Privacy and Personalization: The Trade-off between Data Disclosure and Personalization Benefit

Lisa-Marie Wadle
lisa-marie.wadle@ibp.fraunhofer.de
Fraunhofer IBP, Institute for Building Physics
Stuttgart, Germany

Noemi Martin
noemi.martin@ibp.fraunhofer.de
Fraunhofer IBP, Institute for Building Physics
Stuttgart, Germany

Daniel Ziegler
daniel.ziegler@iao.fraunhofer.de
Fraunhofer IAO, Institute for Industrial Engineering
Stuttgart, Germany

ABSTRACT

Personalization in principle cannot happen without information about individuals, requiring personalization systems to comply with official privacy regulations. However, in order to design personalization systems that provide the best possible privacy-related user experience, a more human-centered perspective has to be taken into account. As a first step towards this goal, in the present work we show the setup and results of an online survey investigating the relation between the intention to disclose certain categories of personal data and the type of benefit promised by personalization.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; • **Human-centered computing** → *Empirical studies in HCI*.

KEYWORDS

Personalization; Privacy Calculus; Positive User Experience; Personal Data; Data Protection

ACM Reference Format:
Lisa-Marie Wadle, Noemi Martin, and Daniel Ziegler. 2019. Privacy and Personalization: The Trade-off between Data Disclosure and Personalization Benefit. In *27th Conference on User Modeling, Adaptation and Personalization (UMAP '19 Adjunct), June 9–12, 2019, Larnaca, Cyprus.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3314183.3323672

1 INTRODUCTION AND BACKGROUND

By its very nature, disclosure of personal information is an essential prerequisite in the context of personalization [14]. How else could personalization systems recommend contents or products matching individual interests or adapt the presentation and interaction mechanisms of user interfaces according to individual needs? However, intensified by public discussions in media, people are increasingly privacy concerned [7, 20]. Users are unsure about what happens with their personal data or feel threatened by hackers [9].

One means that many privacy regulations and recommendations incorporate in order to address this issue is the principle of *data minimization*. It requires that personal data is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [5, art. 5 par. 1 lit. (c)]. Traditional approaches often start from usage data that is already available or can be collected easily [13].

Argumentation regarding privacy and why certain data is required for the personalization purpose might be difficult in these cases. The field of *privacy-enhanced personalization* therefore starts from the privacy perspective and aims "to strive for best possible personalization within the boundaries set by privacy" [14, p. 26].

However, the question regarding how much and what kind of information users are willing to provide cannot be answered easily. Personal data is not only of economic value but also has a specific value for individuals. In the framework of the *Privacy Calculus Theory* [3], the intention of disclosing personal data results from rationally weighing against each other potential risks and benefits. Thus, the decision to disclose data or not can be influenced by the type of data to be disclosed (risk) [14] as well as the benefit promised in return for the data disclosure (utility) [2, 16].

However, as Norberg et al. describe in the so-called *Privacy Paradox* [17], the phenomenon that people do not actually behave according to their expressed intentions with regard to the disclosure of personal information still makes it hard to understand how people decide about data disclosure. The authors argue that the intention to provide personal data is mainly driven by an assessment of the associated risk while actual disclosure behaviour is more influenced by an evaluation of trust in the organization that receives the data.

The level of trust in the receiving organization is a major factor that is taken into account when people decide on disclosure of their personal data [1, 12]. Not disclosing data because of lacking trust might result from the fact that today users are oftentimes confronted with an all-or-nothing decision in privacy policies. Instead, providing them with more fine-grained control can lead to improved trust by users in the organization asking for personal data [15]. Knijnenburg and Kobsa aggregate the factors of trust and self-anticipated satisfaction under the concept of user experience and show that better user experience finally leads to increased actual disclosure of personal information [12].

In general, *positive user experience* is known to emerge when basic needs of the users are addressed [8]. Those needs can also be used to systematically design interactive products or services in order to provide users with positive experiences [6]. For example, the satisfaction of the need for influence might explain the positive effect of more detailed privacy policies [15]. Conversely, the violation of existing user needs leads to negative user experiences associated with the respective product or service. Thus, the existence of the privacy paradox potentially has a negative impact on the overall

UMAP '19 Adjunct, June 9–12, 2019, Larnaca, Cyprus

user experience of personalization systems. It might violate users' needs for competence, self-expression, influence and even security when becoming aware that personal data was disclosed that actually was intended to be kept private.

Thus, given that data disclosure is a prerequisite for the purpose of personalization, minimizing the effect of the privacy paradox by focusing on users' disclosure intention can lead to an improved overall user experience. In order to enable the design of such personalization systems, it is essential to understand how different factors influence the emergence of users' intentions to disclose personal data.

2 RESEARCH QUESTION AND HYPOTHESES

With the aim of contributing to privacy-enhanced personalization processes and hence, better user experience, we designed a study that helps to better understand if and how the intentions of a user to disclose certain categories of personal data depends on the type of benefit promised by a personalization scenario. According to the privacy calculus model, different types of *data categories* represent different levels of risk and the utility of personalization was varied by presenting different *benefit scenarios* in this study. Following the overall research question just mentioned we established three hypotheses as follows.

First, previous studies [12, 14] suggest that people value some categories of personal data more than others in their individual privacy calculus. Accordingly, we expect that participants will agree to disclose some data categories more often than they do for other categories:

Hypothesis 1 (H1). *The intention to disclose personal data depends on the type of data category.*

Second, personalization services and personalized products can provide diverse types of benefits like saving time or getting something unique (see section 3.1 for the list of benefits used in this study). We expect that people in general value some of the benefits promised by personalization more than others in their individual privacy calculus. Accordingly, these types of benefits will motivate participants to disclose more personal information than other benefits:

Hypothesis 2 (H2). *The intention to disclose personal data depends on the benefit scenario promised by personalization.*

H1 and H2 refer to the variation of disclosure intention related to either data categories or benefit scenarios separately. However, we expect that there is a connection between both factors and consequently identifying some categories of personal data that are more dependent on the type of personalization benefit than other categories:

Hypothesis 3 (H3). *The intention to disclose personal data is the result of an interaction between type of data category and benefit scenario.*

3 STUDY DESIGN

An online survey was conducted in Germany over the course of 10 days in order to evaluate the hypotheses mentioned above.

3.1 Apparatus and materials

As, to the best of our knowledge, no suitable stimulus material for our purpose and in German language could be found in previous research we developed item stimuli (data categories and personalization benefit scenarios) in the first step.

Data categories. A list of 17 categories of personal data was developed from which participants had to decide to disclose the respective information or not (Table 1). The list includes 8 data categories referred to as special categories of personal data according to the General Data Protection Regulation (GDPR) due to their sensitivity [5, art. 9 par. 1]. These special data categories which are marked with an *_s* in the table below. The remaining 9 data categories and the examples for each category were derived from websites concerning privacy [4, 10].

Benefit scenarios. A list of 10 benefit by personalization scenarios was developed to point out the various positive outcomes personalization can have which consequently are likely to have an impact on a person's privacy calculation. The benefit scenarios where developed during a group discussion in a research team of psychologists and user experience experts. The list consists of benefits being discussed in the High Performance Center for Mass Personalization[1] or in past research [2, 16]. Some of the benefits refer to basic need theories [19]. In order to prevent participants to rate the potential influence of the data categories on the personalization of a specific product we used abstract descriptions of the potential benefits. To prevent trust to influence the disclosure intention, the scenarios did not mention a receiving organization of the disclosed data.

The stated question (here exemplified for the benefit of saving the environment) was *If you were to save the environment by the personalization of a product, what kind of data would you disclose in return?* or a slightly adapted version of it. Benefit scenarios were as follows (translated from German): save the environment, save money, save time, get something unique, get something absolutely appealing, facilitate decisions, experience something new, do something good for health, get closer to a personal goal, enhance security.

Privacy Concern. A German translation of the Concerns for Information Privacy (CFIP) questionnaire [7] was used in order to assess the participants' individual levels of privacy concern with regard to organizational privacy practice. The instrument consists of 15 items which had to be rated on a seven-point Likert scale ranging from *do not agree at all* to *totally agree* (see [7] and [20] for a detailed description of the tool).

Technical Affinity. The TA-EG questionnaire [11] was used in order to evaluate sample characteristics concerning level of technical affinity. The authors define technical affinity as a personality trait expressing a person's positive attitude, enthusiasm and trust towards technology. Further, we added a control question *Basically, I do not use electronic devices.* We presume that people do have to use electronic devices when being part of an online study panel and filling out online surveys. Thus, we concluded that participants rating this question with *totally agree* or *rather agree* did not participate in the survey seriously and consequently were excluded from the study sample. Hence, in total 20 items had to be rated on a 5-point scale ranging from *do not agree at all* to *totally agree.*

[1] https://www.masspersonalization.de/

Table 1: Categories of personal data used in the online questionnaire (translated from German)

ID	Title	Examples
racial_s	racial or ethnic origin	skin color, ethnicity, nationality
political_s	political opinions	political interest, opinions regarding current topics, voting behavior
religious_s	religious or philosophical beliefs	values and moral concepts, faith communities, conscience
associations_s	membership in associations	political parties, trade unions, associations
genetic_s	genetic data	biological ancestry, disease dispositions, DNA analyses
biometric_s	biometric data for unique identification	fingerprints, facial images, iris scan
health_s	physical or mental health	diagnoses, health, medications
sex_s	data concerning sex life	sexual orientation, frequency, prevention
IDs	identification numbers	social security number, ID number, personnel number
demo	demographic data	age, date of birth, marital status
contact	contact information	home address, phone numbers, email addresses
physical_charact	physical characteristics	weight, hair color, shoe size
financial	financial situation	capital assets, income, liabilities
profession	professional training and occupation	attended schools and universities, obtained degrees, past occupations
relationships	relationship with other persons	relatives, colleagues, frequency of contact
abilities	physical and mental abilities	visual acuity, maximum grip force, IQ
thematic	thematic interests	hobbies, leisure activities, musical style

3.2 Procedure

After opening the online survey, the concept of personalization and the procedure of the study were explained to the participants. An example trial illustrated the task (see Figure 1): In each trial, a benefit scenario was presented as well as a list of data categories. Benefit scenarios and data categories were presented in a randomized way. For each benefit scenario the participants had to select all of the data categories they intended to disclose for the personalization of a product with the stated benefit. Chosen data categories had to be dragged to the box *your choice* (see Figure 1). After having completed the procedure for 10 benefit scenarios, participants filled out the TA-EG [11] and the CFIP [7]. The survey was designed to take 15-20 minutes for full completion and was carried out using a self-hosted installation of the online survey tool LimeSurvey[2].

3.3 Study Sample

Participants were invited to the online study via a certified German panel provider and sample quotas regarding sex and age distribution representing German population were set as inclusion criteria. A total of 1,121 participants filled out the survey completely. Data sets were sorted out when participants answered the control question (see 3.1) in a conspicuous way (110 drop-outs). Further, outliers were defined via overall time needed to fill out the survey (cut-off maximum: $mean + 1,5 * IQR$ (80 drop-outs), cut-off minimum: set to 10 minutes (368 drop-outs)). Additionally, 2 participants were excluded due to overall missing values in the CFIP. Thus, the final data set included 561 participants (45% male) with an age distribution similar to the proposed census age distribution.

Descriptive statistics of the CFIP and the TA-EG were analyzed in order to identify noticeable characteristics of the study sample. For the CFIP, the overall mean (median) was 6.00 (6.21) and means per participant ranged from 1 to 7 points ($SD = 0.76$). The overall mean score was slightly higher compared to past findings [20]. For the TA-EG the overall mean (median) was 3.24 (3.25) and means per participant ranged from 2.20 to 4.10 points ($SD = 0.36$). The characteristics suggest that the sample is, against our expectations, rather highly concerned about privacy and not exceptional concerning technical affinity.

[2]https://www.limesurvey.org/

4 RESULTS

For analyses, the dichotomous variable (intention to disclose data or not) was transformed into relative frequencies. First, descriptive statistics of variables serving as manipulation checks are reported and second, hypotheses are tested.

Manipulation Checks. As manipulation checks, the influence privacy concerns as well as data sensitivity level (as described in 3.1) on data disclosure intention was analyzed. This was necessary in order to test the general plausibility of the design of the study as material was used for the first time. A small to medium sized correlation between privacy concern scores and the total amount of data a person intended to disclose was found ($r(559) = -.21, p < .01$). It indicates that, as expected, participants with higher privacy concern scores intend to disclose less data compared to participants with lower privacy concern scores. A paired-sample t-test indicates that significantly less sensitive data as defined in the GDPR ($M = 0.23, SD = 0.23$) was intended to be disclosed compared to the other data categories ($M = 0.35, SD = 0.23; t(560) = 21.72, p < .01, d = 0.92$). The results support the design of the study.

H1: Data Categories. In order to evaluate whether the different categories of data vary with regard to the frequency with which they are intended to be disclosed, data was collapsed over all benefit scenarios. Boxplots of all data categories are shown in Figure 2 revealing a heterogeneous pattern. For some data categories variance was quite large (e.g. racial, demographic) and for other categories quite small (e.g. IDs, biometric). Means indicate that on average some data categories were intended to be disclosed more often (e.g.

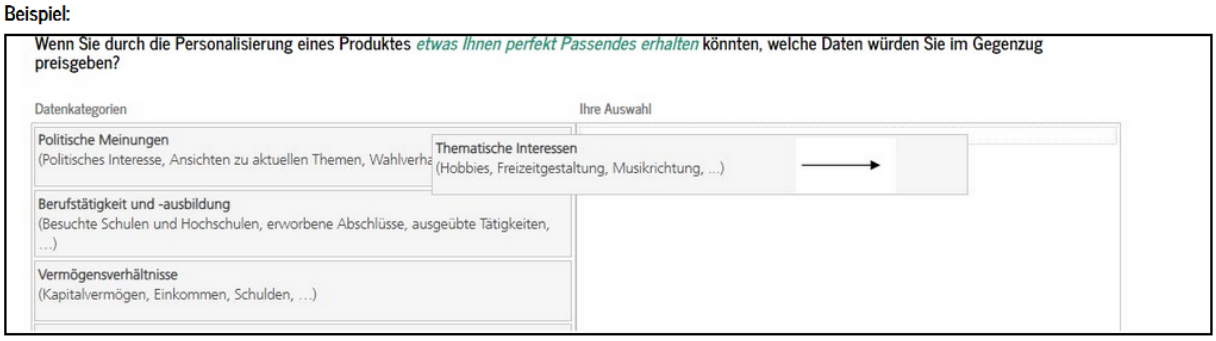

Figure 1: Screenshot of the example trial presented to participants explaining how to select data categories by Drag & Drop they would disclose for each benefit scenario.

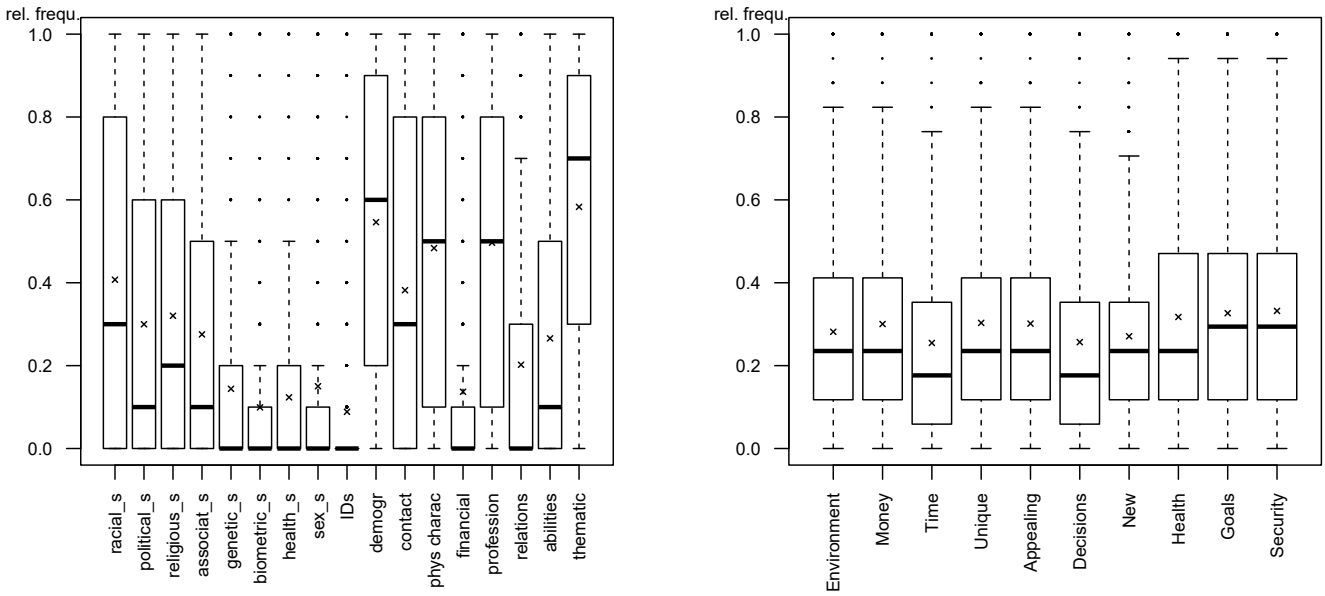

Figure 2: Boxplots displaying the relative frequencies with which data was intended to be disclosed depending on type of data category (left) and benefit scenario (right). Small crosses indicate group means, vertical bars medians and dots outliers.

thematic interests) compared to others (e.g health information). As the values of the dependent variable were not distributed normally, a non-parametric Friedman test was conducted. The results indicate that the amount of information intended to be disclosed differed significantly depending on data category ($\chi^2(16) = 2929.75, p < .01$) resulting in a large effect.

H2: Benefit Scenarios. In order to evaluate whether the different benefit scenarios had an effect on the amount of data a person intended to disclose, data was collapsed over all data categories. Boxplots of all benefit scenarios are shown in Figure 2. The variance was quite large over all benefit scenarios and means differed slightly after visual inspection. As the values of the dependent variable were not distributed normally, a non-parametric Friedman test was conducted in order to evaluate differences in benefit scenarios. The results indicate that the amount of data categories intended to be disclosed differed significantly depending on benefit scenario ($\chi^2(9) = 246.57, p < .01$) resulting in a moderate to large effect.

H3: Interaction of Benefit Scenario and Data Category. The interaction between benefit scenario and data category was analyzed in an exploratory way employing a heat map (see Figure 3). For each combination of data category and benefit scenario the color pattern indicates the relative frequencies with which the data was intended to be disclosed (e.g. a red box implying lower frequencies than a yellow box). The following observations can be made by analyzing the heat map visually.

First, the figure can be inspected column wise. It is interesting to note that for some data categories the pattern is rather homogeneous indicating that this data category is intended to be disclosed with a certain frequency independent of benefit scenarios (e.g. overall low frequency for *financial situation* data and comparatively high

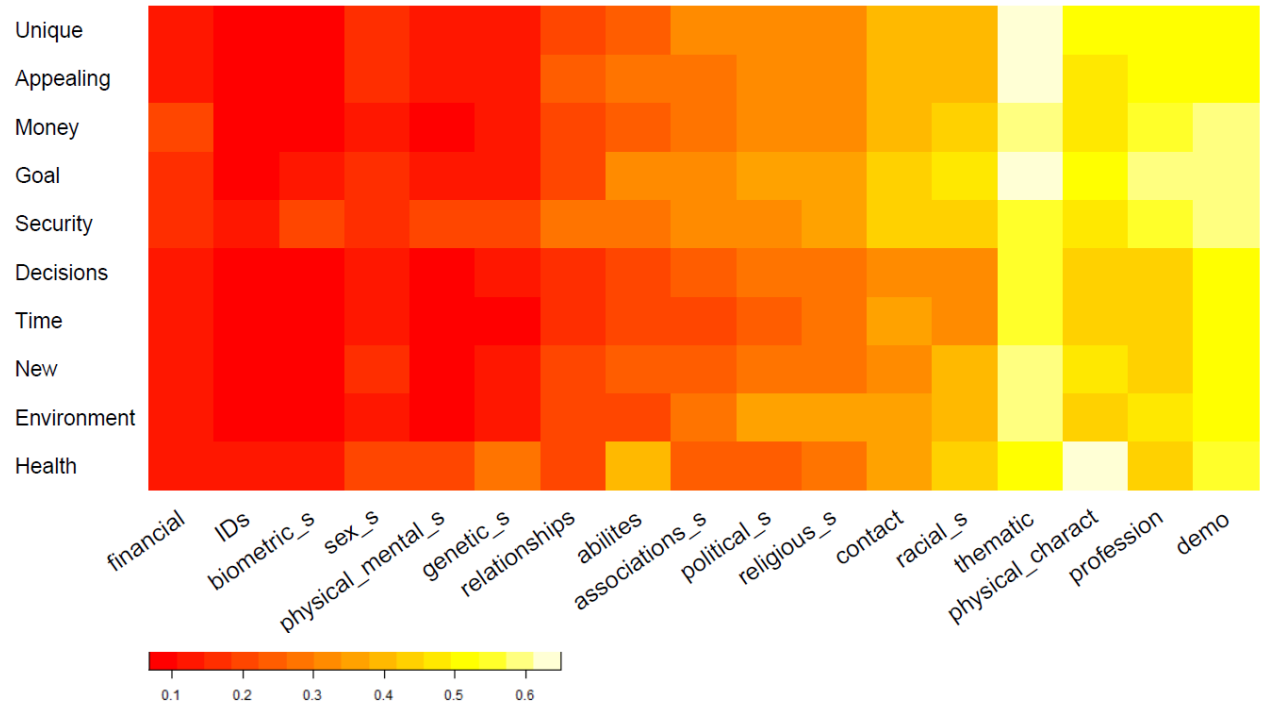

Figure 3: Heat map displaying the relative frequencies data categories were intended to be disclosed with for all combinations of benefit scenarios and data categories (e.g. 0.1 = 10% of the sample intended to disclose information of this data category for the stated benefit through personalization).

frequency for *demographic information*). For other data categories columns are colored heterogeneously indicating that disclosure intention of data depends on benefit scenario (e.g. the frequency to disclose information about someone's *abilities* seems to increase in the case of promised health benefits through personalization compared to the benefit of time saving). To summarize, for some data categories, the intention to disclose information depends on benefit scenarios and for some data categories, this decision is independent of the benefit scenario. Further, it is noticeable that when comparing GDPR special categories of data (marked with an *_s*) to other data categories, the division is not clear-cut: For instance, *financial* information was intended to be disclosed very rarely over all benefit scenarios even though not being referred to as a special category of data whereas data concerning *racial or ethnic origin* was disclosed more frequently than expected for a sensitive data category. *On average* special categories of data were disclosed less frequently than other categories of data, although particular cases deviate from this pattern. The results suggest that data that allows definite identification of a person (e. g. IDs, genetics) was intended to be disclosed less frequently (with the exception of contact information) compared to data that cannot identify a specific person.

Second, data can be inspected row wise, i.e. for each benefit scenario. Here, it has to be noted that for each benefit scenario a heterogeneous pattern is observed regarding the frequencies of disclosing the different data categories. For none of the benefit scenarios every data category or none of the data categories was intended to be disclosed. Further, the graphic suggests that for certain benefit scenarios like *Security* and *Health* the color pattern is slightly lighter and hence indicates that data was intended to be disclosed more often. In contrast, for the benefit scenarios *Save Time* and *Decisions*, the color pattern tends to be darker suggesting rather low frequencies of disclosure intention. The results suggest that for the satisfaction of basic human needs like health or safety disclosure of data is more likely.

Third, analyzing the heat map in an overall manner, it can be concluded that the frequency personal information is intended to be disclosed with depends on the interaction of benefit scenario and type of data category. The combination for which the highest percentage of participants would disclose data was *thematic interests* for the benefit of getting something perfectly appealing through personalization (65% of the sample). In contrast, only 7% of the sample would disclose data concerning *IDs* for the benefit of getting something new. Further, regarding color pattern consistence most notably, the pattern for the *Health* benefit scenario deviates from the overall gradient in the data categories regarding *physical and mental abilities*, *physical characteristics* and *genetic data*. Smaller deviations can be identified for the *Money* benefit scenario in combination with *financial situation* data as well as for the *Security* scenario and the *biometric data* category. These pattern deviations suggest that participants more likely intent to disclose data when they expect some relation of that data to the promised benefit even though only abstract benefit scenarios were used in the study.

5 CONCLUSION AND FUTURE WORK

In the present work, the trade-off between the intention of data disclosure and personalization benefit was evaluated in an online study. An interaction between type of data category and benefit promised by personalization was found. The results suggest that data from a specific data category is less frequently intended to be disclosed when it allows distinct identification of a person (e.g. genetic data). Additionally, findings indicate that people are more willing to disclose data when in the promised benefit scenario basic human needs like health or security are fulfilled. This makes sense from an evolutionary perspective.

This work presents a first step into understanding better the intentions to disclose personal data in the framework of the privacy calculus. As the study was run in Germany and privacy is culture dependent [18], the results are limited in generality to other countries. Replicating the study in other countries, with different nationalities or against the background of other social norms might reveal different patterns. Further, exploratory analyses presented here can be extended by more detailed analyses of the combinations of data categories and benefit scenarios. The heat map suggests vaguely that participants do evaluate if there is a reasonable link between data category and benefit scenario and that disclosure of data is more likely in cases where this relationship is more obvious (e.g. disclosure of financial data for a finance-related benefit). It would also be helpful to develop a theoretical framework in order to better understand the complex interaction of the variables. Moreover, is was interesting to see that the distinction between special data categories and other data is not clear-cut. Hence, it is not sufficient to only protect strongly the types of data that are referred to as special categories in current privacy legislation since other categories of personal data can also be of very high value for users and have to be treated carefully.

To conclude, this study allows insights into the decision making process of data disclosure for the purpose of personalization. The results suggest that the interaction of data category and promised benefit by personalization has to be taken into account when aiming at designing personalization processes in an user experience friendly way. Empowering users to align their actual disclosure behaviour to their individual intention to disclose of personal information will help to prevent the privacy paradox and thus, result in an improved user experience of personalized products and services. Finally, individual differences between users lead to the challenge to implement some kind of *meta personalization* of the personalization process itself including privacy-related mechanisms. This challenge has to be overcome in order to guarantee a positive user experience in the context of personalization.

ACKNOWLEDGMENTS

The authors would like to thank the Ministry of Science, Research and Arts and the Ministry of Economic Affairs, Labor and Housing Construction of Baden-Württemberg for the financial support of the projects within the High-Performance Center for Mass Personalization Stuttgart.

REFERENCES

[1] Susanne Barth and Menno D.T. de Jong. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics* 34, 7 (Nov. 2017), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

[2] Caitlin D. Cottrill and Piyushimita "Vonu" Thakuriah. 2015. Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. *Transportation Research Part C: Emerging Technologies* 56 (July 2015), 132–148. https://doi.org/10.1016/j.trc.2015.04.005

[3] Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10, 1 (Feb. 1999), 104–115. https://doi.org/10.1287/orsc.10.1.104

[4] Datenschutz.org 2018. Was sind personenbezogene Daten? Retrieved March 13, 2019 from https://www.datenschutz.org/personenbezogene-daten/

[5] European Parliament and Council. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved March 13, 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[6] Nora Fronemann and Matthias Peissner. 2014. User Experience Concept Exploration: User Needs As a Source for Innovation. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational (NordiCHI '14)*. ACM Press, New York, NY, USA, 727–736. https://doi.org/10.1145/2639189.2641203

[7] David Harborth and Sebastian Pape. 2018. German Translation of the Concerns for Information Privacy (CFIP) Construct. *SSRN Electronic Journal* (2018), 12. https://doi.org/10.2139/ssrn.3112207

[8] Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. 2010. Needs, affect, and interactive products – Facets of user experience. *Interacting with Computers* 22, 5 (Sept. 2010), 353–362. https://doi.org/10.1016/j.intcom.2010.04.002

[9] Thomas J. Holt and Eric Lampke. 2010. Exploring stolen data markets online: products and market forces. *Criminal Justice Studies* 23, 1 (2010), 33–50. https://doi.org/10.1080/14786011003634415

[10] JuraForum 2018. Sensible Daten §3 Abs. 9 BDSG a.F. – Definition & Beispiele. Retrieved March 13, 2019 from https://www.juraforum.de/lexikon/sensible-daten-s-3-abs-9-bdsg

[11] Katja Karrer, Charlotte Glaser, Caroline Clemens, and Carmen Bruder. 2009. Technikaffinität erfassen – der Fragebogen TA-EG. In *Der Mensch im Mittelpunkt technischer Systeme. 8. Berliner Werkstatt Mensch-Maschine-Systeme*, C. Stößel und C. Clemens A. Lichtenstein (Ed.). ZMMS Spektrum, Vol. 22. VDI Verlag GmbH, Düsseldorf, 196–201.

[12] Bart P. Knijnenburg and Alfred Kobsa. 2013. Making Decisions About Privacy: Information Disclosure in Context-Aware Recommender Systems. *ACM Trans. Interact. Intell. Syst.* 3, 3, Article 20 (Oct. 2013), 23 pages. https://doi.org/10.1145/2499670

[13] Alfred Kobsa. 2001. Generic User Modeling Systems. *User Modeling and User-Adapted Interaction* 11, 1/2 (March 2001), 49–63. https://doi.org/10.1023/a:1011187500863

[14] Alfred Kobsa. 2007. Privacy-enhanced personalization. *Commun. ACM* 50, 8 (Aug. 2007), 24–33. https://doi.org/10.1145/1278201.1278202

[15] Oluwa Lawani, Esma Aïmeur, and Kimiz Dalkir. 2016. Improving Users' Trust Through Friendly Privacy Policies: An Empirical Study. In *Risks and Security of Internet and Systems (Lecture Notes in Computer Science)*, Costas Lambrinoudakis and Alban Gabillon (Eds.), Vol. 9572. Springer International Publishing, Cham, 55–70. https://doi.org/10.1007/978-3-319-31811-0_4

[16] Jin-Myong Lee and Jong-Youn Rha. 2016. Personalization-privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior* 63 (2016), 453–462. https://doi.org/10.1016/j.chb.2016.05.056

[17] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41, 1 (March 2007), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[18] Eva-Maria Schomakers, Chantal Lidynia, Dirk Müllmann, and Martina Ziefle. 2019. Internet users' perceptions of information sensitivity-insights from Germany. *International Journal of Information Management* 46 (2019), 142–150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

[19] Kennon M. Sheldon, Andrew J. Elliot, Youngmee Kim, and Tim Kasser. 2001. What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of Personality and Social Psychology* 80, 2 (2001), 325–339. https://doi.org/10.1037/0022-3514.80.2.325

[20] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly* 20, 2 (June 1996), 167–196. https://doi.org/10.2307/249477