Consumer Preferences for Privacy Management Systems

Björn Hanneke
Goethe University Frankfurt, hanneke@wiwi.uni-frankfurt.de

Lorenz Baum
Goethe University Frankfurt, baum@wiwi.uni-frankfurt.de

Christian Schlereth
WHU – Otto Beisheim School of Management, christian.schlereth@whu.edu

Oliver Hinz
Goethe University Frankfurt, ohinz@wiwi.uni-frankfurt.de

Consumer Preferences for Privacy Management Systems

Completed Research Paper

Björn Hanneke
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
60323 Frankfurt am Main, Germany
hanneke@wiwi.uni-frankfurt.de

Lorenz Baum
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
60323 Frankfurt am Main, Germany
baum@wiwi.uni-frankfurt.de

Christian Schlereth
WHU – Otto Beisheim School of Management
Burgplatz 2
56179 Vallendar, Germany
christian.schlereth@whu.edu

Oliver Hinz
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
60323 Frankfurt am Main, Germany
ohinz@wiwi.uni-frankfurt.de

Abstract

This work presents insights into consumer preferences regarding Privacy Management Systems in the context of the General Data Protection Regulation (GDPR). The authors perform a Choice-Based Conjoint experiment with consumers (n = 589) to elicit preferences over four attributes and compute usage likelihoods for all product configurations. Results show that data sharing for marketing purposes and discounts are the most important attributes for consumers. Furthermore, consumers prefer digital access to privacy-related information, detailed rights management for data sharing and no data sharing for marketing purposes. Moreover, a cluster analysis reveals differing importance weights across clusters. The study concludes that incorporating consumer preferences into the design and development process of Privacy Management Systems could increase their use and effectiveness, ultimately strengthening consumers' privacy rights and companies' legal compliance. The authors suggest researching legal, business, and consumer requirements more holistically to converge these perspectives to improve Privacy Management Systems adoptions.

Keywords: Discrete choice experiment, privacy, CBC, data sharing, clustering, conjoint, privacy management systems, privacy dashboards, privacy types

Introduction

The EU General Data Protection Regulation (GDPR) (European Union 2016) outlines data protection principles, such as lawfulness, fairness, transparency, and more[1], which affect all businesses and individuals that collect, process, and store data from EU residents, or provide goods or services within or to the European Union. Since the introduction of the GDPR, many businesses have faced the challenge of implementing GDPR-compliant technical solutions to handle their data (Teixeira et al. 2019). However,

[1] Purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality as well as accountability; for an overview see https://gdpr.eu/what-is-gdpr.

data-driven decision-making is a source of competitive advantage, and many business models rely heavily on data and data analytics (Davenport 2006; Sorescu 2017). In addition, consumer privacy rights could suffer if solutions are difficult to use or fail to fully comply with GDPR requirements.

Privacy Management Systems (PMS) are technical solutions that enable businesses to assess data processing activities and ensure compliance with privacy regulations (Gartner 2023). By our definition, a PMS might include a consumer front-end to manage privacy settings, and in this respect, it is related to privacy dashboards. Overall, PMS enable businesses to comply with the GDPR, thereby strengthening the privacy rights of consumers. However, consumer preferences regarding GDPR requirements are opaque, e.g., research on privacy requirements and preferences is typically disjunct from a legal perspective and therefore does not consider the requirements of the relatively new GDPR. GDPR-specific research typically considers the law but does not consider consumer preferences, e.g., investigating GDPR requirements (Janßen and Kathmann 2020), proposing GDPR-compliant implementation frameworks (Tapsell et al. 2018), or proposing solutions to specific GDPR requirements, such as privacy dashboards (Angulo et al. 2015) and consent management tools (Kirrane et al. 2018). However, understanding and considering consumers' privacy preferences is critical to the development and adoption of such tools (Hevner et al. 2004).

Given the current lack of consumer preference research on PMS, we elicit consumer preferences through a choice-based conjoint experiment (CBC) (e.g., Natter and Feurstein 2002; Raghavarao et al. 2010) on specific design choices of a fictive PMS in context of online shopping and the GDPR. Consequently, we seek to narrow the gap between general privacy research, GDPR compliance, and consumer privacy preferences. Our results allow the consideration of consumer preferences into the design and development process of a PMS, which could help to increase its use and effectiveness, ultimately strengthening consumers' privacy rights and better addressing business needs.

The paper is organized as follows: The first part provides an overview of the related work. Afterward, we introduce our methodology and present our study design. Thereafter, we present empirical results on the elicited consumer preferences and derive key design decisions for a PMS. Finally, we discuss the implications and summarize our findings. We conclude with limitations and provide an outlook for future research.

Related Work

In this section, we provide an overview of privacy research, including privacy economics and privacy disclosure behavior. We then present work on privacy engineering goals and GDPR-specific requirements, including existing technical solutions, such as privacy dashboards. Overall, related work will inform the design and setup of our choice experiment in the later sections.

Defining privacy is an ongoing endeavor. Some authors argue against a general definition of privacy because it is always context-specific (Smith et al. 2011; among others). However, with the introduction of the GDPR, lawmakers in Europe have taken the position that privacy means being in control over the collection, storage, and use of personal information, as suggested by several scholars (Altman 1975; Petronio 1991; Westin 1968, 2003; among others). Because we focus on information privacy in the context of the GDPR, we refer to privacy as information privacy from here on.

A broad stream of research investigates the economic value of privacy to consumers. Experimental results suggest that most consumers prefer lower prices at the expense of privacy (Hann et al. 2002; Preibusch et al. 2013), but some participants are willing to pay a "privacy premium" either by not disclosing private data or by the service provider promising not to use the data for marketing purposes (Jentzsch et al. 2012). Furthermore, financial incentives and convenience positively influence participants' willingness to create an account with a website (Hann et al. 2007), but salient and accessible privacy information induces some consumers to pay a premium for purchases from privacy-protective websites (Tsai et al. 2011). Thus, businesses may leverage privacy as a competitive advantage in certain settings, as privacy valuations appear to be highly context-specific, exhibit order effects, and depend on non-normative factors (Acquisti et al. 2013). Nevertheless, financial incentives might be relevant in the context of a PMS, as they may motivate usage and allow the valuation of certain design choices.

Another research stream investigates privacy disclosure behavior, with early works showing that stated and revealed preferences of consumer disclosure behavior do not match (Ackerman et al. 1999), and relating this dissonance to behavioral literature (Acquisti 2004). Later works refer to this observation as the "privacy paradox" (Berendt et al. 2005), and suggest that permission-based data collection, as now introduced by the GDPR, may address this paradox (Norberg et al. 2007). The privacy paradox has been a reference point for further studies, e.g., suggesting that an increase in perceived control may increase the willingness to disclose private information (Brandimarte et al. 2013). Furthermore, the extended privacy calculus theory (Dinev and Hart 2006) suggests that trust and personal interest may outweigh the perceived privacy risk of disclosing information. Moreover, privacy disclosure behavior itself may not be stable over time, e.g., especially older people appear to be more likely to provide less information over time (Goldfarb and Tucker 2012). In addition, consumers constantly adapt their behaviors to the privacy practices of firms and vice versa, e.g., Facebook users engage in privacy-seeking behavior, and Facebook implements features to counteract this trend (Stutzman et al. 2013). To address the privacy paradox, we conduct a CBC experiment, to uncover consumer preferences and mitigate potential adverse effects due to the privacy paradox.

Furthermore, to operationalize privacy, researchers have already formulated privacy-engineering goals before the GDPR introduction, e.g., arguing that data collection, control, and awareness are relevant in the context of online privacy (Malhotra et al. 2004), or proposing six dimensions of privacy in IT systems, namely confidentiality, transparency, intervenability, availability, unlinkability, and integrity. However, given the conflicting nature of these dimensions, it is not possible to achieve all goals simultaneously (Hansen et al. 2015). The GDPR introduction allowed the detailing of privacy goals into requirements. While several works suggest frameworks to assess GDPR compliance (Agarwal et al. 2018; Antignac et al. 2016), other works focus on privacy modeling and potential technical implementations (Maguire et al. 2015; Pandit et al. 2018; Tapsell et al. 2018). Some works focus on specific GDPR aspects, such as consent management (Kirrane et al. 2018) or transparency systems (Janßen 2019; Janßen and Kathmann 2020). Regarding the effects of the GDPR introduction, studies from Norway show that most participants trust companies with their personal data (Presthus and Sørum 2019) and that the GDPR introduction did not alter the level of consumer awareness or level of control over personal data (Sørum and Presthus 2021). Even though, these studies provide valuable insights; they do not derive consumer preferences regarding GDPR requirements. More closely related to PMS are privacy dashboards, typically focusing on the consumer frontend of PMS. Several studies investigate privacy dashboards before (Buchmann et al. 2013; Kolter et al. 2010; Zimmermann et al. 2014) and after the GDPR introduction (Bier et al. 2016; Popescu et al. 2016; Raschke et al. 2017). More recently, a case study on the GDPR compliance of privacy dashboards reports incomplete GDPR compliance in most dashboards (Tolsdorf et al. 2021). However, experimental evidence suggests that access to privacy dashboards increases trust and lowers perceived risk compared to sole access to privacy policies (Herder and van Maaren 2020). These findings provide evidence for the benefits of privacy dashboards for consumers and businesses alike. Even though, the aforementioned works design prototypes and in some cases conduct user acceptance tests compared to other privacy dashboards, they do not consider consumer preferences from a general privacy and design perspective.

To summarize this section, we recognize the importance of studies related to privacy disclosure behavior given influencing factors and financial incentives; however, these studies do not consider the recent legal requirements of the GDPR. GDPR-related works incorporate legal requirements and offer potential technical implementations, but do not consider consumer privacy preferences. Therefore, in the following sections, we aim to address this open question by exploring consumer preferences with respect to a fictive PMS and its potential design choices.

Research Methodology

The GDPR sets the regulatory frame and hence defines the overarching design space for potentially compliant PMS. Nevertheless, the success of a PMS depends on specific design choices based on consumer preferences regarding their privacy management needs and preferences. To examine consumer preferences regarding specific design choices of a PMS, we conduct a CBC experiment. The results of this experiment, i.e., the partworths utilities for different design choices, then serve further analyses: We simulated different configurations for PMS to determine the preferred configuration and apply a clustering method to identify consumer groups with similar preferences.

Study Design

We conducted a survey including a CBC experiment (Raghavarao et al. 2010) with consumers, i.e., prospective users of a PMS, potential business requirements are explicitly not the focus of this experiment. The choice experiment consisted of 14 independent choice tasks, each consisting of a set of three configuration alternatives of PMS. For each task, participants had to decide which PMS configuration they prefer, given the alternatives, or not to use any of them. Additionally, we queried further information regarding demographics and latent constructs with a detailed questionnaire. We developed the survey including the CBC in several interdisciplinary workshops with n = 5 researchers from different disciplines, such as information systems (IS), software engineering, and privacy law, to include diverse perspectives into the survey design. Finally, we implemented the CBC and questionnaire in the Dynamic Intelligent Survey Engine (DISE) (Schlereth and Skiera 2012) and hired a leading market research agency to acquire a representative sample for the German internet population. Through this, participants received monetary compensation for successfully participating in the study. The sample selection also explains the use of German throughout the study.

Choice-Based Conjoint Design

We operationalized the preference elicitation using a specific usage scenario of a PMS, to provide a clear and illustrative setting for the participants and their decision process within the CBC. The scenario depicts the potential use of a PMS in the course of an online purchase of shoes with a digital marketplace that the participants regularly use. Furthermore, prior to the experiment, PMS attributes and attribute levels were presented to participants, and displayed during the experiment, to ensure participants could look up any relevant information. An initial quality test, i.e., a comprehension check (Oppenheimer et al. 2009) ensured that respondents understood the scenario and the design of the CBC. If respondents failed the comprehension check, the survey was terminated and their participation in the survey ended without compensation. Within each choice task, we presented a set of three distinct configurations, i.e., stimuli, of the PMS, based on attribute levels and a no-use option. Given our scenario, the no-use option is defined as not using the PMS and not realizing a potential discount; hence, buying the shoes for the full price. We asked participants specifically to choose the PMS configurations that they would use themselves with respect to the given alternatives.

Attributes and attribute levels define a CBC and are therefore critical success factors in conjoint analyses (Auty 1995). Also, the number of attributes and levels per attribute needs to be carefully chosen (Lenk et al. 1996). In the GDPR context, GDPR compliance is an overarching goal, therefore, we rely on predefined non-functional requirements as the basis for the definition of attributes and attribute levels (e.g., Janßen and Kathmann 2020). Furthermore, to investigate consumer preferences, especially two intentions of the GDPR are to be included in the attributes: strengthening the rights of data subjects in transparency (Art. 12 GDPR) and self-control and intervenability (Art. 15–22 GDPR) (Hansen et al. 2015; Janßen and Kathmann 2020). This leads to the first two attributes "*transparency*" and "*data sharing management*". For our scenario, with *transparency,* we refer to the means through which the PMS provides transparency regarding the personal data held by the online marketplace. *Data sharing management* refers to the way users can manage consents or disclosures for data sharing to third parties on the marketplace for a better-tailored shopping experience. Our third attribute "*data sharing for marketing purposes*" is based on the assumption that participants are sensitive to data sharing with third parties, especially for the purpose of marketing (Milne et al. 2017). Hence, this attribute refers to different levels of data sharing with third parties the online marketplace pursues regarding anonymity. Participants were told that a high degree of anonymity might negatively affect recommendation quality and relevance for further purchases on the platform. Finally, in hand with the fictive purchase of the pair of shoes, the online marketplace offers different *discount* levels to the users of the PMS. This allows for a comparison of attribute utilities with this monetary attribute.

After defining the initial set of attributes, we conducted a second round of interdisciplinary interviews on user interface design, user experience design, and privacy law, to validate and refine final attributes and attribute levels, including adjustments to certain expressions or terms. This resulted in the CBC design consisting of four attributes with three to four attribute levels each representing different design choices for the development of a PMS. Table 1 presents all attributes and attribute levels of our CBC (original attributes and levels in German can be found in Table 6 in the Appendix).

Attributes *(range)*	**Attribute levels** *(keyword)*
Transparency *(3)*	• you receive the information by mail via *post*. • you are granted one-time *digital access* to the information upon request (e.g., e-mail or download link). • you can access this data online at any time via a *dashboard*.
Data sharing management *(3)*	• *individually*, i.e., each consent for data sharing must be selected individually and manually. • *consent profiles*, i.e., granting of pre-set consents with one click, e.g., based on a selection recommendation from data or consumer protection organizations. • *maximum consent*, i.e., one-click consent to full and comprehensive data sharing.
Data sharing for marketing purposes *(4)*	• *no sharing*, recommendation quality, and relevance for further purchases are very low. • *anonymized*, but recommendation quality and relevance for further purchases are low. • *person-related*, but the quality and relevance of recommendations for further purchases are good. • *comprehensive*, but recommendation quality and relevance for further purchases are very good.
Discount *(4)*	• *0%* • *4%* • *8%* • *12%*

Table 1. Attributes and attribute levels – translated from German

The attribute levels for each attribute are separable but also useful and relevant for the development of a PMS. Hence, attribute levels describe potential configurations or features of the PMS. Some of the attributes might not correspond to non-functional requirements from the GDPR or national laws, such as a maximum one-click consent for comprehensive data sharing or a general user consent to comprehensive data sharing for marketing purposes. Nevertheless, these attribute levels are included to offer clearly separable attribute levels that participants can easily understand. Moreover, many participants are not aware that these attribute levels are not GDPR-compliant and therefore do not bias their answer behavior. Also, these attribute levels allow us to investigate if convenience or usability might outweigh GDPR compliance from a consumer perspective.

Figure 1 shows an exemplary choice set (I_a) presented to the participants ($h \in H$) with already one configuration, i.e., stimuli (i), selected. For each participant, we randomized the order of the choice tasks (I), the positioning of the individual stimulus in the choice tasks, and the presentation order of the attributes within the stimuli (once done for each respondent). This further contributes to the validity of the results, as order effects can thus be avoided, e.g., change in attention over the time of the experiment or learning effects and transfer effects.

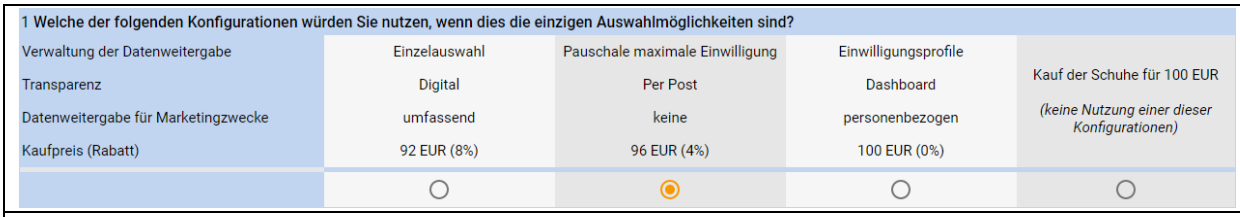

Figure 1. Example of a choice set in German language

Latent Constructs

We measure established scales from marketing, psychology, and IS research as latent constructs (Bruner 2019). For our cluster analysis (see respective section) we use two scales following the literature we base our clustering approach on (Hanneke et al. 2023). First, we derive estimates for privacy importance, to measure participants' sensitivity regarding how companies handle personal information, given privacy is important to them (Martin et al. 2017). Second, we measure GDPR knowledge by adapting the knowledge

of the product class scale (Kelting et al. 2017), which subjectively measures consumers' relative level of familiarity with a product category, to the topic of GDPR.

Finally, we include the choice difficulty scale according to Kelting et al. 2017 to measure participants' difficulty in choosing among the PMS configurations within the CBC experiment. With this, we aimed to increase the comparability of CBC experiments and validate our CBC design. We recognize the importance of maintaining a balance in choice difficulty, neither making choices too challenging nor overly simplistic (e.g., Baier and Brusch 2021). For further clarity, we have summarized the items for our latent constructs in Table 7 in the Appendix, which provides a comprehensive overview of our measurement approach.

Model Estimation

Conjoint analysis has proven to be a valid tool to derive consumer and user preferences. Thereby, CBC is currently the most widely used variant of conjoint analysis (Raghavarao et al. 2010). We apply a CBC with no-choice, i.e., no-use option, to gain insights into participants' preferences regarding different potential configurations, i.e., stimuli, of a PMS.

We define the probability that consumer h chooses stimulus i from a choice set $a \in A$ as

$$P_{h,i,a} = \frac{\exp(u_{h,i} + \varepsilon_{h,i})}{\exp(u_{h,NU} + \varepsilon_{h,NU}) + \sum_{i \in I_a} \exp(u_{h,i} + \varepsilon_{h,i})} \quad (1)$$

to determine the utility u_h for all stimuli and the no-use option (NU) (Natter and Feurstein 2002). $\varepsilon_{h,i\ or\ NU}$ represents the stochastic part of the utility for each stimuli and consumer. The consumer's utility $u_{h,i}$ for a stimulus is the sum of the partworths utilities $\beta_{h,j,m}$ for all attributes $j \in J$ excluding the *discount* and attribute levels $m \in M_j$ and the utility $\beta_{h,discount}$ for the *discount* attribute. Hence, we define

$$u_{h,i} = \sum_{j \in J} \sum_{m \in M_j} (\beta_{h,j,m} \cdot x_{i,j,m}) + \beta_{h,discount} \cdot d_i \quad (2)$$

with $x_{i,j,m}$ as a binary variable indicating whether an attribute level m is part of a stimulus i and d_i as the level of discount granted. Systematically, $u_{h,NU}$ equals $\beta_{h,NU}$.

To enable an efficient estimation of the model parameters, we first optimized the CBC design (see Table 1) with respect to its D-efficiency using open-source software, applying the Federov algorithm, and then second optimized the design regarding the balance within the individual choice sets. This two-step procedure resulted in an experimental design with 12 choice sets with three stimuli each plus a no-use option. Overall, this design results in an excellent D-efficiency of 98.81% compared to the full factorial design, despite the relatively few choice sets. Following the aforementioned procedure, we added two choice sets as holdouts, to evaluate the model's goodness of fit (hit rate, i.e., we calculated the proportion in which the observed decision was the one with the highest probability according to the estimated parameters). This led to a total of 14 choice tasks the participants had to undertake. A typical critique of CBC experiments, the long and monotonic survey participation (Baier and Brusch 2021) is addressed by decreasing the number of choice sets for each survey participant without compromising on an efficient model estimation. The model estimation and preference calculations were performed in aggregate using a hierarchical Bayesian (HB) estimation (Gelman et al. 2014) procedure implemented in MATLAB (Schlereth et al. 2018), as this procedure has proven to be superior to the latent class model estimation (Baier and Brusch 2021).

Simulating Preferred Configurations for Privacy Management Systems

Following the economic theory, consumers maximize their individual surplus; therefore, they select the PMS stimulus, i.e., configuration, that yields the highest surplus, i.e., utility. In our scenario, consumers do not pay but receive *discounts* if they use certain configurations. Assuming our utility function (see Formula 2 above), consumers prefer the configuration with the highest utility with the utility of the no-use option being the baseline, i.e., the intercept of the linear relation of the attributes' utilities. Based on the CBC experiment and HB estimation, utilities for different hypothetical configurations of the PMS can be computed (e.g., Roßnagel et al. 2014). From this, we can calculate the expected usage likelihood for a configuration i with

$$\widehat{UL}_{h,i} = \frac{\exp\left(\beta_{h,NU} + \sum_{j\in J}\sum_{m\in M_j}(\beta_{h,j,m}\cdot x_{i,j,m}) + \beta_{h,discount}\cdot d_i\right)}{\exp\left(\beta_{h,NU} + \sum_{j\in J}\sum_{m\in M_j}(\beta_{h,j,m}\cdot x_{i,j,m}) + \beta_{h,discount}\cdot d_i\right) + 1} \tag{3}$$

for each consumer h. By applying this concept, we can calculate an optimal PMS configuration given all *discount* levels, for every consumer with $i_{max,h} = \max_i \widehat{UL}_{h,i}$. Similarly, the overall optimal PMS configuration i by design choices can be determined by maximizing the mean expected usage likelihood for all $n = |H|$ consumers $h \in H$:

$$i_{max} = \frac{1}{|H|}\max_i \sum_{h\in H} \widehat{UL}_{h,i} \tag{4}$$

Clustering

Lastly, we perform a cluster analysis to determine differences regarding importance weights, demographics, and latent constructs for privacy types. Hanneke et al. (2023) used the latent constructs privacy importance (Martin et al. 2017) and knowledge of the GDPR (adapted from Kelting et al. 2017) to group consumers into four distinct privacy types using a k-means clustering, which included robustness checks regarding the cluster centers and the number of clusters. Hence, consumers within the same privacy type show similar stated characteristics regarding the two scales. In their study, they identify a cluster 1 called "unconcerned" with low privacy importance and low knowledge, a cluster 2 named "pragmatists" with low importance and high knowledge, a cluster 3 ("amateurs") showing high importance and low knowledge, and a 4. cluster with high values for both constructs which they call "fundamentalists" (Hanneke et al. 2023). For our analysis, we use the provided cluster centers to group our participants into the privacy types based on the Euclidian distance between the vector of privacy importance and knowledge of the GDPR of each participant to the centers.

Empirical Results

The market research company recruited our participants between March 3rd and 21st 2022. In total 988 participants started the survey, of which we include 589 in the evaluation. The high rejection rate is due to two employed quality tests, i.e., comprehension and manipulation checks. These quality tests were highly successful in capturing low-quality response behavior with our survey participants, as further quality validations, such as filtering based on duration and positional choices in the CBC experiment, did not improve quality further. Hence, we are confident with the overall quality of the sample.

Demographics

Our sample is representative of the German internet population regarding age and gender distributions, the prospective main user group of a PMS from our scenario (see Table 9 in the Appendix). The sample includes 49.1% women and 50.5% men (n = 3 selected "diverse"). 31.3% of participants had a university degree, whereas 68.7 % completed professional training or still attended school. The median household income range in our sample is 20,000 to 40,000 EUR. Participants indicated an average private online time of 3.8 hours per day. Table 8 in the Appendix outlines more details on demographics.

Latent Constructs

We compute and report Cronbach's α for the relevant latent constructs and compare them to the values of the original studies. As we report similar values for Cronbach's alpha, see Table 2, we use the constructs in further analyses of our study.

Results of CBC Experiment

We evaluate the validity of our CBC experiment by computing the (internal) hit rate (HR) for the 12 choice sets and by calculating the (predictive) HR for the two holdout sets. Thereby, we use the two holdouts as a measure for the predictive validity. Our model achieves an overall prediction HR of 70.97%, i.e., 88.07%

goodness of fit with respect to the remaining choice sets included in the HB estimation (e.g., Roßnagel et al. 2014).

Latent construct	Cronbach's alpha in this study	Cronbach's alpha in original study	Original study introducing the latent construct
Privacy importance	.91	.94	Martin et al. 2017
Knowledge of the GDPR (adapted from product class knowledge)	.92	.89	Kelting et al. 2017
Choice difficulty	.87	.81 / .85	Kelting et al. 2017

Table 2. Cronbach's alpha of latent constructs

Overall importance weights reveal that the attributes *data sharing for marketing purposes* with an importance weight of 36% and the offered *discount* with an importance weight of 33% are the most important factors to our participants. *Data sharing management* with 18% and *transparency* with 12% importance weight are less important. We investigate estimated importance weights relative to gender and age and find them to be relatively stable. Only the *discount* attribute seems to be more important to men than to women (importance weight 35.5% vs. 30.4%). Table 3 summarizes those results.

With respect to potential good PMS configurations, the CBC experiment delivers clear tendencies within the attributes. Regarding *transparency*, participants exhibit a strong preference for digital access (+0.39) to information. The *data sharing management* attribute reveals a preference for individual (and manual) consent management (+0.64). Participants also value consent profiles positively (+.50), which were described to be more convenient but less detailed than manual consent. Maximum full consent is associated with the lowest utility contribution (-1.14). The attribute *data sharing for marketing purposes* offers a similar divided result. On the one hand, the preferred options "no data sharing" (+1.67) and "anonymized sharing" (+1.55) are positively associated. Even though, participants accept low recommendation quality and relevance at the same time. Thereby, the difference between no sharing and anonymized sharing is marginal, demonstrating that participants are willing to share their data anonymously. On the other hand, participants are not willing to share their person-related (-1.20) or comprehensive data (-2.02). Finally, the *discount* factor exhibits a positive utility contribution (+.47) per change in the percentage of the *discount*.

Altogether, participants value privacy-preserving attributes higher, as postulated by the GDPR. Additionally, convenience and financial incentives are prevalent over the average utilities of all attributes.

Attributes	**Attribute levels**	Mean utilities $\bar{\beta}$	Std.	Mean Importance weights	Std. Importance weights
Transparency	Post	-.41	.56	12.19%	10.47%
	digital access	.39	.43		
	dashboard	.02	.49		
Data sharing management	Individually	.64	.61	18.80%	12.60%
	consent profiles	.50	.46		
	maximum consent	-1.14	.98		
Data sharing for marketing purposes	no sharing	1.67	1.21	36.03%	16.68%
	anonymized	1.55	.97		
	person-related	-1.20	1.01		
	comprehensive	-2.02	1.21		
Discount	% discount	.47	.70	32.99%	21.91%

Table 3. Results of HB estimation of CBC experiment

Preferred Configurations of Privacy Management Systems

Based on estimated utility levels and all possible combinations of attribute levels, we derive usage likelihoods for each participant. Table 4 presents the top three configurations regarding the average usage likelihoods. For all configurations, usage likelihoods increase with the *discount* rate and range between 57.93% at 0% *discount* to 78.07% at 12% *discount* for the Top 1 configuration. The Top 1 configuration with the highest average usage likelihood of 74.95% at 9% *discount* rate offers digital access to information,

individual selection within the *data sharing management,* and no *data sharing for marketing purposes*. Other configurations are slightly less but similarly attractive, e.g., at a 9% *discount*, the Top 2 configuration achieves 74.89% average usage likelihood, and the Top 3 configuration 73.76%. For comparison, we also include the PMS configuration with the lowest usage likelihood in Table 4. The difference in usage likelihood is striking, especially at the 0% *discount* level. The Top 1 configuration has a 3.44 times higher likelihood than the worst configuration. However, the offered *discount* has a larger effect on this configuration than on the top configurations, increasing its likelihood by a factor of 2.56 up to 43.29%.

The preferred configuration remains stable for discount levels 0%, 4%, and 8%. At 12% *discount* level, the *data sharing* attribute level switches from "no sharing" to "anonymized", which might indicate participants' higher willingness to share their data in return for a higher *discount*. However, from an economic perspective, this result is counterintuitive, because an individual's preference should still be to share less data even if a higher discount is granted. It is possible that participants assumed that they must share more data to receive a higher discount, e.g., based on a feeling of fairness or business sense. However, we explicitly did not suggest this in the CBC scenario description.

Attributes	**Top 1 configuration**	**Top 2 configuration**	**Top 3 configuration**	**Worst configuration**
Transparency	digital access	digital access	dashboard	post
Data sharing management	individually	individually	individually	maximum consent
Data sharing for marketing purposes	no data sharing	anonymized	anonymized	comprehensive
Average usage likelihoods for given discounts				
0% discount	57.93%	56.81%	52.67%	16.84%
4% discount	67.07%	66.75%	64.70%	29.94%
8% discount	73.70%	73.54%	72.28%	37.21%
12% discount	77.82%	78.07%	77.17%	43.29%

Table 4. Preferred PMS configurations

Clustering

We derive four clusters based on the privacy importance scale, as the intention to act, and the knowledge of GDPR scale as the ability to act. We follow Hanneke et al. (2023) regarding the cluster labels for "unconcerned" with low privacy importance and low knowledge (cluster 1), "pragmatists" with high knowledge and relatively low privacy importance (cluster 2), "amateurs" with relatively low knowledge but high privacy importance (cluster 3), and "fundamentalists" with high knowledge and high privacy importance (cluster 4). Table 8 in the Appendix holds demographics for each cluster and indicates where significant differences between the clusters exist.

The results for the importance weights presented in Table 5 indicate notable differences between clusters. For comparison, importance weights for the entire sample are shown in the total sample column. *Transparency* reflects overall little importance across all clusters. Interestingly, the unconcerned have the highest *transparency* importance weight, however, still on a low level of 13.04%. The *data sharing management* exhibits more variance across clusters (significant differences between at least two clusters with $p < .001$). Its importance weights increase steadily from cluster 1 (15.37%) to 4 (20.91%), with the largest absolute difference between cluster 2 (16.61%) and 3 (20.01%). Next, *data sharing for marketing purposes* exhibits even more variance across clusters (significant differences between at least two clusters with $p < .001$), again with increasing importance weights from cluster 1 (26.82%) to 4 (41.07%). The largest absolute difference was between cluster 1 and cluster 2 (33.08%). Lastly, *discount* shows significant differences ($p < .001$) between at least two of the clusters with highest importance weights for cluster 1 (44.76%) and lowest for cluster 4 (26.28%). *Discount* shows the largest between-cluster differences and the highest overall importance weight for cluster 1. The results confirm the intuition that high privacy importance (clusters 3 and 4) relates to higher importance weights for the attributes *data sharing management* and *data sharing for marketing purposes*. Furthermore, these results indicate that the importance weights derived by the CBC experiment reflect the clustering dimensions of intention to act

(privacy importance scale) and ability to act (knowledge of GDPR scale) or vice versa, providing further evidence for their validity (Hanneke et al. 2023).

Cluster results		**Cluster**				**Total sample**
		1 uncon-cerned	2 pragma-tists	3 amateurs	4 funda-mentalists	
Observations n (in %)		90 (15.3)	141 (23.9)	157 (26.7)	201 (34.1)	589 (100.0)
Knowledge of GDPR (cluster center)	Mean**	2.06	4.49	2.33	4.91	3.69
	Std.	.80	.84	.79	.87	1.50
Privacy importance (cluster center)	Mean**	2.97	4.00	5.69	6.11	5.01
	Std.	1.01	.75	.75	.68	1.42
Transparency	Mean	13.04%	12.28%	12.19%	11.73%	12.19%
	Std.	11.30%	10.83%	9.08%	10.88%	10.47%
Data sharing management	Mean**	15.37%	16.61%	20.01%	20.91%	18.80%
	Std.	12.05%	12.49%	12.67%	12.39%	12.60%
Data sharing for marketing purposes	Mean**	26.82%	33.08%	37.50%	41.07%	36.03%
	Std.	17.01%	17.28%	15.88%	14.55%	16.68%
Discount	Mean**	44.76%	38.02%	30.30%	26.28%	32.99%
	Std.	27.15%	23.49%	19.83%	16.09%	21.91%
Choice Difficulty	Mean**	3.24	2.99	3.35	2.73	3.04
	Std.	1.48	1.27	1.55	1.44	1.46
Note: Between-group difference significance ** at $p < 0.01$ using Kruskal-Wallis tests.						

Table 5. Importance weights and latent constructs for clusters

Over the total sample, a choice difficulty of 3.04 on a seven-point Likert-scale, indicates that participants neither perceived the CBC tasks as too difficult nor too easy. However, there are significant differences between clusters, i.e., unconcerned and amateurs perceived choice difficulty higher as pragmatists and fundamentalists. As mean values range between 2.73 (fundamentalists) and 3.35 (amateurs), we infer the validity of the CBC experiment regarding choice difficulty.

Discussion, Implications, and Limitations

This work investigates consumer preferences regarding PMS design choices and privacy considerations in the context of the GDPR. Our consumer preference elicitation confirms several findings of previous general privacy research and contributes new insights.

First, the participants' preference for the attribute levels "anonymized" or "no data sharing" in the *data sharing for marketing purposes* attribute provides evidence for the suggestion that consumers are less concerned with data collection, storage, and usage if data is processed on an aggregate, e.g., anonymized level, compared to person-related or comprehensive data sharing (Xie et al. 2006). This intuitive result highlights the importance of privacy for most participants; i.e., even clusters with lower privacy importance, such as the unconcerned or pragmatists, exhibit a higher importance level for this attribute. Second, these preferences also suggest that customers tend to dispense convenience and service quality, e.g., worse or less personalized recommendations, if they have to share more data, i.e., personalized data as opposed to anonymized data or no data at all (Xu et al. 2011). Again, this finding highlights the importance of privacy to the participants. Third, our participants show an inclination for heuristics when taking privacy decisions, visible with the high utility contribution consent profiles from known and trusted privacy security and consumer protection agencies. This relates to previous findings regarding the use of heuristics in privacy decisions (Acquisti and Grossklags 2005). Moreover, this finding shows the potential of predefined consent profiles for platforms or PMS operators aiming to build trust with consumers regarding privacy in an online environment. Future research could investigate how independent experts could be included in privacy systems, offering an added value to consumers that goes beyond current practices, such as privacy or trust labels (Bargh et al. 2022). Fourth, we find evidence that privacy-concerned consumers tend to value features for privacy protection, as demonstrated by the cluster analysis; this is in line with previous research (Lee et al. 2011). Furthermore, future research could investigate whether consumers accept more data

collection if they understand the benefits of this action (Malhotra et al. 2004). In our experiment, the potential benefit of sharing data was only descriptive but not included as a separate attribute, i.e., sharing less data diminishes shopping recommendations quality. Therefore, our experiments and results do not allow an evaluation of the suggestion of clearly communicating data-sharing benefits. The same holds for the suggestion that consumers are less concerned if data requests match the provided service (Beke et al. 2018). Both questions are highly relevant and should be addressed in future related works.

Prior research suggests that consumers tend to be comfortable if they have the feeling to be in control of their data, which might even increase their willingness to disclose more information (Brandimarte et al. 2013). This is in line with our findings regarding the data sharing attribute, as anonymized data sharing and no data sharing have similar utility contributions, suggesting that the fact to be in control to decide how to share the data has a similar influence as not sharing the data. Regarding the PMS configurations with the highest usage likelihoods, it is notable that the top three configurations are rather similar, the main differentiators being digital access versus privacy dashboard for *transparency*, and anonymized data sharing versus no *data sharing for marketing purposes*. From the perspective of potential companies developing or implementing PMS, it is interesting that anonymized data sharing compared to no data sharing does not decrease usage likelihood as much as one might expect, given the high importance weight of *data sharing for marketing purposes*. To optimize overall welfare, it might be better to deviate from overall usage likelihood considerations but consider preferences for different privacy types or on an individual level. Also, to increase welfare when implementing a PMS, developers should consider the preferences of both, consumers, and companies. In this regard, future work could investigate the preferences of businesses with respect to the described attributes and attribute levels, including potentially varying development and implementation costs and economic benefits of certain design choices. This might lead to PMS that support both consumers and businesses alike and hence, increase overall adoption.

Furthermore, Tolsdorf et al. (2021) show that in a sample of privacy dashboards, most are not fully GDPR-compliant, especially regarding the completeness of privacy-related information, data sources, and technical data provided. They argue that online services should provide this information to not lose consumers' trust. However, data providers might provide just the right amount of information to induce trust, as their dashboards gauge the feeling of being in control (Beke et al. 2018). From our findings, the low importance weight of the *transparency* attribute indicates that access to the privacy information (*transparency*) is less important than control over the information flow and the data sharing itself. This might provide evidence for the privacy paradox, as participants want to be in control, even to a detailed level (e.g., individual consents), but do not thoroughly care much about the presentation of the information or the access to it. In this sense, our participants seem to trust companies providing the information and holding the data (Presthus and Sørum 2019).

Moreover, this observation opens the discussion regarding GDPR requirements, supposably large implementation efforts including technical difficulties to adhere to legal requirements but potentially little consumer preferences regarding these requirements. Maybe this divergence is a cause for the frustration of many companies regarding the GDPR (Härting et al. 2020). In this respect, introducing standard processes and privacy services for consumers is economically rational if consumers demand these services. However, if demand is too low, most companies will default to manual processes and will not provide comprehensive PMS, despite potential long-term savings, legal security, and better serving of consumer privacy rights.

In summary, our study shows that consumers have an understanding of what privacy means to them and which preferences they have for a PMS. On the investigated points, participants' stated preferences are not conflicting with the privacy protection goals of the GDPR. However, convenience is a secondary requirement, as users do not want to invest too much time and effort into dealing with this subject (Hanneke et al. 2023). Also, we confirm that being in control is more important than having access to privacy-related information itself, which might provide evidence for the privacy paradox. Looking forward, the question remains how stable consumer preferences regarding PMS attributes are over time. Larger privacy awareness and broader adoption and usage of privacy tools, e.g., PMS and privacy dashboards, might ultimately influence the preferences of consumers. Future works may also contribute to a better understanding of what matching expectations between data requirements and data usage are from

consumer and business perspectives. Exploring consumers' privacy and business' data requirements more holistically might help to converge legal requirements, business implementation efforts, and consumer preferences.

Finally, our research faces similar limitations as other CBC experiments. First, our results are not inherently generalizable, as the findings apply to the current state of the German internet population. However, the use of standard scales and a transparent CBC design allows the reproduction of results for potentially different regions or populations. With this, future research could investigate how privacy preferences differ between populations or for other contexts. Additionally, scholars could also focus more on the underlying theories involved in humans' privacy preferences and data sharing. Second, although our sample is representative regarding age and gender, we cannot rule out sample (self-)selection biases, for example, privacy-concerned people might not participate in anonymous online studies or privacy-unconcerned people might not choose to take part in privacy-related studies. Third, even though our attributes root in prior literature, our scenario and the selected attributes (i.e., the non-GDPR-compliance of maximum consent) for the fictive PMS are a simplification of real-world PMS and use cases. Thus, experiments with real-world PMS are necessary to fully understand human behavior. Finally, limitations from our clustering approach apply here as well, e.g., regarding the number of clusters (see Hanneke et al. 2023).

Conclusion

This work offers privacy research insights into consumer preferences regarding a PMS in the context of the GDPR. Incorporating consumer preferences into the design and development process of PMS could help to increase their use and effectiveness, ultimately strengthening consumers' privacy rights.

In our CBC experiment, we elicit consumer preferences over four attributes and derive the following importance weights in descending order: *data sharing for marketing purposes* (36.03%), *discount* (32.99%), *data sharing management* (18.80%), *transparency* (12.19%). Furthermore, we compute usage likelihood for all product configurations. We find that the top 3 configurations with the highest usage likelihoods share similar attribute levels, namely digital access or a dashboard for privacy information in the *transparency* attribute, individual consent management for *data sharing management,* and no or anonymized data sharing in the attribute *data sharing for marketing purposes*. Additionally, we perform a cluster analysis by applying two standard scales, privacy importance and knowledge of the GDPR. Clustering results indicate differing importance weights across four resulting clusters. The importance weights per cluster adhere to intentions regarding the underlying scales to perform the clustering, e.g., clusters with high privacy importance exhibit higher importance weights for privacy-preserving PMS attributes, whereas low privacy importance clusters value monetary incentives (*discount*) higher. This coherence provides validation for our CBC results and applied scales. We discuss that our CBC results reflect findings of prior privacy research. Furthermore, we suggest researching legal, business, and consumer requirements more holistically to converge these perspectives.

Current diverging legal requirements, business data needs, and consumer preferences might result in lower PMS adoption and therefore impair consumer privacy rights execution and companies' legal compliance.

Acknowledgements

We thank the German Federal Ministry of Education and Research for the generous funding of the PERISCOPE project (funding number: 16KIS1480), which enabled us to conduct our research. We also acknowledge and thank our colleagues in the PERISCOPE project, who provided us with invaluable feedback throughout the research process. Their contributions significantly contributed to the success of this study.

References

Ackerman, M. S., Cranor, L. F., and Reagle, J. 1999. "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," in *Proceedings of the ACM Conference on Electronic Commerce*: *Denver, Colorado, November 3 - 5, 1999*, Default (ed.), New York: ACM Press, pp. 1-8.

Acquisti, A. 2004. "Privacy in electronic commerce and the economics of immediate gratification," in *EC'04*: *Proceedings of the 5th ACM conference on electronic commerce*, J. Breese, J. Feigenbaum and M.

Seltzer (eds.), New York, NY, USA. 17.05.2004 - 20.05.2004, New York, New York, USA: ACM Press, p. 21 (doi: 10.1145/988772.988777).

Acquisti, A., and Grossklags, J. 2005. "Privacy and rationality in individual decision making," *IEEE Security & Privacy* (3:1), pp. 26-33 (doi: 10.1109/MSP.2005.22).

Acquisti, A., John, L. K., and Loewenstein, G. 2013. "What Is Privacy Worth?" *The Journal of Legal Studies* (42:2), pp. 249-274.

Agarwal, S., Steyskal, S., Antunovic, F., and Kirrane, S. 2018. "Legislative Compliance Assessment: Framework, Model and GDPR Instantiation," in *Privacy technologies and policy*: *6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised selected papers / Manel Medina, Andreas Mitrakas, Kai Rannenberg, Erich Schweighofer, Nikolaos Tsouroulas (eds.)*, M. Medina, A. Mitrakas, K. Rannenberg, E. Schweighofer and N. Tsouroulas (eds.), Cham, Switzerland: Springer, pp. 131-149 (doi: 10.1007/978-3-030-02547-2_8).

Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Brooks/Cole Publishing Company.: CA: Brooks/Cole Publishing.

Angulo, J., Fischer-Hübner, S., Pulls, T., and Wästlund, E. 2015. "Usable Transparency with the Data Track," in *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, pp. 1803-1808 (doi: 10.1145/2702613.2732701).

Antignac, T., Scandariato, R., and Schneider, G. 2016. "A Privacy-Aware Conceptual Model for Handling Personal Data," in *Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques*, T. Margaria and B. Steffen (eds.), Cham: Springer International Publishing, pp. 942-957 (doi: 10.1007/978-3-319-47166-2_65).

Auty, S. 1995. "Using conjoint analysis in industrial marketing: The role of judgment," *Industrial Marketing Management* (24:3), pp. 191-206 (doi: 10.1016/0019-8501(94)00078-B).

Baier, D., and Brusch, M. 2021. *Conjointanalyse*: *Methoden - Anwendungen - Praxisbeispiele*, Berlin, Heidelberg: Springer Berlin Heidelberg.

Bargh, M. S., van de Mosselaar, M., Rutten, P., and Choenni, S. 2022. "On Using Privacy Labels for Visualizing the Privacy Practice of SMEs," in *The 23rd Annual International Conference on Digital Government Research*, pp. 166-175 (doi: 10.1145/3543434.3543480).

Beke, F. T., Eggers, F., and Verhoef, P. C. 2018. "Consumer Informational Privacy: Current Knowledge and Research Directions," *Foundations and Trends® in Marketing* (11:1), pp. 1-71 (doi: 10.1561/1700000057).

Berendt, B., Günther, O., and Spiekermann, S. 2005. "Privacy in e-commerce," *Communications of the ACM* (48:4), pp. 101-106 (doi: 10.1145/1053291.1053295).

Bier, C., Kühne, K., and Beyerer, J. 2016. "Privacy Insight: The Next Generation Privacy Dashboard," in *4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings*, pp. 135-152 (doi: 10.1007/978-3-319-44760-5_9).

Brandimarte, L., Acquisti, A., and Loewenstein, G. 2013. "Misplaced Confidences," *Social Psychological and Personality Science* (4:3), pp. 340-347 (doi: 10.1177/1948550612455931).

Bruner, G. C. (ed.). 2019. *Marketing scales handbook*, Fort Worth, Texas., Birmingham, AL, USA: GCBII Productions; EBSCO Indusries Inc.

Buchmann, J., Nebel, M., Roßnagel, A., Shirazi, F., Simo, 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 (doi: 10.3233/978-1-61499-295-0-139).

Davenport, T. H. 2006. "Competing on Analytics," *Harvard business review 84*.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80 (doi: 10.1287/isre.1060.0080).

European Union. 2016. *General Data Protection Regulation*: *GDPR*.

Gartner. 2023. "Privacy Management Tools," available at https://www.gartner.com/en/information-technology/glossary/privacy-management-tools.

Gelman, A., Carlin, J. B., Stern, H. S., Dunson, D. B., Vehtari, A., and Rubin, D. B. 2014. *Bayesian data analysis*, Boca Raton, London, New York: CRC Press Taylor and Francis Group.

Goldfarb, A., and Tucker, C. 2012. "Shifts in Privacy Concerns," *American Economic Review* (102:3), pp. 349-353 (doi: 10.1257/aer.102.3.349).

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., and Png, I. P. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13-42 (doi: 10.2753/MIS0742-1222240202).

Hann, I.-H., Kai-Lung, H., Tom, L., and Png, I. (eds.). 2002. *Online Information Privacy: Measuring the Cost-Benefit Trade-Off,* 2002.

Hanneke, B., Baum, L., and Hinz, O. 2023. "GDPR Privacy Type Clustering: Motivational Factors for Consumer Data Sharing," *ECIS 2023 Research Papers* (409).

Hansen, M., Jensen, M., and Rost, M. 2015. "Protection Goals for Privacy Engineering," in *2015 IEEE Security and Privacy Workshops,* San Jose, CA. 21.05.2015 - 22.05.2015, IEEE, pp. 159-166 (doi: 10.1109/SPW.2015.13).

Härting, R.-C., Kaim, R., and Ruch, D. 2020. "Impacts of the Implementation of the General Data Protection Regulations (GDPR) in SME Business Models—An Empirical Study with a Quantitative Design," in *Agents and Multi-Agent Systems: Technologies and Applications 2020 (pp.295-303)*, pp. 295-303 (doi: 10.1007/978-981-15-5764-4_27).

Herder, E., and van Maaren, O. 2020. "Privacy Dashboards: The Impact of the Type of Personal Data and User Control on Trust and Perceived Risk," in *28th ACM Conference on User Modeling, Adaptation and Personalization*, pp. 169-174 (doi: 10.1145/3386392.3399557).

Hevner, A. R., March, Salvatore T. Salvatore T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Q.* (28).

Janßen, C. 2019. "Towards a System for Data Transparency to Support Data Subjects," in *Business Information Systems Workshops*: *BIS 2019 International Workshops, Seville, Spain, June 26-28, 2019, Revised Papers / Witold Abramowicz, Rafael Corchuelo (eds.)*, W. Abramowicz and R. Corchuelo (eds.), Cham: Springer International Publishing; Springer, pp. 613-624 (doi: 10.1007/978-3-030-36691-9_51).

Janßen, C., and Kathmann, J. 2020. "Legal Requirement Elicitation, Analysis and Specification for a Data Transparency System," *Business Information Systems. BIS 2020. Lecture Notes in Business Information Processing* (389), pp. 3-17 (doi: 10.1007/978-3-030-53337-3_1).

Jentzsch, N., Preibusch, S., and Harasser, A. 2012. *Study on monetising privacy: An economic model for pricing personal information. Report*.

Kelting, K., Duhachek, A., and Whitler, K. 2017. "Can copycat private labels improve the consumer's shopping experience? A fluency explanation," *Journal of the Academy of Marketing Science* (45:4), pp. 569-585 (doi: 10.1007/s11747-017-0520-2).

Kirrane, S., Fernández, J. D., Dullaert, W., Milosevic, U., Polleres, A., Bonatti, P. A., Wenning, R., Drozd, O., and Raschke, P. 2018. "A Scalable Consent, Transparency and Compliance Architecture," in *The Semantic Web: ESWC 2018 Satellite Events*, A. Gangemi, A. L. Gentile, A. G. Nuzzolese, S. Rudolph, M. Maleshkova, H. Paulheim, J. Z. Pan and M. Alam (eds.), Cham: Springer International Publishing, pp. 131-136 (doi: 10.1007/978-3-319-98192-5_25).

Kolter, J., Netter, M., and Pernul, G. 2010. "Visualizing Past Personal Data Disclosures," in *International Conference on Availability, Reliability and Security, ARES*, pp. 131-139 (doi: 10.1109/ARES.2010.51).

Lee, Ahn, and Bang. 2011. "Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection," *MIS Quarterly* (35:2), p. 423 (doi: 10.2307/23044050).

Lenk, P. J., DeSarbo, W. S., Green, P. E., and Young, M. R. 1996. "Hierarchical Bayes Conjoint Analysis: Recovery of Partworth Heterogeneity from Reduced Experimental Designs," *Marketing Science* (15:2), pp. 173-191.

Maguire, S., Friedberg, J., Nguyen, M.-H. C., and Haynes, P. 2015. "A metadata-based architecture for user-centered data accountability," *Electronic Markets* (25:2), pp. 155-160 (doi: 10.1007/s12525-015-0184-z).

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), pp. 336-355 (doi: 10.1287/isre.1040.0032).

Martin, K. D., Borah, A., and Palmatier, R. W. 2017. "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing* (81:1), pp. 36-58 (doi: 10.1509/jm.15.0497).

Milne, G. R., Pettinico, G., Hajjat, F. M., and Markos, E. 2017. "Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing," *Journal of Consumer Affairs* (51:1), pp. 133-161 (doi: 10.1111/joca.12111).

Natter, M., and Feurstein, M. 2002. "Real world performance of choice-based conjoint models," *European Journal of Operational Research* (137:2), pp. 448-458 (doi: 10.1016/S0377-2217(01)00147-3).

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100-126 (doi: 10.1111/j.1745-6606.2006.00070.x).

Oppenheimer, D. M., Meyvis, T., and Davidenko, N. 2009. "Instructional manipulation checks: Detecting satisficing to increase statistical power," *Journal of Experimental Social Psychology* (45:4), pp. 867-872 (doi: 10.1016/j.jesp.2009.03.009).

Pandit, H. J., O'Sullivan, D., and Lewis, D. 2018. "Queryable Provenance Metadata For GDPR Compliance," *Procedia Computer Science* (137), pp. 262-268 (doi: 10.1016/j.procs.2018.09.026).

Petronio, S. 1991. "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples," *Communication Theory* (1:4), pp. 311-335 (doi: 10.1111/j.1468-2885.1991.tb00023.x).

Popescu, A., Hildebrandt, M., Breuer, J., Claeys, L., Papadopoulos, S., Petkos, G., Michalareas, T., Lund, D., Heyman, R., van der Graaf, S., Gadeski, E., Le Borgne, H., deVries, K., Kastrinogiannis, T., Kousaridas, A., and Padyab, A. 2016. "Increasing Transparency and Privacy for Online Social Network Users – USEMP Value Model, Scoring Framework and Legal," in *Privacy Technologies and Policy*, pp. 38-59 (doi: 10.1007/978-3-319-31456-3_3).

Preibusch, S., Kübler, D., and Beresford, A. R. 2013. "Price versus privacy: an experiment into the competitive advantage of collecting less personal information," *Electronic Commerce Research* (13:4), pp. 423-455 (doi: 10.1007/s10660-013-9130-3).

Presthus, W., and Sørum, H. 2019. "Consumer perspectives on information privacy following the implementation of the GDPR," *International Journal of Information Systems and Project Management* (7:3), pp. 19-34 (doi: 10.12821/ijispm070302).

Raghavarao, D., Wiley, J. B., and Chitturi, P. 2010. *Choice-Based Conjoint Analysis*, Chapman and Hall/CRC.

Raschke, P., Küpper, A., Drozd, O., and Kirrane, S. 2017. "Designing a GDPR-Compliant and Usable Privacy Dashboard," in *IFIP Advances in Information and Communication Technology*, pp. 221-236 (doi: 10.1007/978-3-319-92925-5_14).

Roßnagel, H., Zibuschka, J., Hinz, O., and Muntermann, J. 2014. "Users' willingness to pay for web identity management systems," *European Journal of Information Systems* (23:1), pp. 36-50 (doi: 10.1057/ejis.2013.33).

Schlereth, C., and Skiera, B. 2012. "DISE: Dynamic Intelligent Survey Engine," in *Quantitative Marketing and Marketing Management*, L. Hildebrandt, W. Fritz, A. Bauer and A. Diamantopoulos (eds.), Wiesbaden: Gabler Verlag, pp. 225-243 (doi: 10.1007/978-3-8349-3722-3_11).

Schlereth, C., Skiera, B., and Schulz, F. 2018. "Why do consumers prefer static instead of dynamic pricing plans? An empirical study for a better understanding of the low preferences for time-variant pricing plans," *European Journal of Operational Research* (269:3), pp. 1165-1179 (doi: 10.1016/j.ejor.2018.03.033).

Smith, Dinev, and Xu. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), p. 989 (doi: 10.2307/41409970).

Sorescu, A. 2017. "Data-Driven Business Model Innovation," *Journal of Product Innovation Management* (34:5), pp. 691-696 (doi: 10.1111/jpim.12398).

Sørum, H., and Presthus, W. 2021. "Dude, where's my data? The GDPR in practice, from a consumer's point of view," *Information Technology & People* (34:3), pp. 912-929 (doi: 10.1108/ITP-08-2019-0433).

Stutzman, F., Gross, R., and Acquisti, A. 2013. "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook," *Journal of Privacy and Confidentiality* (4:2) (doi: 10.29012/jpc.v4i2.620).

Tapsell, J., Akram, R. N., and Markantonakis, K. 2018. "Consumer Centric Data Control, Tracking and Transparency – A Position Paper," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE),* New York, NY, USA. 01.08.2018 - 03.08.2018, IEEE, pp. 1380-1385 (doi: 10.1109/TrustCom/BigDataSE.2018.00191).

Teixeira, A. G., Da Mira, M. S., and Pereira, R. 2019. "The critical success factors of GDPR implementation: a systematic literature review," *Digital Policy, Regulation and Governance* (21:4), pp. 402-418 (doi: 10.1108/DPRG-01-2019-0007).

Tolsdorf, J., Fischer, M., and Lo Iacono, L. 2021. "A Case Study on the Implementation of the Right of Access in Privacy Dashboards," in *Privacy Technologies and Policy*, N. Gruschka, L. F. C. Antunes, K. Rannenberg and P. Drogkaris (eds.), Cham: Springer International Publishing, pp. 23-46 (doi: 10.1007/978-3-030-76663-4_2).

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254-268 (doi: 10.1287/isre.1090.0260).

Westin, A. F. 1968. "Privacy And Freedom," *Washington and Lee Law Review* (25), pp. 166-170.
Westin, A. F. 2003. "Social and Political Dimensions of Privacy," *Journal of Social Issues* (59:2), pp. 431-453 (doi: 10.1111/1540-4560.00072).
Xie, E., Teo, H.-H., and Wan, W. 2006. "Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior," *Marketing Letters* (17:1), pp. 61-74 (doi: 10.1007/s11002-006-4147-1).
Xu, H., Luo, X., Carroll, J. M., and Rosson, M. B. 2011. "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decision Support Systems* (51:1), pp. 42-52 (doi: 10.1016/j.dss.2010.11.017).
Zimmermann, C., Accorsi, R., and Muller, G. 2014. "Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy," in *Availability, reliability, and security in information systems*: *IFIP WG 8.4, 8.9, TC 5 International Cross-Domain Conference, CD-ARES 2014 and 4th International Workshop on Security and Cognitive Informatics for Homeland Defense, SeCIHD 2014, Fribourg, Switzerland, September 8-12, 2014*, S. Teufel, T. A min, I. You and E. Weippl (eds.), Fribourg, Switzerland. 9/8/2014 - 9/12/2014, Cham: Springer, pp. 152-157 (doi: 10.1109/ARES.2014.27).

Appendix

Attributes *(range)*	**Attribute levels** *(keyword)*
Transparenz *(3)*	• diese per *Post* an Sie verschickt werden. • Ihnen auf Anforderung ein einmaliger *digitaler Zugriff* auf die Informationen gewährt wird (z. B. E-Mail oder Download). • Sie diese Daten über ein *Dashboard* jederzeit online aufrufen können.
Verwaltung der Datenweitergabe *(3)*	• *Einzeln*, d. h. jede Einwilligung zur Datenweitergabe muss individuell und manuell ausgewählt werden. • *Einwilligungsprofile*, d. h. Erteilung von voreingestellten Einwilligungen mit einem Klick z. B. basierend auf einer Auswahlempfehlung von Daten- und Verbraucherschutzorganisationen. • *Pauschale maximale Einwilligung*, d. h. mit einem Klick wird der umfassenden Datenweitergabe zugestimmt.
Datenverarbeitung für Marketingzwecke *(4)*	• *keine Datenweitergabe* für Marketingzwecke, dafür sind Empfehlungen bei weiteren Einkäufen jedoch nur zufällig. • *anonymisiert*, dafür sind Empfehlungsqualität und -relevanz bei weiteren Einkäufen nur gering. • *personenbezogen*, dafür sind Empfehlungsqualität und -relevanz bei weiteren Einkäufen gut. • *umfassend*, dafür sind Empfehlungsqualität und -relevanz bei weiteren Einkäufen sehr gut.
Rabattstufen *(4)*	• 0% • 4% • 8% • 12%

Table 6. Attributes and attribute levels of CBC (German original)

Construct	**Item**
Privacy importance (Martin et al. 2017)	Bewerten Sie folgende Aussagen zur Privatsphäre: (1 stimme überhaupt nicht zu) – (7 stimme voll und ganz zu)
	• Ich bin sensibel für die Art und Weise, wie Unternehmen mit meinen persönlichen Daten umgehen.
	• Es ist wichtig, dass meine Privatsphäre gegenüber Online-Unternehmen gewahrt bleibt.
	• Die persönliche Privatsphäre ist im Vergleich zu anderen Themen sehr wichtig.
	• Ich bin besorgt über die Bedrohung meiner persönlichen Privatsphäre.
Knowledge of the GDPR (adapted from Kelting et al. 2017)	• Wie vertraut sind Sie mit der DSGVO (Datenschutz-Grundverordnung)? (1) gar nicht vertraut – (7) sehr vertraut
	• Wie viel wissen Sie über die DSGVO? (1) sehr wenig – (7) sehr viel

	• Wie würden Sie Ihr Wissen über die DSGVO im Vergleich zum Rest der Bevölkerung einschätzen? (1) Ich bin unter den am wenigsten Wissenden – (7) Ich bin unter den am meisten Wissenden
Choice difficulty (Kelting et al. 2017)	Insgesamt waren die Entscheidungen für eine Konfiguration aus der Auswahl: (1) – (7)
	• überhaupt nicht schwierig – extrem schwierig
	• überhaupt nicht verwirrend – extrem verwirrend
	• überhaupt nicht überwältigend – extrem überwältigend

Table 7. Latent constructs and items (German original)

Cluster demographics		**Clusters**				**Total sample**
		1 uncon-cerned	2 pragma-tists	3 amateurs	4 funda-mentalists	
Observations n		90	141	157	201	589
Age (in years)	Mean**	36.4	40.1	47.1	46.6	43.6
	Std.	15.4	13.7	15.5	13.7	15.0
Gender (in %) (** if excluding "diverse")	male	50.0	58.2	38.5	54.7	50.5
	female	50.0	40.4	61.5	45.3	49.1
	diverse	–	1.4	–	–	.4
Education (in %)**	university degree	18.9	39.3	23.1	37.8	31.3
	no university degree	81.1	60.7	76.9	62.2	68.7
Occupational status (in %)**	working	46.6	71.4	53.9	71.2	63.0
	not working	53.4	28.6	46.1	28.8	37.0
Income range (in k euro)	Median	20-40	40-60	20-40	20-40	20-40
Private Internet time (in hours per day)	Mean	4.2	3.9	3.6	3.7	3.8
	Std.	3.1	2.9	2.6	3.0	2.9
Note: Between-group difference significance ** at $p < 0.01$ using Kruskal-Wallis tests.						

Table 8. Demographics of our sample (n = 589) for each cluster

(in % of respondents)		**Gender**			**Total sample**
		male	female	diverse	
Age groups	< 18	0.9	1.0	–	1.9
	18 - 24	5.0	6.6	.2	11.8
	25 - 34	10.0	7.8	.2	18.0
	35 - 44	8.8	8.7	–	17.5
	45 - 54	10.5	9.2	–	19.7
	55 - 64	11.4	12.9	–	24.3
	65+	3.9	2.9	–	6.8
Total sample		50.5	49.1	.4	100.0

Table 9. Distribution of age and gender within our sample (n = 589)