search events according to their tastes or browse one of the proposed event categories. However, the high personalization treatment not only facilitated personalized search but also offered accurately tailored event recommendations, an individualized newsletter, and the option to integrate events into a user's personal calendar.

The level of information-use transparency is reflected by the extent to which an online service provider informs users about how and for what purposes acquired information is used as well as about which control features are available as required by law (e.g., the right to be forgotten [20, 21]). Thus, the service's terms of use regarding data collection and analysis were the same in both transparency treatments. In the low transparency setting, however, only the website's privacy policy was available to participants via a link provided below the website screenshot. This manipulation reflects a realistic scenario that most online service users face (i.e., the status quo). In the high transparency condition, we provided users with explicit information about the purposes for which consumer data were gathered and used and for how long it would be stored (see Appendix Figure A1). It also highlighted the consumer's right to oppose the processing of personal data for legitimate reasons. Finally, an overview of the personal information stored in the company's database was depicted. We particularly chose information that an event recommendation service might legitimately ask for to offer a personalized service experience.

After being confronted with the stimulus material, we assessed individuals' DTVP. Since DTVP is a personality trait, we could not manipulate this independent variable; instead, we measured it after the manipulation took place.[3] We also assessed the participants' understanding of the proposed service offer with control questions, the respondents' overall experience with online personalization offerings, and previous encounters with event recommendation services as potential confounding variables. The test subjects also indicated their intentions to disclose information to the described service and had to answer manipulation check items. Last, we collected demographic information and debriefed the participants on the study's actual background.

Measurement of Constructs

We adapted constructs from measurement scales used in prior studies to fit the context of personalized event recommendations. Our survey questions are statement-like items that are rated on a seven-point Likert scale. We generally used at least three or four items per construct to adequately identify the construct and to assess its validity [29]. We used several items to measure individuals' DTVP [40, 66]. To measure the intention to disclose information (ID), we adapted the scale of Malhotra et al. [46]. We also included control variables such as gender, age, education, income level, Internet use, and experience with the Internet (EXPI) that were employed by previous studies [38, 40, 66, 68]. In addition, we measured participants' experiences with online personalization [25] and whether they had used similar event recommendation services in the past (EXPP) [38, 68]. The measurement model is depicted in Table 4.

Sampling and Participants

We conducted a pilot test with 28 participants to determine whether our manipulations worked effectively. The pretest was also used to assess the clarity and conciseness of the instructions and items. All test subjects were encouraged to give qualitative feedback. Their reviews were used to shorten the questionnaire and to improve the wording and layout of a few items.

The data for our main study were collected in April 2016. We conducted our scenario-based experiment online. This is an appropriate way to reach potential users of an event recommendation service because regular online access is required to use such services. German participants were recruited via e-mail, social networks, forums, and local online classified advertisements. To assure the high quality of our data set, we applied a data-cleaning process to detect satisficing participants. We deleted answers with very low response times and respondents who failed to answer a control question [45]. Remaining were 286 valid responses. To obtain a medium effect size ($f = 0.25$) with a power of 0.80 at a 0.05 significance level, the required total sample size is 128. Thus, the size of the sample should be sufficient to observe medium effects. Demographics and descriptive statistics are presented in Table 5. We tested the distribution of gender, age, income, occupation, Internet experience, and experience with personalized services among our different groups and did not find any significant differences.

Findings

Manipulation Check

Before proceeding with the analysis of the differences in behavioral intentions among the test groups, a manipulation check was carried out. Perceived personalization of the

Table 4. Measurement Model

Constructs	Definition	ID	Items
Intention to disclose information [46]	The extent to which an individual would reveal personal information to use a particular service offering		In order to use the offered service . . .
		ID_01	. . . I would make the necessary data available.
		ID_02	. . . it is probable that I would disclose the required information.
		ID_03	. . . I am willing to provide the relevant data.
Disposition to value privacy [40, 65]	A personality attribute that represents a person's general need to preserve specific information boundaries in order to frame their personal space in different situations and contexts		Compared to others . . .
		DTVP_01	. . . I am more sensitive about the way online companies handle my personal information.
		DTVP_02	. . . I see more importance in keeping personal information private in Internet transactions.
		DTVP_03	. . . I am less concerned about potential threats to my personal privacy on the Internet (reversed).
		DTVP_04	. . . I tend to reveal as little information as possible in online transactions.
Experience with the Internet [24, 47]	A user's familiarity with and confidence in using the Internet	EXPI_01	I have a great deal of experience with the Internet.
		EXPI_02	I am very confident in using the Internet.
		EXPI_03	I am familiar with the different possibilities of using the Internet.
Experience with online personalization [25, 48]	A user's familiarity with and confidence in using personalized online services	EXPP_01	I have a great deal of experience with personalized online services.
		EXPP_02	I am very confident in using personalized online services.
		EXPP_03	I am familiar with the different possibilities of using personalized online services.

Table 5. Respondents' Characteristics

Variable	Category	Respondents	Percentage
Gender	Female	191	66.8
	Male	95	33.2
Age group	18–25	118	41.3
	26–34	89	31.1
	35–44	23	8.0
	45–54	36	12.6
	55–64	19	6.6
	65 or more	1	0.3
Occupation	In training	154	53.8
	Working	119	41.6
	Not employed	9	3.1
	Other	4	1.4
Internet usage (hours per day)	Less than 1	24	8.4
	1–2	71	24.8
	3–4	98	34.3
	5–6	53	18.5
	7–10	30	10.5
	10 or more	7	2.4
	Not specified	3	1.0
Experience with event recommendation services	Yes	54	18.9
	No	232	81.1

service offering was evaluated based on four items (e.g., "The described service provides me with event recommendations that may suit my interests"), which were measured on a seven-point Likert scale. Perceived information-use transparency was measured with four items (e.g., "I can see at a glance which data are collected, what the data are used for, how long the data will be stored, and how I can control the usage of my data"). The independent sample *t*-tests revealed that our participants distinguished between different levels of personalization and information-use transparency across the designed conditions. In the high personalization setting, respondents rated personalization as higher compared to the low personalization setting ($M\Delta = -0.38$; $t(284) = -3.28$, $p < 0.005$). Similarly, information-use transparency received higher scores in the high transparency conditions than in the low transparency conditions ($M\Delta = -1.02$; $t(268.80) = -10.53$, $p < 0.001$).

Moreover, we investigated the interaction between individuals' DTVP, personalization, and transparency. To show that the manipulations did not influence the personality trait DTVP, we conducted an analysis of variance with DTVP as a dependent variable and transparency and personalization as independent variables. As expected, we did not obtain any significant main effects or interaction effects. Thus, DTVP is not significantly different across the treatments, and we conducted a median split and used two groups with low and high DTVP, respectively, in our subsequent analysis.

Measurement Model Validation

Confirmatory factor analysis was used to assess the validity and reliability of our latent variables DTVP, ID, EXPI, and EXPP. We employed principal components analysis with varimax rotation. As expected, we obtained four factors with eigenvalues greater than one. A total of 82.36 percent of the variance can be explained by these four factors. Then we derived factor scores using the regression method for further analysis. A summary of the measurement model assessment is given in Table 6.

To assess the convergent validity of the measured reflective constructs, we checked the factor loadings (all above 0.7), reliability of items (Cronbach's α exceeds 0.7 for all constructs), and average variance extracted (AVE, above 0.5 for all constructs so that the latent construct accounts for the majority of the variance of its indicators) [29, 43].

The discriminant validity of the measurement instrument was evaluated in two steps. First, we investigated whether the items loaded more strongly on their corresponding construct than on other constructs in the model. This criterion was fulfilled and indicates that all constructs share more variance with their indicators than with other latent constructs. Second, we tested the Fornell–Larcker criterion, which suggests that the square root of the AVE for each variable should be greater than its correlation with any other construct in the model [24]. All latent variables fulfilled this criterion. The correlation matrix for all latent constructs is given in Table 7. In summary, we can conclude that our measurement instrument fulfills the requirements of convergent and discriminant validity.

Table 6. Statistics for the Latent Constructs

Constructs	Items	Factor loadings	Mean	Std. dev.	Chronbach's α	AVE
Intention to disclose information	ID_01	0.96	4.02	1.66	0.95	0.91
	ID_02	0.96	4.10	1.68		
	ID_03	0.95	4.04	1.65		
Disposition to value privacy	DTVP_01	0.90	4.47	1.68	0.84	0.69
	DTVP_02	0.88	4.88	1.68		
	DTVP_03	0.72	4.71	1.76		
	DTVP_04	0.80	4.88	1.72		
Experience with Internet	EXPI_01	0.93	5.77	1.25	0.93	0.87
	EXPI _02	0.95	5.67	1.26		
	EXPI _03	0.92	5.73	1.24		
Experience with online personalization	EXPP_01	0.92	3.41	1.69	0.92	0.87
	EXPP_02	0.93	3.46	1.73		
	EXPP_03	0.94	3.47	1.72		

Table 7. Correlations Between Latent Constructs

Constructs	Intention to disclose information	Disposition to value privacy	Experience with Internet	Experience with online personalization
Intention to disclose information	**0.95**			
Disposition to value privacy	–0.35***	**0.83**		
Experience with Internet	0.14*	–0.17**	**0.93**	
Experience with online personalization	0.27***	–0.19**	0.49***	**0.93**

Notes: Significance: ***p < .001; **p < .01; *p < .05. The square root of the average variance extracted is displayed on the diagonal in bold font.

Results

To analyze our data, we conducted an *analysis of covariance* (ANCOVA) with personalization, transparency, and DTVP as independent variables and intention to disclose as the dependent variable after checking that all necessary assumptions of ANCOVA were fulfilled.[4] With regard to potential covariates, we first included all control variables. Experience with personalization was the only significant covariate and was thus the only covariate included in our final model. Moreover, even though we did not hypothesize any interactions between the level of personalization and information-use transparency as well as between DTVP and information-use transparency, we ran a fully specified model and included those interaction terms in our analysis as their omission may lead to biased estimates [9] (see Table 8).

Regarding the main effects, we find a significant impact of DTVP on disclosure intentions ($F(1,275) = 12.08$, $p < 0.001$). Our results also suggest that personalization has a strong impact on intention to disclose ($F(1,275) = 6.17$, $p < 0.05$). Yet, before we can actually interpret those findings, we have to investigate all interaction terms to determine whether any disordinal interactions are present that may lead to erroneous interpretations of those main effects. As we can see in Table 8, the interaction effect between personalization and DTVP ($F(1,275) = 7.04$, $p < 0.01$) is the only significant interaction. Thus, we can directly conclude that the results of the ANCOVA support the “Disposition to Value Privacy Personalization Hypothesis” (H4). The interaction effect is depicted graphically in Figure 1.

To assess this interaction in more detail and to be able to further evaluate our main effects, we applied simple main effects analysis to determine which groups differed from each other with regard to individuals’ disclosure intentions.[5] As a result, we can observe that individuals with low DTVP have significantly higher intentions to disclose

Table 8. ANCOVA Results

Source	Type III sum of squares	DF	Mean square	*F*	Significance
Corrected Model	45.41	8	5.68	6.57	< 0.001***
Intercept	0.001	1	0.00	0.00	0.97
Disposition to Value Privacy (DTVP)	10.44	1	10.44	12.08	< 0.001***
Transparency Features (TRANS)	1.42	1	1.42	1.64	0.20
Personalization (PERS)	5.33	1	5.33	6.17	0.01*
Experience with Online Personalization	18.90	1	18.90	21.87	< 0.001***
DTVP x TRANS	0.02	1	0.02	0.02	0.89
DTVP x PERS	6.09	1	6.09	7.04	< 0.01**
TRANS x PERS	0.12	1	0.12	0.13	0.72
DTVP x TRANS x PERS	1.48	1	1.48	1.71	0.19
Error	237.59	275	0.86		
Total	283.00	284			
Corrected Total	283.00	283			

Notes: Dependent variable: Intention to disclose information. Significance: *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$.

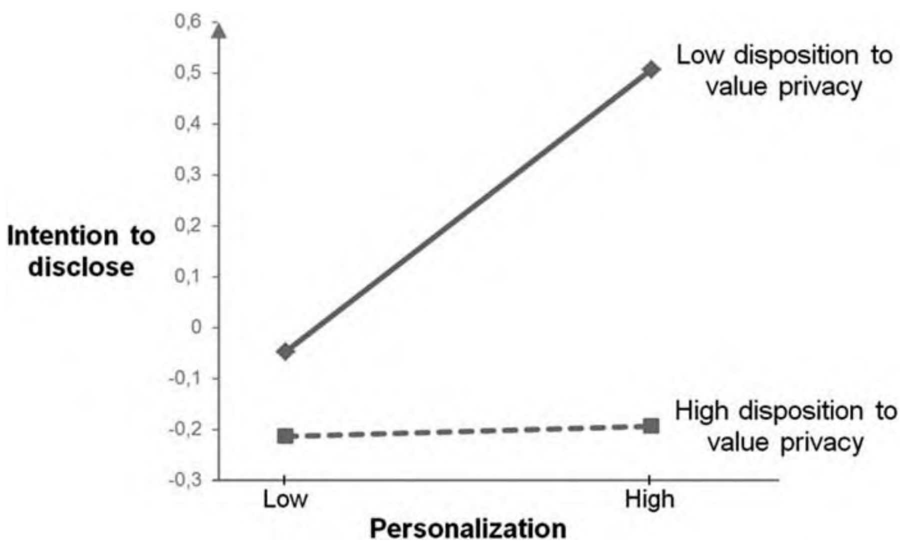

Figure 1. Interaction Effect Between Personalization and Disposition to Value Privacy

information to the highly personalized service compared to their disclosure intentions regarding the poorly personalized alternative ($F(1,275) = 13.06$, $p < 0.001$), but there are no differences for individuals with high DTVP ($F(1,275) = 0.02$, $p > 0.05$) (see Appendix Table A1). Moreover, in the highly personalized scenario, subjects with low DTVP have significantly higher disclosure intentions than individuals with high DTVP ($F(1,275) = 19.03$, $p < 0.001$), while there are no differences in the low personalized setting ($F(1,275) = 0.35$, $p > 0.05$) (see Appendix Table A2). Our data therefore indicate that we do not have any opposite effects of DTVP or personalization, so we can also conclude that our "Disposition to Value Privacy Hypothesis" (H1) and our "Personalized Service Hypothesis" (H2) are supported.

Surprisingly, transparency features have no influence on disclosure intention ($F(1,275) = 1.64$, $p > 0.05$). Therefore, the "Information-use Transparency Features Hypothesis" (H3) is not supported by our study. Moreover, no significant interaction was found among the distinct levels of personalization, transparency, and DTVP ($F(1,275) = 1.71$, $p > 0.05$). The differences in disclosure intentions between the services with low and high levels of personalization are not statistically significant across distinct levels of information-use transparency for both types of individuals either with low or high DTVP. Hence, the "Disposition-Specific Transparency Personalization Hypothesis" (H5) is not supported by the data. To gain deeper insights into this finding, we also conducted an analysis of simple main effects (see Appendix Table A3). As expected, none of the differences are significant but these details will help future researchers to interpret and build on this finding.

Finally, the covariate for experience with personalization was significantly related to the participants' intentions to disclose information ($F(1,275) = 21.87$, $p < 0.01$). The β-value for the covariate was positive ($\beta = 0.26$, $t = 4.68$, $p < 0.01$), which suggests a positive relationship between experience with personalization and intention to disclose information.

Discussion and Conclusion

The objective of our study was to investigate how individuals' privacy dispositions, the personalization of a service, and transparency features influence their intention to disclose information. In the following, we discuss our results regarding the three factors and their interactions, and highlight how our results support, extend, and contradict prior studies.

First, we found that personalization itself motivates information disclosure. Our results complement prior studies suggesting that personalization increases the perceived benefits of a service [7, 67] and that many consumers provide data to enjoy those benefits [12].

Second, our results highlight how the valuation of privacy influences individuals' willingness to disclose information. We found that those who value privacy are less willing to be profiled online. This is in line with the personalization–privacy paradox first discovered by Awad and Krishnan [6]. At the same time, our results indicate that this phenomenon is not limited to the area of personalization. Instead, we found support for this relationship independent of the level of service personalization. Nevertheless, the negative relationship is stronger if the data are used for highly personalized services. In line with information boundary theory, we found that individuals' valuations of privacy interact with situational characteristics [3] such as the level of service personalization. Individuals with low DTVP are more willing to trade their privacy for personalization benefits compared to individuals with high DTVP who do not equally appreciate information disclosure. The latter ones tend to protect their information boundaries from intrusions of highly personalized services and mostly avoid sharing personal information in exchange for any benefits. In contrast, individuals with low DTVP are willing to open their information boundaries but only if they benefit from this opening, for example, in terms of personalized service offerings.

Third, we found that transparency features do not directly impact the information disclosure of individuals. This is surprising since it is often suggested that making procedures transparent could be a fruitful path to motivate information sharing [61]. We also found no situational effect of transparency features, for instance, in situations where personalization creates additional benefits. This lack of significance cannot be explained by temporal alleviation of information [5] because our subjects were able to recite the transparency information made available to them even after significant delay. Although available in all conditions, transparency features also created increased awareness of the control that legislators have implemented for privacy protection. Based on prior studies, this should have further increased the impact of the transparency features [2]. Nevertheless, the inclusion of transparency features did not considerably change individuals' behavioral intentions.

A potential explanation for our finding about the lack of significance of transparency features is a duality of effects of transparency features. We expected that transparency features provide information that is relevant for rational decision making and would tend to be a positive force [70]. However, the information displayed in a consumable way is not only a signal of fairness [70] but also increases individuals' privacy concerns, which results in concealing personal data [35]. This reverse impact of transparency features can also be found in studies on personalized advertisements. Although consumers respond positively to firms' implicit use of personal information (e.g., product-based e-mail recommendations), individuals' responses to personalized greetings (e.g., a consumer's name) were negative because the use of consumers' information was explicit and gave rise to privacy concerns [63].

This duality can also explain the lack of an interaction between DTVP, personalization, and transparency. We expected that the combination of personalization and transparency features might have counterproductive effects for individuals with high DTVP because transparency would reinforce their prevailing caution. At the same time, we argued that individuals with low DTVP would perceive it as fair if they were told how and what data were used to offer highly personalized services. In the case of low personalized service offerings, we hypothesized that the availability of transparency features would raise individuals' awareness that a lot of information is collected but not used to an individuals' personal advantage, so that this should lower individuals' disclosure intentions. However, even though the simple main effects analysis revealed differences pointing in the expected directions (see Appendix Table A3), none of those differences were significant. This lack of significance implies that if any effect existed at all, it would require a significantly larger sample to detect it, and its impact on digital services would be negligible or small. Thus, we can conclude that the contrary influences of transparency features apply in ways that are independent of the personal disposition and personalization features. These findings have important implications for firms and policymakers.

Our study makes theoretical contributions in two ways. First, we provide empirical support for the personalization–privacy paradox in an experimental setting where the quality of the privacy policy is controlled. We confirm its general proposition but find that the postulated relationship—although much stronger in the context of personalized services—is not limited to services with personalization. Instead, it also holds for other types of digital services that require personal information. Second, we show that transparency features do not help to reduce reluctance to share personal information. We show that there is no general impact of transparency features, although it is frequently postulated [61], nor does their impact depend on personalization features or privacy dispositions. We explain this difference with the dual perception that transparency features trigger. Fostering trust and fairness perceptions, transparency can help to drive information disclosure but also makes privacy issues explicit and individuals hesitant.

Our study also has practical implications. Businesses that want to collect personal information when offering digital services can benefit from knowledge about the privacy dispositions of their consumers. While people with low DTVP are willing to disclose personal information if they receive benefits, people who emphasize their privacy seem to be more skeptical and have lower intentions to disclose information. Personalized services could convince the former segment to share personal data, yet such benefits do not change the intent of people who emphasize their privacy; this makes it very difficult for businesses to offer personalized services for this consumer segment. At the same time, organizations that have invested a considerable amount in making their information-handling behavior more transparent [26, 52] should redirect those expenses to other endeavors. Organizations should either try to focus on attracting individuals with lower DTVP or to further investigate how individuals with higher DTVP could be persuaded to share the necessary information, for instance, by trying to tackle their general disposition toward privacy, as done by firms such as Google [15, 27, 55]. At the same time, policymakers must react to the fact that making information collection and use transparent is not perceived positively. Policymakers must aim to create a general awareness among their citizens that shared information can be used for positive as well as negative purposes. This is in line with repeated calls that more education regarding privacy is necessary [3]. Once this general goal is achieved, transparency features have the potential to differentiate quality providers from those who try to hide their behavior.

We note several limitations of our study that offer avenues for future research. First, we selected an experimental setting to control individuals' interactions with the website and isolated the effects of personalization and transparency features. In the next steps, a field experiment using a real website or a mobile application will likely provoke stronger perceptions of privacy risks regarding information-use transparency and information sharing. Also, this experimental setup could be used to assess feelings of reciprocity and fairness. Second, we measured self-reported consumer intentions instead of actual behavior. Tricking individuals to share actual private data in an experimental setting using the wrong leads is unethical; thus, our results do not account for potential differences between intention and behavior [49]. Investigating individuals in real-world settings would also have led to considerable selection bias with regard to privacy dispositions, since participants who opt to use those services have already made an adoption decision. Our experimental design allowed us to investigate participants independently of their attitudes toward privacy and personalization. Nevertheless, our results on transparency and personalization features could benefit from a validation using a real website or mobile application. Third, our counterintuitive findings regarding the impact of transparency features and their interactions open up avenues for future studies that can try to isolate and channel its opposing impacts.

The personal data of consumers allow digital businesses to improve or monetize their services. However, it is difficult for firms to overcome the general hesitations of consumers to gain permission for access to these data, especially for consumers who put special emphasis on their privacy. Our study reveals a strong interaction between privacy valuation and offering personalized services toward information disclosure. For people with low DTVP, the personalization of a service offering had a strong effect on intentions of disclosing information, but personalization did not convince people with high privacy valuation to disclose information. In contrast to our expectations, our investigation of information disclosure revealed neither a direct impact of transparency features nor an interaction effect in the network with privacy disposition and personalization. We tried to explain this finding by theorizing about the reverse impacts of transparency features. As a result, our study provides the first causal experimental evidence on previously postulated relationships. Regarding other aspects, this study contradicts prior knowledge and creates opportunities for future research as well as challenges for policymakers. Finally, this research provides guidance for firms seeking to succeed in an age where personal data are the prime currency.

Acknowledgments: An earlier version of this article was published in the *Proceedings of the Hawaii International Conference on System Sciences* (HICSS). The authors are very grateful to the guest editors Eric Clemons, Rajiv Dewan, Rob Kauffman, and Thomas Weber, editorial assistant Emmy Hoang Ai Phuong, and three anonymous reviewers for their valuable suggestions and encouragement during the development of this manuscript. The authors also appreciate the constructive feedback of HICSS 2017 minitrack "Information Security and Privacy" participants and cochairs, Tung Bui and Eric Clemons, on the preliminary version of this study. Moreover, fruitful discussions with seminar participants at the University of Augsburg helped the authors to strengthen the study. The authors also thank the Competence Center for Global Business Management of the University of Augsburg for funding part of this research.

Notes

1. We refer to *information-use transparency* as the extent to which an online firm provides features that allow consumers to access the data collected about them and informs them about how and for what purposes the acquired information is used [6]. Information-use transparency differs from other types of *information transparency*, which was defined as the level of availability and accessibility of market information to its participants [69]. Here, information-use transparency refers to information about the individual, whereas information transparency refers to the access to information about price, product, inventory, cost, and processes in a marketplace [28]. The latter type of transparency has found further resonance in the marketing and information systems literature investigating consumer informedness. Consumer informedness about products and prices can be influenced strategically to guide consumers' choices [14, 37]. In contrast to informedness about vendors, products, and prices, the information-use transparency features investigated in this study facilitate consumers' informedness about firms' dealings with their personal data. While both types of transparency can be controlled by firms strategically, the exploitation of consumers' private information involves severe risk for the individual.

2. As transparency and control features are often discussed in combination [2, 59], we would like to point out the difference between the two types of features as we manipulate the availability of transparency features as part of our experiment while keeping the availability of control features constant. *Transparency features* aim at informing consumers about which data is collected, how it may be used, or to whom it may be passed on; thus, these features are a passive instrument [4]. On the other hand, *control features* enable consumers to actively manage who has access to which piece of information, thus providing consumers with the possibility to control the release and the accessibility of information [10].

3. The test described in the section "Manipulation Check" indicates that DTVP is independent of the manipulations of personalization and transparency. An alternative approach of dealing with individuals' DTVP as an independent variable would have been to categorize individuals into groups with high and low DTVP in advance of running the experiment. We could then pull in people at random from the two groups to ensure that an equal number of individuals from each group were assigned to each treatment. Depending on the way the groups were formed, this approach could have led to two different types of potential biases: if measured explicitly in advance, individuals would be confronted with questions about their privacy valuation in comparison to others. This might have raised their awareness for privacy issues and thus might have influenced the way they evaluate the personalization and information-use transparency treatments that were presented as part of the experiment. If the two groups were formed implicitly by inferring privacy valuation from behavior (e.g., service use by sampling users from privacy-sensitive services such as Threema or ProtonMail, and nonsensitive services such as Gmail or Facebook messenger), individuals would previously have self-selected into those groups. As we know from adoption research, such decisions are based on a plentitude of individual characteristics that would then characterize and bias the two groups. In light of those considerations, we decided to measure DTVP once the treatments were displayed. Our treatment groups were sufficiently large at about 70 participants. As individuals were randomly assigned to the treatments, each group included the same distribution of individuals with low and high DTVP. This permitted us to further split up the treatment groups according to individuals' DTVP for further analysis.

4. Before proceeding with our analysis, we assessed the assumptions for ANCOVA in five ways [22, 29]. First, we ensured the normal distribution of the dependent variable in each experimental condition through analysis of quantile-quantile plots, the Kolmogorov–Smirnov test, and outlier analysis. Second, we tested whether there is heteroskedasticity among the

experimental groups using Levene's test; the result was insignificant. Third, we assessed the correlation between the covariate and the dependent variable, and found a significant bivariate correlation between experience with personalization and information disclosure. Fourth, we checked the independence between the covariate and the independent variables using one-way analysis of variance with the groups as predictors and experience with personalization as the dependent variable. The analysis indicated no significant differences among treatments. Fifth, we tested whether there is homogeneity of regression slopes for the dependent variable and the covariate. The interactions between the independent variables and experience with personalization were all insignificant. In summary, we conclude that ANCOVA is well-suited to analyze our data set.

5. We applied the conservative Bonferroni correction [22] to account for potential Type I error inflation in the simple main effects analysis.

References

1. Ackerman, M.S.; Cranor, L.F.; and Reagle, J. Privacy in e-commerce: Examining user scenarios and privacy preferences. In *Proceedings of the First ACM Conference on Electronic Commerce*. New York, NY: ACM Press, 1999, pp. 1–8.
2. Acquisti, A.; Adjerid, I.; and Brandimarte, L. Gone in 15 seconds: The limits of privacy transparency and control. *IEEE Security Privacy*, *11*, 4 (July 2013), 72–74.
3. Acquisti, A.; Brandimarte, L.; and Loewenstein, G. Privacy and human behavior in the age of information. *Science*, *347*, 6221 (January 2015), 509–514.
4. Acquisti, A., and Gross, R. Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences*, *106*, 27 (July 2009), 10975–10980.
5. Adjerid, I.; Acquisti, A.; Brandimarte, L.; and Loewenstein, G. Sleights of privacy: Framing, isclosures, and the limits of transparency. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*. New York, NY: ACM Press, 2013, Article Number 9.
6. Awad, N.F., and Krishnan, M.S. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*, 1 (March 2006), 13–28.
7. Benlian, A. Web personalization cues and their differential effects on user assessments of website value. *Journal of Management Information Systems*, *32*, 1 (Spring 2015), 225–260.
8. Berendt, B.; Günther, O.; and Spiekermann, S. Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM*, *48*, 4 (April 2005), 101–106.
9. Brambor, T.; Clark, W.R.; and Golder, M. Understanding interaction models: Improving empirical analyses. *Political Analysis*, *14*, 1 (Winter 2006), 63–82.
10. Brandimarte, L.; Acquisti, A.; and Loewenstein, G. Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science*, *4*, 3 (May 2013), 340–347.
11. Chellappa, R.K. and Shivendu, S. An economic model of privacy: A property rights approach to regulatory choices for online personalization. *Journal of Management Information Systems*, *24*, 3 (Winter 2007/2008), 193–225.
12. Chellappa, R.K., and Sin, R.G. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*, 2–3 (April 2005), 181–202.
13. Child, J.T.; Pearson, J.C.; and Petronio, S. Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology*, *60*, 10 (October 2009), 2079–2094.
14. Clemons, E.K.; Gao, G.; and Hitt, L. When online reviews meet hyperdifferentiation: A study of the craft beer industry. *Journal of Management Information Systems*, *23*, 2 (October 2006), 149–171.
15. Constine, J. Facebook lobbying spend up 196%, Google up 70% in 2012 to try to sway privacy, anti-trust legislation. 2013. Available at: http://social.techcrunch.com/2013/01/23/google-facebook-lobbying-spend/ (accessed on March 30, 2017).

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

17. Culnan, M.J., and Bies, R.J. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*, 2 (July 2003), 323–342.

18. Dinev, T., and Hart, P. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*, 1 (March 2006), 61–80.

19. Dinev, T.; Hart, P.; and Mullen, M.R. Internet privacy concerns and beliefs about government surveillance: An empirical investigation. *Journal of Strategic Information Systems*, *17*, 3 (September 2008), 214–233.

20. European Parliament. Directive 95/46/EC of the European Parliament and of the Council.Official Journal L 281, 23/11/1995 P. 0031-0050; October 1995. Available at: http://eur- lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=DE (accessed on April 5, 2017)

21. European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council. April 2016. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (accessed on April 5, 2017)

22. Field, A. *Discovering Statistics Using IBM SPSS Statistics*. London, UK: Sage, 2013.

23. Field, A., and Hole, G. *How to Design and Report Experiments*. London, UK: Sage, 2002.

24. Fornell, C., and Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*, 1 (February 1981), 39–50.

25. Frambach, R.T.; Roest, H.C.A.; and Krishnan, T.V. The impact of consumer Internet experience on channel preference and usage intentions across the different stages of the buying process. *Journal of Interactive Marketing*, *21*, 2 (March 2007), 26–41.

26. Google. Transparency, choice and control—now complete with a Dashboard! Official Google Blog. November 5, 2009. Available at: https://googleblog.blogspot.com/2009/11/transparency- choice-and-control-now.html (accessed on April 5, 2017)

27. Google. Google Privacy |Why data protection matters. 2017. Available at: http://privacy.google.com/intl/en_ALL/your-data.html (accessed on April 5, 2017)

28. Granados, N.; Gupta, A.; and Kauffman, R.J. Research commentary—information transparency in business-to-consumer markets: Concepts, framework, and research agenda. *Information Systems Research*, *21*, 2 (December 2009), 207–226.

29. Hair, J.F.; Black, W.C.; Babin, B.J.; and Anderson, R.E. *Multivariate Data Analysis*. Upper Saddle River, NJ: Pearson, 2009.

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

31. Harris Interactive. Privacy on and off the internet: What consumers want. Rochester, NY, 2002. Available at: http://www.ijsselsteijn.nl/slides/Harris.pdf (accessed on June 8, 2016)

32. Ho, S.Y. Opportunities and challenges of mobile personalization: An exploratory study. In *Proceedings of the Seventeenth European Conference on Information Systems*. Verona, Italy. Atlanta, GA: Association for Information Systems, 2009, pp. 1211–1222.

33. Hong, S.-J., and Tam, K.Y. Understanding the adoption of multipurpose information appliances: The case of mobile data services. *Information Systems Research*, *17*, 2 (June 2006), 162–179.

34. Hui, K.-L.; Teo, H.H.; and Lee, S.-Y.T. The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*, 1 (March 2007), 19–33.

35. John, L.K.; Acquisti, A.; and Loewenstein, G. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, *37*, 5 (February 2011), 858–873.

36. Jones, A. Identity and marketing: Capturing, unifying, and using customer data to drive revenue growth. San Francisco, 2015. Available at: http://insight.venturebeat.com/report/customer-identity-marketing-capturing-storing-and-enriching-right-data (accessed on June 8, 2016)

37. Li, T.; Kauffman, R.J.; Van Heck, E.; Vervest, P.; and Dellaert, B.G. Consumer informedness and firm information strategy. *Information Systems Research*, *25*, 2 (May 2014), 345–363.

38. Li, T., and Unger, T. Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, *21*, 6 (November 2012), 621–642.

39. Li, Y. Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*, 1 (December 2012), 471–481.

40. Li, Y. The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57* (January 2014), 343–354.

41. Liang, T.-P.; Lai, H.-J.; and Ku, Y.-C. Personalized content recommendation and user satisfaction: Theoretical synthesis and empirical findings. *Journal of Management Information Systems*, *23*, 3 (Winter 2006/2007), 45–70.

42. Lowry, P.B.; Cao, J.; and Everard, A. Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*, 4 (Spring 2011), 163–200.

43. MacKenzie, S.B.; Podsakoff, P.M.; and Podsakoff, N.P. Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*, 2 (June 2011), 293–334.

44. Mai, B.; Menon, N.M.; and Sarkar, S. No free lunch: Price premium for privacy seal-bearing vendors. *Journal of Management Information Systems*, *27*, 2 (December 2014), 189–212.

45. Malhotra, N. Completion time and response order effects in web surveys. *Public Opinion Quarterly*, *72*, 5 (January 2008), 914–934.

46. Malhotra, N.K.; Kim, S.S.; and Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*, 4 (December 2004), 336–355.

47. Metzger, M.J. Communication privacy management in electronic commerce. *Journal of*
34 *Computer-Mediated Communication*, *12*, 2 (January 2007), 335–361.

48. Murray, K.B., and Schlacter, J.L. The impact of services versus goods on consumers' assessment of perceived risk and variability. *Journal of the Academy of Marketing Science*, *18*, 1 (Winter 1990), 51–65.

49. Norberg, P.A.; Horne, D.R.; and Horne, D.A. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*, 1 (June 2007), 100– 126.

50. Petronio, S. Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, *1*, 4 (November 1991), 311–335.

51. Petronio, S. *Boundaries of Privacy*. Albany, NY: State University of New York Press, 2002.

52. Rogers, M., and Myerson, T. Windows 10 privacy journey continues: More transparency and controls for you. Windows Experience Blog. April 5, 2017. Available at: https://blogs.windows.com/windowsexperience/2017/04/05/windows-10-privacy-journey-continues-more-transparency-and-controls-for-you/ (accessed on April 6, 2017)

53. Sheehan, K.B. Toward a typology of Internet users and online privacy concerns. *Information Society*, *18*, 1 (January 2002), 21–32.

54. Sheng, H.; Nah, F.F.-H.; and Siau, K. An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, *9*, 6 (June 2008), 344–376.

55. Smith, C. Google Ad Preferences thinks it knows who you are, what you search. *Huffington Post*. January 27, 2012. Available at: http://www.huffingtonpost.com/2012/01/27/google-ap-35preference_n_1237054.html (accessed on March 30, 2017)

56. Smith, H.J.; Dinev, T.; and Xu, H. Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*, 4 (December 2011), 989–1016.

57. Sutanto, J.; Palme, E.; Tan, C.-H.; and Phang, C.W. Addressing the personalization–privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, *37*, 4 (December 2013), 1141–1164.

58. Thirumalai, S., and Sinha, K.K. To personalize or not to personalize online purchase interactions: Implications of self-selection by retailers. *Information Systems Research*, *24*, 3 (March 2013), 683–708.

59. Treiblmaier, H., and Pollach, I. Users' perceptions of benefits and costs of personalization. In *Proceedings of the Twenty-Eightth International Conference on Information Systems*, Montreal, Canada. Atlanta, GA: Association for Information Systems, 2007, Article Number 141.

60. TRUSTe. TRUSTe/National Cyber-Security Alliance: U.S. consumer privacy index, 2016. San Francisco, 2016. Available at: https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/ (accessed on June 12, 2016)

61. Tsai, J.Y.; Egelman, S.; Cranor, L.; and Acquisti, A. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*, 2 (June 2011), 254–268.

62. Wattal, S.; Telang, R.; and Mukhopadhyay, T. Information personalization in a two-dimensional product differentiation model. *Journal of Management Information Systems*, *26*, 2 (Fall 2009), 69–95.

63. Wattal, S.; Telang, R.; Mukhopadhyay, T.; and Boatwright, P. What's in a "Name"? Impact of use of customer information in e-mail advertisements. *Information Systems Research*, *23*, 3–1 (November 2011), 679–697.

64. Westin, A.F. *Privacy and Freedom*. New York, NY: Atheneum, 1967.

65. Xu, H.; Dinev, T.; Smith, H.; and Hart, P. Examining the formation of individual's privacy concerns: Toward an integrative view. In *Proceedings of the Twenty-Ninth International Conference on Information Systems*, Paris. Atlanta, GA: Association for Information Systems, 2008, Article Number 6.

66. Xu, H.; Dinev, T.; Smith, J.; and Hart, P. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*, 12 (December 2011), 798–824.

67. Xu, H.; Luo, X.; Carroll, J.M.; and Rosson, M.B. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*, 1 (April 2011), 42–52.

68. Xu, H.; Teo, H.-H.; Tan, B.C.Y.; and Agarwal, R. The role of push–pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*, 3 (Winter 2009), 135–173.

69. Zhu, K. Information transparency of business-to-business electronic markets: A game-theoretic analysis. *Management Science*, *50*, 5 (May 2004), 670–685.

70. Zimmer, J.C.; Arsal, R.; Al-Marzouq, M.; Moore, D.; and Grover, V. Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems*, *48*, 2 (January 2010), 395–406.

Appendix

Use of customer data at glance

- All data in your customer profile are used to improve the personalization of our online service
- Your data will be stored in our database for 18 months since your last purchase

- You can object to the data processing for legal reasons at any time
- For more information on privacy, please click on our Privacy Policy link

In case you have further questions regarding privacy, please contact our team
info@deineventverzeichnis.de

Your customer profile at glance

The following information about you will be stored in our database:

Personal information	Additional information	Online behavior and transactions
Name, invoicing and shipping address	Event category preferences (theater, trade fair, sport events etc.)	Shopping history, website activities and used features (e.g., viewed events)
Age and gender	Education, current occupation, income level	Location (e.g., country, zip code)
E-mail, phone number	Lifestyle (e.g., free time activities, hobbies, visited countries)	Used devices (desktop, tablet, smartphone, etc.)
Payment information (e.g., credit card number, PayPal e-mail address)	Family details (e.g., marital status, children)	Browser information (Internet Explorer, Google Chrome, etc.) and operating system (e.g., Windows, Mac)
IP-address	Social media profile data (likes, interests and visited events from social media profiles)	

Note: you can keep the information in your customer profile up to date

Figure A1. Screenshot of Transparent Presentation of Data Collection and Use

Table A1. Simple Main Effects Analysis of Personalization Within Each Level of DTVP

Groups DTVP		Sum of squares	Df	Mean square	Mean diff. Low PERS– High PERS	F	Significance
Low DTVP	Contrast	11.29	1	11.29	-0.57	13.06	< 0.001***
	Error	237.59	275	0.86			
High DTVP	Contrast	0.01	1	0.01	0.02	0.02	0.90
	Error	237.59	275	0.86			

Notes: Dependent variable: Intention to disclose information. Each F tests the simple effects of personalization in each level combination of the other effects shown. Significance: *** $p < 0.001$; ** $p < 0.01$; *$p < 0.05$.

Table A2. Simple Main Effects Analysis of DTVP Within Each Level of Personalization

Groups PERS		Sum of squares	Df	Mean square	Mean diff. Low DTVP – High DTVP	F	Significance
Low PERS	Contrast	0.30	1	0.30	0.09	0.35	0.56
	Error	237.59	275	0.86			
High PERS	Contrast	16.44	1	16.44	0.68	19.03	< 0.001***
	Error	237.59	275	0.86			

Notes: Dependent variable: Intention to disclose information. Each F tests the simple effects of DTVP within each level combination of the other effects shown. Significance: ***$p < 0.001$; ** $p < 0.01$; * $p < 0.05$.

Table A3. Simple Main Effects Analysis of Information-Use Transparency Within Each Level of the Combination of DTVP and Personalization

Groups DTVP	Groups personalization		Sum of squares	Df	Mean square	Mean Diff. Low TRANS – High TRANS	F	Significance
Low DTVP	Low PERS	Contrast	1.69	1	1.69	0.31	1.96	0.16
		Error	237.59	275	0.86			
	High PERS	Contrast	0.06	1	0.06	-0.58	0.07	0.79
		Error	237.59	275	0.86			
High DTVP	Low PERS	Contrast	0.05	1	0.05	0.52	0.06	0.81
		Error	237.59	275	0.86			
	High PERS	Contrast	1.20	1	1.20	0.26	1.39	0.24
		Error	237.59	275	0.86			

Notes: Dependent variable: Intention to disclose information. Each F tests the simple effects of DTVP within each level combination of the other effects shown. Significance: $^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$.