



THE PERSONALIZATION PRIVACY PARADOX: THE IMPACT OF PERCEIVED DATA SENSITIVITY ON THE EFFECT OF TRANSPARENCY FEATURES

Master's Thesis

from

Aaron Kopf

Matriculation Numbers: 85724 (Passau) and 2104611 (Turku)

University of Passau

and

University of Turku

Supervisors: Prof. Dr. Thomas Widjaja

Prof. Jukka Heikkilä

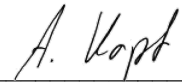
Assisted by: Philipp Sleziona

20. September 2022

Declaration of Authorship

I hereby give my truthful assurance that I have written the work independently and have not used any sources and aids other than those indicated that I have marked the passages taken over either literally or in terms of content as such and that I have observed the statutes of the University of Passau for the safeguarding of good scientific practice in the currently valid version.

Passau, 20th September 2022

A handwritten signature in black ink, appearing to read 'A. Kopf', is written above a horizontal line.

Aaron Kopf

Table of Contents

List of Figures	v
List of Tables.....	vi
1 Introduction	1
2 Theoretical Background	2
2.1 Privacy.....	2
2.2 Personalization	3
2.3 Personalization Privacy Paradox.....	3
2.4 Transparency Features.....	4
2.5 Data Sensitivity	5
2.6 Privacy Calculus.....	5
3 Method.....	5
4 Relevant Factors of the Personalization Privacy Paradox	7
4.1 Context	7
4.1.1 Types of Personalization	7
4.1.2 Pull versus Push based Personalization.....	8
4.1.3 Information Security	10
4.1.4 Transparency Features.....	10
4.1.5 Situation	11
4.1.6 Personalization Intensity	11
4.1.7 Sensitivity of Data.....	13
4.2 Inner Working Mechanism of the Personalization Privacy Paradox	13
4.2.1 Impact of Personalization on the Benefits versus Privacy Concerns Trade-off.....	13
4.2.2 Different Privacy Personalities.....	15
4.2.3 Happiness	16
4.2.4 Trust	17
5 Quantitative Experiment	18
5.1 Goal of Experiment	18
5.2 Hypothesis Development	19
5.2.1 The Privacy Calculus	19
5.2.2 Transparency Features and Data Sensitivity	20

5.2.3	Trust	21
5.2.4	Model Presentation.....	22
5.3	Survey Context.....	22
5.4	Survey Procedure	23
5.5	Data Analysis and Results	28
5.5.1	Participation and Group Distribution	28
5.5.2	Manipulation Check	29
5.5.3	Model Test.....	31
5.5.4	Effect of Data Sensitivity	33
5.5.5	Effect of Different Privacy Personalities.....	35
5.5.6	Demographic Effects	38
6	Discussion.....	39
	References.....	45
	Appendix	49

List of Figures

Figure 1: Search String of Structured Literature Review	6
Figure 2: Hypothesis Model.....	22
Figure 3: Age Distribution	28
Figure 4: Comparing the Two Transparency Groups.....	33
Figure 5: Differences in the Sensitivity Perception.....	36
Figure 6: Hypothesis Model with Privacy Group Separation	37

List of Tables

Table 1: Measured Constructs in the Survey	27
Table 2: ANOVA Test for the Three Groups.....	29
Table 3: Descriptive Survey Information.....	29
Table 4: Descriptive Survey Information Part 2	30
Table 5: Path Model Estimation and Hypothesis Evaluation.....	32
Table 6: Total Effects of Transparency Features and Trust	32
Table 7: Total Effects of Data Sensitivity when Group 2 and 3 are compared.....	34
Table 8: Group Differences in the Context of Privacy Personalities	35
Table 9: Gender Differences Across Groups	38
Table 10: Age Differences Across Groups.....	39
Table 11: Concept Matrix Part 1	49
Table 12: Concept Matrix Part 2	50

1 Introduction

The possibility to collect huge amounts of data gives companies new opportunities to reshape their business models or to create new ones. One possibility for data usage is to offer personalized services or advertisement, tailoring the offer to the users' interests and needs (Cloarec, 2020; Xu, Luo, Carroll, & Rosson, 2011). The use of personalization has the potential to gain competitive advantage. Personalization can for example have a huge positive impact for retailers, as it can increase spontaneous purchases (Thirumalai & Sinha, 2013; Xu et al., 2011). It can also extend the time a service is used, or the amount of data disclosed to the provider (Sutanto, Palme, Tan, & Phang, 2013). Therefore, personalization is an attractive way to generate positive outcomes for a business. However, companies face the problem that personalization does not only come with positive impacts, but also raises privacy concerns (Bleier & Eisenbeiss, 2015; Karwatzki, Dytynko, Trenz, & Veit, 2017; Sutanto et al., 2013). This paradoxical situation, where personalization provider create value, but also concerns for users due to personalization, is called the personalization privacy paradox (Hayes, Brinson, Bott, & Moeller, 2021; Sutanto et al., 2013; Xu et al., 2011).

Conducting research in the area of the personalization privacy paradox comes with similar problems compared to other privacy related research: individuals perceptions about privacy and their data disclosure process is a complex, psychological issue. The perceptions can for example be different from culture to culture, different in various contexts, or are dependent on the person who is providing the data (Acquisti, John, & Loewenstein, 2012; Kehr, Kowatsch, Wentzel, & Fleisch, 2015; Westin, 1991). The complexity explains why various research is necessary, which is also the case for the personalization privacy paradox. For example, Awad and Krishnan (2006) argued that companies should focus on the benefits of personalization, while trying to minimize the privacy concerns is less important. In contrast, Sutanto et al. (2013) showed that building a privacy-safe environment could help companies to increase usage of services, as well as the data disclosure rate. Thus, they argue that such an environment can overcome the personalization privacy paradox. These differences indicate a need for further research.

The goal of this work is to conduct a structured literature review to present the current standing of the literature. This thesis firstly investigates some contextual factors, which are the prerequisites for users when they face a personalized situation. The second goal is to analyze the inner work mechanism of individuals to find out over which avenues personalization succeeds. This is also important for companies to understand how the decision process of users is developing.

After the presentation of the literature, an own quantitative experiment is introduced. It investigates the impact of transparency features together with different sorts of data sensitivity.

The results have theoretical implications, as this is the first work combining the effect of transparency features with data sensitivity. It will also help companies to gain a better understanding about the mechanism of the personalization privacy paradox and makes it possible to take actions to further improve their business.

2 Theoretical Background

For a good understanding of the personalization privacy paradox and the following work, it is important to introduce some of the main concepts. To achieve this, privacy, personalization, the personalization privacy paradox, transparency features, data sensitivity and the privacy calculus are explained.

2.1 Privacy

Privacy has been defined in different ways. It can for example be described as the “ability of the individual to control the terms under which personal information is acquired and used” (Westin, 1967). Others state that it is about users’ right to keep control over the decision which data is getting disclosed and which is not (Rognehaugh, 1999). They have in common that privacy occurs when individuals are able to decide which information is disclosed to which party. Additionally, those individuals must have the possibility to control the usage of the data which has been disclosed.

However, the privacy management of people and their decision making when to disclose data can be seen as complex process. Smith, Dinev, and Xu (2011) for example proposed the APCO model (Antecedents, Privacy Concerns, and Outcomes model). The goal of this study was to unite different avenues of research. However, additional research has shown that the APCO model has to be extended, for example by situational components like affect or the cognitive resources (Dinev, McConnell, & Smith, 2015). This was also supported by other literature, for example by Kehr et al. (2015). Those articles show that individuals’ privacy decisions are a complex process, which differs from situation to situation.

2.2 Personalization

Personalization can be found in many different contexts. This makes it important to have a consistent understanding of personalization in this work. The following list provides some definitions of the term personalization:

1. *“Personalization is the combined use of technology and customer information to tailor electronic commerce interactions between a business and each individual customer” (Personalization Consortium, 2003).*
2. *Personalization is the “ability to proactively tailor products to tastes of individual consumers based upon their personal and preference information” (Chellappa & Sin, 2005).*
3. *Personalization as “delivering to a group of individuals relevant information that is retrieved, transformed, and/or deduced from information sources” (Kim, 2002).*

Those definitions have three similarities:

1. Products or services are tailored
2. This tailoring is for specific individuals or groups
3. Customer information is used

Therefore, these three aspects can be seen as the core concept of personalization. Thus, personalization is occurring when all three points occur.

2.3 Personalization Privacy Paradox

The literature mainly provides two definitions of the personalization privacy paradox:

1. *“Consumers who value information transparency features are less willing to be profiled online for personalized service and advertising” (Awad & Krishnan, 2006).*
2. *The second definition describes the personalization privacy paradox as a tension between personalization benefits and privacy concerns, which arises in the context of personalization (Aguirre, Mahr, Grewal, Ruygter, & Wetzels, 2015; Chellappa & Sin, 2005; Sutanto et al., 2013; Xu et al., 2011).*

The paper of Awad and Krishnan (2006) were the first which specifically mentioned the term “personalization privacy paradox”. Their key notion was to question the use of transparency features in a personalized context. Some others are following this definition of Awad and Krishnan (2006) for the personalization privacy paradox (Karwatzki et al., 2017). The main difference between the two definitions is that the first has a narrower view. Awad and Krishnan (2006) concentrate on the so-

called privacy fundamentalists, who have high general privacy concerns, so that they are less willing to participate in personalized offerings. The transparency features have a paradoxical role in this definition, as those features are mainly implemented for those fundamentalists.

In contrast, the second definition, which is about the tension between personalization benefits and privacy concerns, has a broader understanding, considering not only transparency features and different privacy personalities, but also other impact factors. To gain a broader understanding in the context of personalization, the second definition is used in this work. This makes the tension between personalization benefits and privacy concerns the central part of the analysis. Privacy concerns in this context mean that individuals perceive high risk and lack of control over their information in a specific situation (Sutanto et al., 2013). Xu et al. (2011) and Hayes et al. (2021) directly measure perceived risks of information disclosure instead of privacy concerns. Therefore, the personalization privacy paradox is more about the tension between perceived risks and perceived benefits in their understanding. However, the meaning of both constructs, perceived risks and privacy concerns, in their papers are similar, measuring the negative aspects of data disclosure in a specific situation. This is why no hard line is drawn between privacy concerns and perceived risks in this work, considering both as synonyms.

2.4 Transparency Features

Research has shown that customers do not know a lot about the actual amount of collection and usage of their personal data (Treiblmaier & Pollach, 2007). To prevent this, transparency features can be introduced. This term can be explained as following:

“By information transparency features we mean features that give consumers access to the information a firm has collected about them, and how that information is going to be used” (Awad & Krishnan, 2006).

Therefore, transparency features inform individuals about the collection and the usage of their personal data.

Awad and Krishnan (2006) also state that transparency features have to be seen separated from privacy policies. According to them, transparency features make it possible for all consumers to understand the collection and use of the data, whereas privacy policies are a written statement, which are usually not read by customers.

2.5 Data Sensitivity

For the second part of this work, the quantitative analysis, it is important to understand the term data sensitivity. One commonly used definition is the following:

Data sensitivity is “the level of discomfort an individual perceives when disclosing that specific personal information to a specific Web site” (Li, Sarathy, & Xu, 2011).

This implies that data sensitivity is person-specific, as every individual can have a different level of discomfort, even when the same data is requested. Therefore, it is usual that the perceived sensitivity of individuals is measured. To deviate the objective sensitivity of a special sort of data, the average of several perceived sensitivity items are combined (Hui, Teo, & Lee, 2007). Based on this, it is possible to objectively evaluate which data is more or less sensitive for a majority of people.

2.6 Privacy Calculus

The Privacy Calculus was shown to have an important role in information privacy literature, including the personalization privacy paradox (Hayes et al., 2021; Xu et al., 2011). Culnan and Armstrong (1999) firstly argued that individuals' data disclosure process is based on a privacy calculus. Culnan and Bies (2003) further argued that the outcome of the information disclosure process is based on a risk-benefit trade-off. Following that, people are disclosing personal information if the benefits exceed the risks of disclosure. However, one criticism of this approach is that people are not acting after such a cognitive approach (Hayes et al., 2021). This is why more recent literature has paid attention to an extension of the privacy calculus, which includes more situational, affective and emotional factors (Dinev et al., 2015).

3 Method

To get an overview of the personalization privacy paradox literature, a structured literature review was carried out, which was presented by Webster and Watson (2002). To ensure high quality of the papers, the search was limited to the FT Research Rank 50, VHB-Jourqual ranking of “B” or better, and to the AIS Senior Scholars' Basket of Journals. To limit the results not only on information systems, those collections were not restricted to specific research areas. The process of the search can be clustered into four parts.

The first was to create the search string. This was done by the help of two research questions:

1. Which components are involved in the personalization privacy paradox?
2. Which different contexts are common and which role do they play in the personalization privacy paradox?

Therefore, the goal is to get a better understanding of the mechanisms of the personalization privacy paradox. This makes it necessary to set it into a broader context. As already described, the personalization privacy paradox can be defined in different ways. Based on this, it is important to search not only about the “personalization privacy paradox”, but more after personalization in a privacy context. This approach provides the advantage that a bigger variety of articles can be found, which include the trade-off between personalization benefits and privacy concerns. The following Figure shows the search string, which was used for the structured literature review:

Personalization	AND	Privacy OR Information OR Data OR Paradox
------------------------	-----	---

Figure 1: Search String of Structured Literature Review

All papers must contain the term “personalization” in their abstract, title or keyword section, as well as one of the words “privacy”, “information”, “data”, or “paradox”. The two words “Information” and “data” are added as a synonym of “privacy”, as privacy has a strong connection to information and data. “Paradox” was added to find all articles, which address a paradoxical situation in a personalization context. Additionally, some papers call the personalization privacy paradox only personalization paradox, without mentioning privacy (Aguirre et al., 2015). Therefore, searching for personalization paradox provides a wider selection of articles, which is not excluding important literature. The search string, together with the quality restrictions provided 336 articles.

In the second step, those 336 articles were screened to find the most relevant. To do so, only articles where the title has a privacy context were considered. This is necessary, as the search string does not prevent that the first part (personalization) comes independent from the second part (privacy, information, data, and paradox). Therefore, also articles were suggested, which do not contain content about personalization in the privacy context. However, this cannot be prevented by the search design, as the risk appears to exclude relevant articles otherwise. At the end of this step, 96 papers were selected.

In the third step, the abstract of the 96 articles were read. Only those articles were selected, which address the tension between personalization benefits and the privacy concerns, which is resulted by the personalization. At the end of this step, 19 papers were selected.

In the last step, a forward and backward search was conducted based on the previous found 19 papers. The same requirements were applied as described earlier. In the end, two additional articles were added to the list.

Therefore, 21 relevant articles were found in total to be relevant in the context of the personalization privacy paradox. The concept matrix, which is summarizing the most important findings of the papers, can be found in the appendix. Moreover, the outcome of the search is described in the following chapter.

4 Relevant Factors of the Personalization Privacy Paradox

The results of the structured literature review can be clustered into two parts. The first part contains the context, and the second one the inner working mechanism of the personalization privacy paradox. Even though the two parts are presented separately, they intercorrelate. This means, that for example the context can have an impact on the internal working mechanism of the personalization privacy paradox (Xu et al., 2011). However, this can also be seen in the next chapters.

4.1 Context

The context includes the boundary conditions, which surround the personalization privacy paradox. In other words, the context is same for all users, even though they might experience it differently. This includes the type of personalization, pull versus push based approaches, information security, the use of transparency features, the situations in which users are facing personalized offerings, personalization intensity, and the sensitivity of data which is used for personalization.

4.1.1 Types of Personalization

Personalization can be separated into the two main categories of service personalization and advertisement personalization. However, it must be mentioned that those types can be separated again into smaller categories. For example, advertisement personalization can be in the context of location-aware personalization, where the location of the customer is used for personalized advertising, or by a behavioral specific context, where the behavior of people triggers the tailoring of the advertisements

(Hayes et al., 2021; Unni & Harmon, 2007; Xu et al., 2011). However, as the focus of this work is not to develop a taxonomy to find all relevant types of personalization, this is not further discussed.

Service Personalization can be recognized when customers enjoy improved products and services, for example by a better preference match, a better communication, or a better experience for an individual (Vesänen, 2007).

In contrast, advertisement personalization can be defined as a “customer-oriented marketing strategy that aims to deliver the right content to the right person at the right time, to maximize immediate and future business opportunities” (Aguirre et al., 2015; Tam & Ho, 2006).

The line between these definitions, however, can get blurred. For example, in a social media context, a better advertisement personalization can lead to a better experience, as the content of the ads matches the preferences of the customers. Therefore, people can also perceive the value of the service higher (Cloarec, Meyer - Waarden, & Munzel, 2022).

Both personalization types are discussed in the literature regarding the personalization privacy paradox. However, only little research was done comparing both types in this context. Awad and Krishnan (2006) indicate that customers value personalization for services higher than for advertisements. By having an impact on the perceived value for users, the differentiation into the types of personalization can make a difference in the personalization privacy paradox. This can be seen, as different constructs have unequal outcomes when a different type of personalization is used. For example, previous privacy invasions are significant and have a negative impact on the advertisement personalization group, but are insignificant in the service personalization group (Awad & Krishnan, 2006). Therefore, different types of personalization can make a difference in the personalization privacy paradox.

4.1.2 Pull versus Push based Personalization

The differentiation of pulled and pushed personalization features can mainly be found in the location-based advertising literature. Location-based advertising is a form of marketing that uses location tracking technology to be able to provide personalized adverts to users, based on their location (Unni & Harmon, 2007). Pull and push based personalization can be distinguished as following:

- **Pull based**: Personalization is only delivered when the user explicitly request for it (Unni & Harmon, 2007). In literature, this is also called the overt based approach (Xu et al., 2011).
- **Push based**: Personalization is delivered even though the user did not request it in that specific moment. Therefore, the provider automatically personalizes the content for the customer (Unni & Harmon, 2007). This can also be called the covert based approach, as the personalization process is taking place covertly (Xu et al., 2011).

Literature has shown that differences occur when either of the two approaches is used. This also has a direct impact on the personalization privacy paradox. Xu et al. (2011) found out that the push (covert) based approach comes with higher benefits compared to the pull (overt) based variant. However, both are increasing the benefits for the users significantly, compared to no personalization. In contrast, Unni and Harmon (2007) measured that perceived benefits and perceived value are higher in a pull (overt) based context. Unni and Harmon (2007) also state that the effect of the personalization on the benefits is dependent on the quality of the suggestions done by personalization. Similar findings were shown by Aguirre et al. (2015). They measured that an overt data collection signals benevolence and trust, which has a positive impact on the acceptance of the personalization. Hayes et al. (2021) measured neither that a pull, nor a push approach has higher perceived benefits compared to the other variant.

Xu et al. (2011) have also shown in their study that their location-based advertising results in more spontaneous buyers when a push (covert) approach is used, while the pull (overt) variant encourages planned purchases.

Those approaches can also have an impact on the perceived risks or privacy concerns. According to Unni and Harmon (2007), perceived privacy concerns were greater in the push based approach, compared to the pull based. This goes in line with the findings of Aguirre et al. (2015), Hayes et al. (2021) and Xu et al. (2011), where the push (covert) based approach comes with higher perceived risks. Aguirre et al. (2015) showed that the covert data collection comes with a higher perceived vulnerability and loss of control, compared to the overt approach. This happens, because people have the feeling that data is collected secretly and without their explicit consent in the covert approach. In the measurement of Xu et al. (2011), within the pull (overt) based approach, the impact of personalization on the perceived risks was not only smaller, but not significant, indicating that personalization does not provide a higher risk perception in this context. In other words, this means that perceived risks do not increase, while advantages through personalization still occur. Therefore, this can be one option to avoid the personalization privacy paradox for providers.

However, the use of pull (overt) based personalization can overcome the personalization privacy paradox but can also limit the capabilities of personalization benefits. Even though the effect on perceived benefits is not clear in literature, the effects on perceived risks are consistent. Therefore, when providers use the push (covert) based approach, they should manage the arising privacy concerns (Xu et al., 2011).

4.1.3 Information Security

Sutanto et al. (2013) showed in their article that information security, which is implemented by technical design, is able to overcome the personalization privacy paradox. They built a personalized privacy-safe application, where data about the individuals is stored locally on the device and is not transferred to third parties. They compared this application with one that provides the same features but transfers personal data to their advertisement partners. In the privacy-safe version, the users were informed that personal information is only stored on the device, so that the personalization takes place without transfer of personal information beyond the own mobile phone.

In the privacy-safe environment, people had less privacy concerns compared to the non-privacy-safe environment. Additionally, the benefits of the personalization are perceived to be stronger. This resulted in a higher usage rate and a higher encouragement of data disclosure.

Xu, Li, and Yao (2022) also investigated the need of security investments when data is disclosed in return for personalization. They state that for some people, who switch between personalization benefits and privacy concerns, information security is essential, as privacy concerns can be reduced. To integrate those people into the personalization procedure, it is necessary to invest and communicate the information security to them in advance. If the company is not proactive in this case, it is likely that firms and consumer fall into a prisoner's dilemma, where people who value security are not participating in the personalization offering, while the company sees no need to invest, as their customers do not perceive a high value for those security investments. In contrast, providing information security can lead to a win-win situation for the company and the users. The users have less privacy concerns and can enjoy the benefits of personalization, while companies can attract more users for their personalized service.

Those examples show that information security can have a significant impact within the personalization privacy paradox, as it is able to mitigate privacy concerns.

4.1.4 Transparency Features

Awad and Krishnan (2006) made transparency features to one of the most central constructs in the personalization privacy paradox. Their outcome is that transparency features are mainly valued by people who are less willing to be profiled in general. This means, transparency features are implemented for people who are less willing to participate in personalized offerings. Therefore, they claimed that providers should not invest in transparency features but concentrate on personalization benefits.

Similar claims, to not use transparency features, were provided by Karwatzki et al. (2017). They separated two groups, one which values data privacy higher, and one with people who have a lower data privacy valuation. The outcome was that transparency features have no impact on the intentional

willingness to disclose information for personalization, regardless how important data privacy is for people. Moreover, the two groups did not value transparency features significantly different. This contradicts with the outcomes, provided by Awad and Krishnan (2006), that transparency features are only valued by some user segments, which have a high value for privacy. Karwatzki et al. (2017) emphasize that transparency features function as a signal of fairness, which is opposed by privacy concerns. Those privacy concerns are raised, as transparency features awake awareness for privacy thoughts in individuals' minds. The fairness and the privacy concerns end up in a balanced trade-off, so that transparency features have neither a negative, nor a positive impact.

In contrast, Bleier and Eisenbeiss (2015) showed that transparency can be essential when personalization is high. Click-through rates of banner advertisement were decreasing when personalization strength exceeded one point. To counteract this, companies which provide strong personalization features can inform customers about the collection and use of the data processed for personalization.

4.1.5 Situation

Sheng, Nah, and Siau (2008) showed in their experimental study that one aspect impacting the personalization privacy paradox is the context. In other words, the existence of the personalization privacy paradox is varying from situation to situation. To show that, they introduced two different situations: one emergency and one non-emergency. In the emergency, customers are confronted with incidents, which causes significant negative effects for them. When personalization is offered, they showed that privacy concerns are greater in a non-emergency context. Additionally, the adoption rate indicates that people are more willing to use personalized services in an emergency situation. In contrast, confronting people with a non-emergency situation, privacy concerns increased, and intentional usage of the service declined due to the personalization. Therefore, this shows the occurrence of the personalization privacy paradox, as personalization results in a lower rate of usage, compared with no personalization. Additionally, it shows that in a non-emergency context, people prefer the non-personalized option over the personalized. Therefore, situational factors like context can drive the personalization privacy paradox.

4.1.6 Personalization Intensity

In many papers, personalization intensity is not measured, as one personalization strength is provided as boundary condition (Awad & Krishnan, 2006; Chellappa & Sin, 2005; Li & Unger, 2012). However, Xu et al. (2011), as well as Hayes et al. (2021), used a perceived personalization scale, thus measuring how intense personalization is perceived from a customer's point of view. They found out that the higher personalization is perceived for individuals, the higher the benefits are evaluated. The impact of the height of personalization on the perceived risks were dependent on the personalization

type: overt or covert. Xu et al. (2011) measured that the higher the personalization perception, the higher the perceived risks. In contrast, providing the personalization overtly, with a pull based approach, this effect could be mitigated. However, these measurements provided the same personalization settings, thus different steps between personalization strengths can hardly be interpreted.

Aguirre et al. (2015) also investigated overt versus covert approaches and distinguished between two different personalization strength groups. They found out that people feel more vulnerable when personalization intensity is high and personalization is provided covertly. In contrast, by offering the personalization overtly (pull based), this increased vulnerability can be overcome.

Karwatzki et al. (2017) also differentiated between two different personalization strength groups. They showed that the effect of personalization strength depends on the individual valuation of privacy of the users. This means, people who value privacy less, disclosed more data for personalization when personalization was high. In contrast, for people with a high privacy valuation, the strength of personalization did not significantly change the willingness to disclose data for personalization.

In contrast, Bleier and Eisenbeiss (2015) distinguished two different personalization strengths. The first is personalization depth, which describes how close the advertisements target consumers' preferences. This is also the primary dimension of personalization and usually the only one measured in the context of personalization strength. The second is personalization breadth, which is how complete the interests of an individual are targeted by advertisement. They show that in some combinations, depth and breadth personalization can lead to a higher usefulness, but can also cause negative effects like privacy concerns. For example, when a retailer is trustworthy, and offers high depth personalization, narrow breadth personalization leads to a higher perceived usefulness, compared to a wider breadth personalization. However, this only holds to a certain extent, as when depth personalization increases beyond one point, consumers experience privacy concerns. For less trusted retailers, this point is already reached earlier, as in addition to the lower perceived usefulness, higher privacy concerns are occurring when high depth personalization is offered.

This shows that personalization strength can have an impact on the personalization privacy paradox, as benefits, as well as privacy concerns, are affected. However, literature has shown that this effect is dependent on different variables, like the trustworthiness of retailer or if personalization is offered covertly or overtly (Aguirre et al., 2015; Bleier & Eisenbeiss, 2015; Hayes et al., 2021; Karwatzki et al., 2017; Xu et al., 2011).

4.1.7 Sensitivity of Data

Little research was done in the combination of data sensitivity and the personalization privacy paradox. One study, investigating the role of perceived sensitivity in this context, was conducted by Sutanto et al. (2013). Thus, not the objective sensitivity of data was measured, but the individually perceived sensitivity of data of every person. Perceived sensitivity had a significant and negative impact on the willingness to share data for personalization. As a result, higher perceived sensitivity is increasing the privacy concerns for customers.

Hayes et al. (2021) argued that customers perceive the data which they disclose as less sensitive when marketers are perceived as more trustworthy. Therefore, the reduced perception of data sensitivity had a positive impact on the willingness to have the information used for personalization. However, this argument was not proofed by measurement, but derived from Markos, Milne, and Peltier's (2017) outcomes, which was not in the context of the personalization privacy paradox.

Zhu, Ou, van den Heuvel, and Liu (2017) connected the sensitivity of data with the different privacy personalities. They argue that data sensitivity should be collected dependent on the different personality characters. In other words, highly sensitive data will have a negative effect regarding data disclosure rate and participation when privacy fundamentalists are the customer base, while this negative effect will have less impact for unconcerned users.

4.2 Inner Working Mechanism of the Personalization Privacy Paradox

The second part deals with the inner working mechanism of the personalization privacy paradox. This part should explain how the personalization privacy paradox is working and how people weight the different aspects in their decision-making process.

4.2.1 Impact of Personalization on the Benefits versus Privacy Concerns Trade-off

The personalization privacy paradox was defined as a tension between personalization benefits and privacy concerns (Chellappa & Sin, 2005; Sheng et al., 2008; Sutanto et al., 2013; Xu et al., 2011). This shows the central role of personalization benefits and privacy concerns in the personalization privacy paradox. As described earlier, definitions of privacy concerns and perceived privacy risks can be quite similar. Thus, both constructs are considered to be synonyms in this work.

To start with the benefits, personalization can enhance the utility and therefore comes with benefits for customers. For example, personalized services can reduce information overload and cognitive efforts for users by targeting the needs and interests of them (Karwatzki et al., 2017; Lowry, Cao, & Everard, 2011). This goes in line with other research, which shows that personalization increases the benefits for users (Hayes et al., 2021; Sutanto et al., 2013; Xu et al., 2011; Zhao, Lu, & Gupta, 2012). However, the perception of benefits is dependent on different other factors. As already described, the use of push or pull based personalization is one of these factors, as push based personalization brings higher perceived benefits (Xu et al., 2011). Additionally, Awad and Krishnan (2006) found differences in service and advertisement personalization. They showed that service personalization comes with higher benefits for customers. Therefore, the type of personalization is also involved in the benefit assessment.

On the other side, personalization comes with the collecting and using of personal data. This can create privacy concerns for users (Awad & Krishnan, 2006; Sheng et al., 2008; Xu et al., 2011; Zhao et al., 2012). The privacy concerns or perceived privacy risks are also dependent on other factors. It has for example be shown that eliminating privacy risks, which are created by personalization, is possible. This was the outcome of Xu et al. (2011) and also Hayes et al. (2021), when pull based personalization approach is used. Sutanto et al. (2013) also showed that using privacy safe technologies can reduce individuals' privacy concerns. In contrast, Albashrawi and Motiwalla (2019) presented that people do not link their privacy concerns to the ease of use they experience due to personalization. In other words, this result questions the direct connection of personalization and the perception of risks.

However, considering perceived benefits and risks also has its criticism. For example, Karwatzki et al. (2017) used the information boundary theory, with the argumentation that benefits and risks correlate from the beginning and cannot be seen independently. One way to integrate that into the privacy calculus is to add the construct perceived value. This is a trade-off of perceived benefits and perceived risks and describes the value individuals perceive from specific data disclosures (Xu et al., 2011). Chellappa and Sin (2005), for example, suggest that consumers are willing to use personalization services when this trade-off is positive, while they are not doing so when the trade-off is negative. Therefore, personalization is used when the value of personalization is positive.

Hayes et al. (2021), as well as Xu et al. (2011), showed that personalization increases the value for users and encourages them to disclose more data for personalization. This is the case, even though privacy concerns are created. This is possible, when the benefits exceed the concerns, created by personalization. Karwatzki et al. (2017) showed that people are willing to trade their personal information against benefits, as they perceive positive value from this data disclosure. This, however, only holds for people who have a low valuation for privacy. People for whom privacy is important in

general, the evaluation of risks exceeds the benefits, so that personalization is valued less. Similar outcomes are presented by Awad and Krishnan (2006) who argue that personalization can override privacy concerns so that users have a positive perception of the personalization, while people who value privacy are more likely to refuse the use of personalized services.

Therefore, literature has shown that personalization can add value to individuals. This is possible when the benefits exceed the privacy concerns people get due to personalization (Awad & Krishnan, 2006; Karwatzki et al., 2017). One exception was found when people have a high privacy valuation. In this context, the privacy concerns of personalization were able to exceed the perceived benefits (Karwatzki et al., 2017).

4.2.2 Different Privacy Personalities

Awad and Krishnan (2006) described in their definition of the personalization privacy paradox that people who value transparency features are less willing to get profiled online. They specifically describe those people as privacy fundamentalists, who are very concerned about their information use. Therefore, Awad and Krishnan (2006) stated that different people are existent, who see privacy issues more or less important. Additionally, some are more concerned than others, which makes this aspect relevant in the context of the personalization privacy paradox.

Karwatzki et al. (2017) measured the disposition to value privacy disclosure (DTVP). Their result is that people with a low DTVP, who are people who do not value privacy that much, disclose more data in a personalized context than those with a high DTVP. Personalization mainly had an impact on the low DTVP group, while personalization did not influence the data disclosure of the high DTVP group significantly. In other words, people who indicated to have a low privacy evaluation, were more willing to trade their data in return for personalization benefits.

Xu et al. (2022) directly focused on the privacy group, which switches between information disclosure and non-disclosure. Those are people with a medium level of privacy concerns, the so-called privacy pragmatists. They argue that this group is especially relevant in the context of the personalization privacy paradox, as they alter between the personalization benefits and privacy concerns. They also mention two other groups, which do not have a high relevance in the personalization privacy paradox. The first are the conservatists, that are highly concerned about privacy, so that they are not disclosing data, also not in return for personalization benefits. The second are the unconcerned, who focus more on the benefits and do not have a high value for privacy, so that they are not concerned about the data disclosure which is necessary for the personalization (Westin, 2003). Xu et al. (2022) deducted that the pragmatists can be convinced by providers to disclose data for personalization, for example by providing high information security standards. Moreover, they emphasize the need for every personalization provider to know which customer group is targeted.

Pragmatists, for example, need another level of information security than unconcerned, which should affect the personalization provider's decision making. These findings go in line with those of Zhu et al. (2017). They also used three customer segments, which are pragmatists, unconcerned, and fundamentalists. In this study, fundamentalists are equal to privacy conservatists. Their conclusion is that every group has different requests. For example, unconcerned people do not mind that much about privacy, but value a high degree of personalization. Therefore, a high extent of personalization benefits is more efficient in this privacy group than mitigating privacy concerns. In contrast, for people who have a strong valuation for privacy, companies should offer standardized products, which do not need personal data for personalization. Moreover, and in line with the outcomes of Xu et al. (2022) and Zhu et al. (2017), it can be essential for pragmatists that personalization provider care about their privacy concerns, as the balance between those and the benefits of the personalization decide whether they are willing to use the personalized service or not.

Lee, Ahn, and Bang (2011) argue with a game theoretical approach that these different personalities can be targeted with different personalization settings. This does not only have advantages for the customers, but also for the companies, as competition can be prevented. Customers benefit, as they can choose privacy settings which are closer to their desires. In contrast, for companies this can be one opportunity to overcome privacy concerns, especially those which vary from person to person. As a result, personalization providers are able to include a larger customer base, also preventing that another provider can start a similar service, by serving those more privacy sensitive customer.

To sum up, literature agrees that the perception of different people about privacy is a very important aspect in the personalization privacy paradox. Some people enjoy only the benefits of personalization, others concentrate on the privacy concerns (Karwatzki et al., 2017). Thus, this plays an important role in the evaluation of the tension between privacy concerns and personalization benefits.

4.2.3 Happiness

Happiness can be seen as a long lasting, powerful, and positive emotion (Ong, Chang, & Lee, 2015). Cloarec et al. (2022) investigated the role of happiness in the context of the personalization privacy paradox. They found out that happiness is one of the most important drivers for the willingness to provide personal information in return for personalization. When people are happier, they use less cognitive resources and focus more on heuristics, which concentrate on the benefits, while subordinating the negative aspects (Cloarec et al., 2022; Dinev et al., 2015). Therefore, Cloarec et al. (2022) claim that firms should provide more benefits than costs for users, but mainly should ensure that customers are happy with the service and the personalization. This is, as people will ignore their privacy concerns when they are in a happy mood. Additionally, this shows that the personalization privacy paradox must also consider situational and affective constructs like happiness, as people are not always using cognitive approaches for their personal data disclosing process.

4.2.4 Trust

Consumers' trust to personalization providers has been shown to play a relevant role in the personalization privacy paradox. This can be seen as higher trust, or using trust building features, increases the likelihood of using personalized features (Aguirre et al., 2015; Bleier & Eisenbeiss, 2015; Chellappa & Sin, 2005; Cloarec et al., 2022; Hayes et al., 2021; Kobsa, 2007). This is, as trust intercorrelates negatively with privacy concerns. This makes trust one factor, which can mitigate privacy concerns for customers when offering personalization (Chellappa & Sin, 2005). However, companies face themselves in a paradoxical situation, as trust can not only mitigate those privacy concerns, but privacy concerns themselves, for example due to data collection, can lower trust. Therefore, trust and privacy concerns have a double-sided relationship (Chellappa & Sin, 2005; Cloarec et al., 2022; Kobsa, 2007).

Besides the mitigation of the negative aspects, trust also has a positive impact on the data disclosure and use of personalized services. Cloarec et al. (2022) for example, have shown that trust has a positive impact on the happiness of using a service, which further increases the willingness to disclose data for personalization.

Bleier and Eisenbeiss (2015) also investigated the effect of trust on the perceived usefulness. Their results indicate that when personalization is high, people perceive personalized banner advertisement more useful with a trusted marketer, compared to a less trusted one. Therefore, trust can shape the perception of individuals in the context of usefulness. This goes in line with the findings of Hayes et al. (2021). In their study, trust increases the perceived value for consumers by perceiving stronger benefits. Bleier and Eisenbeiss (2015) additionally showed the importance of trust on the click-through rates. When personalization is high, trusted brands had higher click-through rates, while less trusted had less. Thus, the less trusted group is a perfect example for the occurrence of the personalization privacy paradox, as personalization decreases the performance of the advertisement. This finding also means that the paradox can be mitigated by trust. However, they additionally state that even high trusted companies like Amazon should communicate transparency about their data collection, the data usage, and the presence of privacy settings, when extremely high personalization is offered. Aguirre et al. (2015) presented complementary findings. They showed that when companies inform customers about the personalization, the data collection, and the usage of those data increases trust. Thus, they argue that one of the main advantages to use pull based (overt) personalization is that it is increasing trust.

Another view of trust is in combination with data sensitivity. Chellappa and Sin (2005) showed that trust building factors are also important in non-financial transactions, which are less sensitive. Thus, they assume that trust is important for less sensitive contexts as well.

To sum up, trust has shown to play an active role in the personalization privacy paradox (Chellappa & Sin, 2005) and can increase customers' willingness to disclose data for personalization (Bleier & Eisenbeiss, 2015; Cloarec et al., 2022). Therefore, one option to mitigate the personalization privacy paradox is to balance the amount of personalization with the amount of trust a provider receives from their customers. Thus, building trust is one option to ensure a positive effect of the personalization. In contrast, this also means that new, unknown companies should be careful with providing personalized services and advertisements (Bleier & Eisenbeiss, 2015).

5 Quantitative Experiment

The literature review provided an overlook over the existing impact factors of the personalization privacy paradox. To further add value to research, this work offers an own quantitative analysis to gain a better understanding of the paradox in areas where literature is not united or lacks research.

5.1 Goal of Experiment

The role of transparency features in the personalization privacy paradox remains unexplained. Awad and Krishnan (2006) stated that transparency features only have a positive impact for people who are not likely to participate in personalization anyway, which makes transparency features unnecessary. The findings from Karwatzki et al. (2017) go one step further, finding no significant positive impact for all people, regardless to which privacy group they belong. In contrast, Bleier and Eisenbeiss (2015), for example, showed in their experiment that transparency features can be essential when personalization is high.

This shows that the question about the impact of transparency features cannot be answered across different studies. This indicates that the effect of transparency features is dependent on the context in which they are occurring. For example, Sutanto et al. (2013) showed that transparency can have a positive impact when companies offer privacy safe applications. Therefore, there might be situations in which transparency has a positive impact, while it has no impact in others.

Moreover, Cloarec et al. (2022) called to investigate the impact of data sensitivity, as little research was done in combination with the personalization privacy paradox. This was also shown in the literature review of this work.

Thus, the research question for the quantitative experiment in this work can be described as following:

“Which role has the sensitivity of data on the impact of transparency features
in the personalization privacy paradox”

The combination of transparency features and data sensitivity has also the advantage that the sensitivity of the data can be communicated. This makes it easier to investigate data sensitivity in the context of the personalization privacy paradox, as people are directly confronted with the sensitivity of data. Therefore, this enables to observe more precisely how people react on different data sensitivity.

5.2 Hypothesis Development

To investigate the impact of data sensitivity and transparency features in the experiment, different hypothesis are deviated from prior literature.

5.2.1 The Privacy Calculus

The privacy calculus has shown to be a good framework to explain and analyze the personalization privacy paradox (Chellappa & Sin, 2005; Cloarec, 2020; Hayes et al., 2021; Kobsa, 2007; Xu et al., 2011; Xu, Teo, Tan, & Agarwal, 2009). Therefore, this framework is suitable for this experiment as well.

The privacy calculus model also determines the first hypotheses. Xu et al. (2009), Xu et al. (2011), and Hayes et al. (2021) showed that perceived risks of information disclosure and perceived benefits of information disclosure result in the willingness to disclose data for personalization. However, perceived value is not considered in this thesis, as this aims the goal to show that the privacy calculus mechanism is working, which has been shown several times (Hayes et al., 2021; Xu et al., 2011). It is expected that perceived benefits have a positive impact on the information disclosure, while the perceived risks have a negative impact. Therefore, the first two hypotheses are:

H1: Perceived benefits of information disclosure have a positive impact
on the willingness to disclose data for personalization.

H2: Perceived risks of information disclosure have a negative impact on
the willingness to disclose data for personalization.

5.2.2 Transparency Features and Data Sensitivity

Literature has shown that transparency features have two facets. On the one side, they can be seen as a signal of fairness, opposing privacy concerns, and reducing the perceived risks of individuals. This is at least the case for some individuals and in specific situations, for example when high personalization is present (Awad & Krishnan, 2006; Bleier & Eisenbeiss, 2015; Karwatzki et al., 2017). On the other side, Karwatzki et al. (2017) claimed that transparency features increase the awareness of data collection. This means individuals using the personalized services are informed about the types of data that are collected and how they are used. This awareness then creates privacy concerns and increases the perceived risks. Therefore, transparency features can have two opposite effects.

One possible explanation is that the effect is dependent on contextual factors. For example, one way to explain the findings of Bleier and Eisenbeiss (2015) is that people value transparency features in a highly personalized context, as they expect the degree of data collection as worse than it actually is. Thus, users will perceive the data collection as fair. In contrast, without transparency features, users would expect a certain amount of data collection, which may not be perceived as fair.

To test this hypothesis, data sensitivity is used as one situational factor, on which the effect of transparency features can be dependent. Therefore, it is expected that with high data sensitivity, transparency features have a weaker positive, or even negative effect on the willingness to disclose data for personalization. In contrast, when fewer sensitive data is collected for the same personalization, people perceive this as fair, and are more willing to disclose data for personalization. To embed this into the privacy calculus model, transparency features are generally expected to have a negative effect on perceived risks, as people are perceiving the personalization as fair and are less concerned. However, this relationship is negatively moderated by data sensitivity, which makes it possible that the risk mitigating effect of transparency features disappears. Moreover, this effect can change the direction, making transparency features enhancing the risks. Therefore, hypothesis three and four are as following:

H3: The usage of transparency features has a negative impact on the perceived risks of information disclosure.

H4: Data sensitivity negatively moderates the effect of transparency features on perceived risks of information disclosure.

The effect of transparency features on perceived benefits lacks research. However, following the argument of Karwatzki et al. (2017) about the awareness of data collection, transparency features can also shape the awareness of the positive effects of personalization. Transparency features can for

example highlight all the advantages, people have due to the personalization. Therefore, it is expected that transparency features have a positive impact on the perceived benefits of information disclosure. This is tested with hypothesis five:

H5: The usage of transparency features has a positive impact on the perceived benefits of information disclosure.

5.2.3 Trust

It has been shown that trust has a positive impact on the users' willingness to disclose personal information for personalization (Aguirre et al., 2015; Bleier & Eisenbeiss, 2015; Chellappa & Sin, 2005; Cloarec et al., 2022; Hayes et al., 2021; Kobsa, 2007). By using the privacy calculus, it is expected that the increased disclosure is reached over the two constructs perceived risks and perceived benefits. Therefore, it is suggested that trust has no direct impact on the willingness to disclose personal data, but works over the privacy calculus (Kehr et al., 2015).

Chellappa and Sin (2005) showed that trust building factors have a negative relationship with concerns for privacy. Thus, trust can have a negative impact on privacy concerns, also decreasing perceived risks, as hypothesis six states:

H6: Trust has a negative impact on the perceived risks of information disclosure.

Moreover, trust can increase the perceived usefulness (Bleier & Eisenbeiss, 2015). Also in other privacy literature, which is not directly connected to the personalization privacy paradox, trust has shown to have a positive impact on the perceived benefits (Kehr et al., 2015). As an increased usefulness is closely connected to an increase of perceived benefits, the next hypothesis is as following:

H7: Trust has a positive impact on the perceived benefits of information disclosure.

Therefore, the hypotheses suggest that trust impacts the data disclosure for personalization on both ways in the privacy calculus: by mitigating perceived risks and by increasing the perceived benefits.

Another aspect, which makes trust highly relevant in this experiment, is the impact of transparency features on trust. Aguirre et al. (2015), as well as Bleier and Eisenbeiss (2015), argued that providing transparency can increase users' trust, as customers value that the provider is proactively

communicating the privacy issues. Therefore, it is expected that the use of transparency features increases the trust of customers. Therefore, the eighth and last hypothesis is as following:

H8: Transparency features have a positive impact on trust.

5.2.4 Model Presentation

The used constructs and expected hypotheses result in a model, which is visually presented in the following.

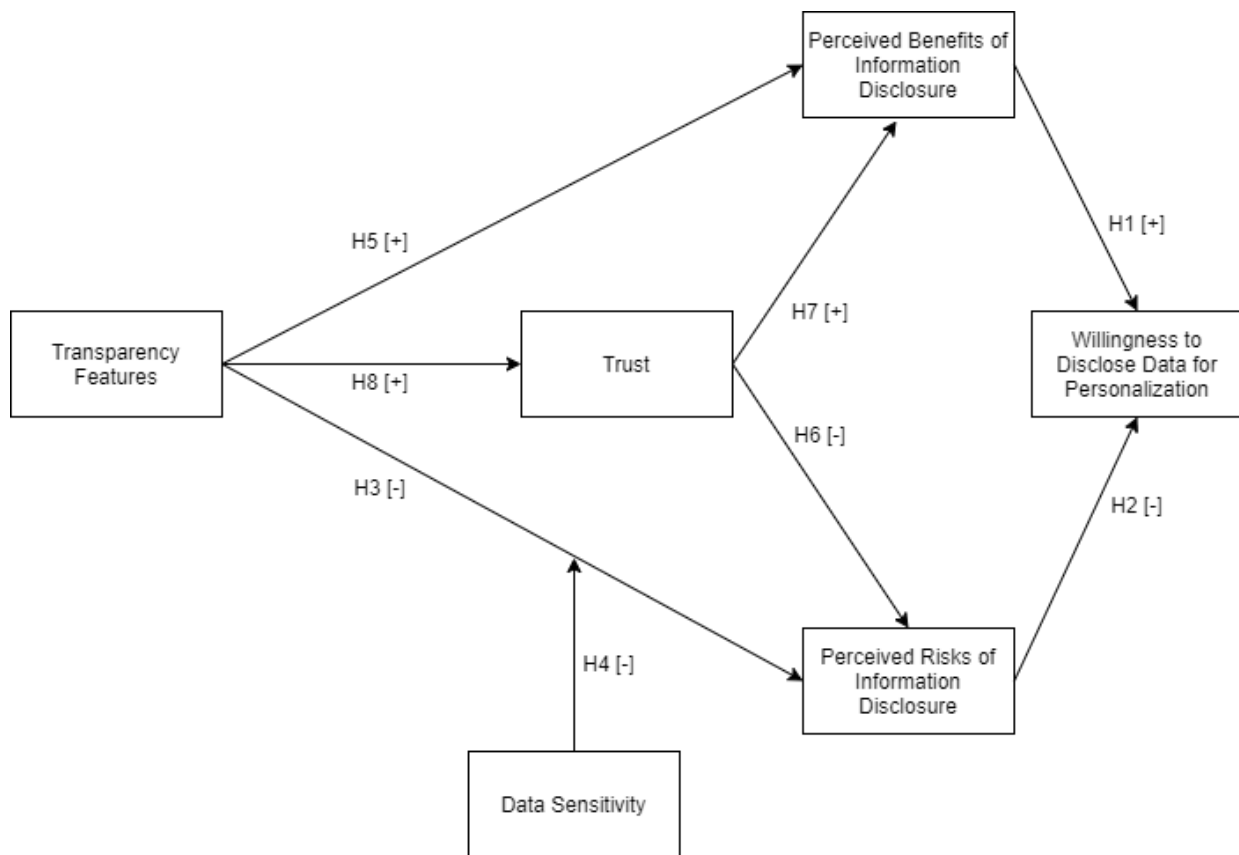


Figure 2: Hypothesis Model

5.3 Survey Context

To measure the different effects within the personalization privacy paradox, a survey was conducted. Therefore, it is not possible to measure real behavior, but only intentional behavior. The survey is in the context of service personalization. Literature has shown that people generally value this type more than advertisement personalization (Awad & Krishnan, 2006). Therefore, it is more likely that people

do not decline to use the personalization at all, but decide dependent on the situation. As the executing provider of the personalization an online pharmacy is chosen. This has several advantages.

First, it is expected that sensitivity manipulation is successful in the context, as people perceive their medical data as sensitive (Hui et al., 2007). This makes it more likely that users care about their privacy and are more conscious about it. Following that, it is expected that users apply more cognitive decision making than in a less sensitive environment.

Second, online pharmacies in Germany are not as commonly used as other online shops. For example, in 2020, all online pharmacies in the top ten reached together a revenue of 2.2 billion euros, whereas Amazon alone generated 29.5 billion dollars (about 28.9 billion euros) in Germany (Boersenblatt, 2021; Brandt, 2021). The advantage to take less used online services is that participants of the survey are less likely associating the online pharmacy with a known, really existing one. This reduces affective effects and already pre-existing biases like different trust perceptions. This is also the reason why no pictures are included in the survey. Therefore, the survey concentrates as much as possible on the cognitive decision-making process of the individuals.

5.4 Survey Procedure

The participants received a hyperlink of the survey provider Unipark to participate. Participation is voluntary and not compensated financially or in any other way. The survey is available in English and German, thus speaking one of the languages fluent is required. The participants were able to choose the language in the beginning. Important to note is that at no time people were informed that the survey investigates their behavior in a privacy context.

After a short introduction about the procedure of the survey, a short explanation of a situation is introduced to the participants:

Imagine, you are in the following situation:

You want to buy something from an online pharmacy. The products you can buy are similar to those available in normal offline pharmacies. However, the difference is that the online pharmacy has a much wider variety of products. This has the advantage that any product needed can be found. In contrast, it takes a lot of time to search and find the right product. Additionally, as a customer, you are more uncertain about which product is the best for you.

In the next step, people were randomly allocated into one of the three different groups. The groups are designed to have the same sample size, as the participants are evenly distributed. The first group gets the following information:

During the usage of the online pharmacy website, you recognize that your search results are personalized. They suggest you some products you may be interested in. Additionally, some products are displayed more likely when you search for something on the website. However, the online pharmacy does not explain anything about the personalization.

Therefore, the first group is without transparency features and without any information about data sensitivity. The main information they receive is that the online pharmacy is personalizing the search results. This sample size is seen as the reference group and shows how people expect the sensitivity of information to be when they have no knowledge about that. This comes close to reality when no transparency features are implemented, as people are hardly reading any privacy policies (Awad & Krishnan, 2006). Therefore, note that to this group, no transparency features are provided.

The second and third group have in common that information sensitivity is manipulated by giving the participants different information about which data is collected about them to personalize the web shop of the pharmacy. The second group is getting the following information:

The online pharmacy informs you that your search will be personalized. For that, the following data will be used for personalization purposes only:

- *Gender*
- *Age*
- *Country of residence*

It is expected that the participants experience little perceived sensitivity in this group, as gender, age, and country of residence were found to create low sensitivity feelings in prior literature (Hui et al., 2007; Xie, Teo, & Wan, 2006). In the third group, the same message is displayed, with the difference of the collected data. There, the exact GPS location of the participants, the household income, and the medical history is used for personalization. Those data was found to be perceived as highly sensitive in prior literature (Ackerman, Cranor, & Reagle, 1999; Hui et al., 2007; Kehr et al., 2015). It can also be seen that the number of data is fixed to three different sorts at both groups. It is important to fully concentrate on the effect of data sensitivity and not on additional factors like amount of data collected (Xu et al., 2022). Additionally, no information about the quality of personalization is provided. This is

important to ensure that people perceive the quality of personalization similar across groups (Li & Unger, 2012).

Moreover, the participants do not only get the information about which data is used for personalization, but also how it is used, as this is one additional part of providing transparency features (Awad & Krishnan, 2006). For that, people in the groups two and three are getting displayed the same information in the survey:

Additionally, you get the following information from the online pharmacy:

- *All data can be deleted, whenever you request that.*
- *The personalization enables you a faster shopping experience: Due to the recommendations of our search, you find products faster, which saves unnecessary search time for you.*
- *The personalization allows you to find the best fitting from the large number of products. Therefore, it will not be necessary to try many different products to get the wanted effect.*
- *The data is not shared to other parties and is only used for personalization of the online shop.*

The first and the last bullet point are formulated to give the participants a privacy assurance. The goal is to reduce the negative aspects of the data disclosure and to ensure users that the data will not be used in a bad way. Therefore, the goal is punishment avoidance (Zeng, Ye, Yang, Li, & Song, 2019). In contrast, the second and third point informs about the positive aspects of the personalization. The effect of both variants has been discussed in literature (Hui et al., 2007; Zeng et al., 2019). To neither focus on benefits only, nor on punishment avoidance, a combination of both is chosen. Additionally, they are weighted with the same number of bullet points (two each). This ensures that the formulation of the transparency features has smaller impact and is more general.

After the participants received different, group-specific information about the data collection and the use of data, all received the same questions. The items for those questions are adopted from prior literature. However, small adjustments must be done at some points to make the questions suitable for the context. For all constructs, seven-point Likert scales are used.

First, the willingness to disclose data for personalization is asked. The construct is copied from Culnan and Armstrong (1999) and Hayes et al. (2021). Asking this in the beginning has the advantage that the people are not aware that the survey is about privacy, which makes it more likely that they are answering more honest. At the second position, the perceived sensitivity is measured to control if the

manipulation was successful. There, a one item construct is used, copied from Hui et al. (2007) and Xie et al. (2006). After that, the two main components of the privacy calculus are measured. Those are the perceived risks of information disclosure (Xu et al., 2011) and perceived benefits of information disclosure (Hayes et al., 2021; Unni & Harmon, 2007; Xu et al., 2011). Last, trust (Jarvenpaa, Tractinsky, & Saarinen, 1999; Malhotra, Kim, & Agarwal, 2004) and general privacy concerns are asked. General privacy concerns are integrated in the survey, even though it is not part of the hypothesis model, as different privacy personalities were found to be one of the main drivers of the personalization privacy paradox. Therefore, it is added to control if the participants of all groups have a similar attitude towards privacy in general. The scale of general privacy concerns is taken from Martin, Borah, and Palmatier (2017), which was initially developed by Malhotra et al. (2004), but developed at some points. The following table gives an overview of the used constructs and the questions asked in the survey:

Construct	Questions	Source	Scale (all seven-point Likert)
Willingness to disclose data for personalization	How interested would you be in having your personal information used from the pharmacy for personalization?	Culnan and Armstrong (1999) and Hayes et al. (2021)	Very unlikely to very likely
	How likely would you provide your personal information to the pharmacy to have personalized recommendations?		
Perceived Sensitivity	How sensitive do you perceive the data, or think it is, which is used for the personalization?	Hui et al. (2007) and Xie et al. (2006)	Not sensitive at all to very sensitive
Perceived Risks of Information Disclosure	Providing the pharmacy with my personal information would involve many unexpected problems.	Xu et al. (2011)	Strongly disagree to strongly agree
	It would be risky to disclose my personal information to the online pharmacy.		
	There would be high potential for loss in disclosing my personal information to the pharmacy.		
Perceived Benefits of	The personalization reduces my search time to find the product that I need.	Xu et al. (2011), Hayes et al. (2021)	Strongly disagree to strongly agree

Information Disclosure	The personalization can provide me with the convenience to instantly access the products that I need.	and Unni and Harmon (2007)	
	Overall, I feel that using the personalization service is beneficial.		
Trust	The pharmacy would be trustworthy in handling the information	Malhotra et al. (2004) and Jarvenpaa et al. (1999)	Strongly disagree to strongly agree
	The pharmacy would tell the truth and fulfill promises related to the information provided by me.		
	I trust that the pharmacy would keep my best interests in mind when dealing with the information.		
	The pharmacy is predictable and consistent regarding the usage of the information.		
	The pharmacy is always honest with customers when it comes to using the information that I am providing.		
General Privacy Concerns	I am sensitive to the way companies handle my personal information.	Martin et al. (2017) and Malhotra et al. (2004)	Strongly disagree to strongly agree
	It is important to keep my privacy intact from online companies.		
	Personal privacy is very important, compared to other subjects.		
	I am concerned about threats to my personal privacy.		

Table 1: Measured Constructs in the Survey

5.5 Data Analysis and Results

5.5.1 Participation and Group Distribution

In total 151 participants finished the study. All questions were mandatory to finish the survey, which makes it not possible that the dataset has missing values. However, this was checked again, but no missing values were found. Of the 151 Participants, 49 (32%) were in group one, 54 (36%) in group two, and 48 (32%) in group three. The difference of the group size can be explained with the fact that not all participants finished the experiment. The equal distribution of the groups, however, only occurs in the beginning of every survey and does not check if the person stopped the participation. Of all 151 participants, 136 (90%) participated in German and 15 (10%) in English. Therefore, the majority of people were German speaking in this survey. Females were the majority ($n = 96$; 64%), before males ($n = 54$; 36%) and one diverse person (0.7%). The age was in average 28.36 across all groups. The age distribution is also illustrated in Figure 3, which shows that most of the participants are between 18 and 33 years old.

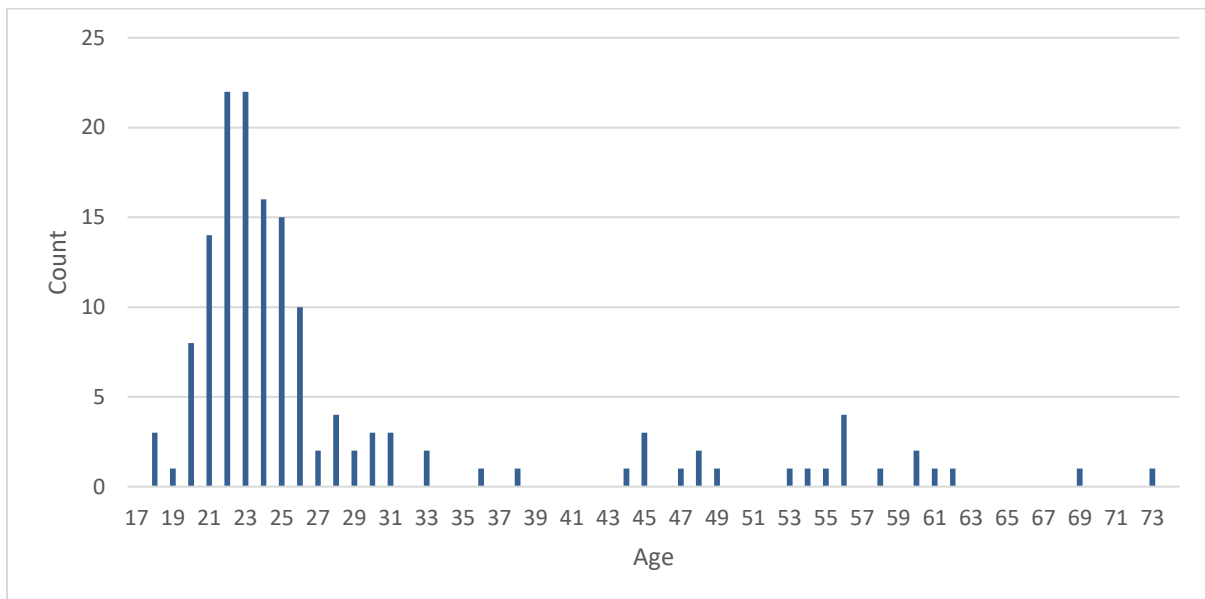


Figure 3: Age Distribution

The control of the general privacy concerns shows that group one and three have slightly higher concerns than group two. However, the ANOVA test shows that no significant difference can be found for the general privacy concerns. This also holds for the other variables, which show that no significant differences between the groups occur regarding the participants.

	Age	Gender	Language	General Privacy Concerns
P-Values of ANOVA	0.73	0.63	0.71	0.87

Table 2: ANOVA Test for the Three Groups

The following Table 3 shows the descriptive statistics of the previous mentioned measures, to have a detailed overview over the outcomes of the different groups.

	Total		Group 1 (No transparency)		Group 2 (Transparency, low sensitivity)		Group 3 (Transparency, high sensitivity)	
	Number/ Mean	sd	Number/ Mean	sd	Number/ Mean	sd	Number/ Mean	sd
Participants	151	-	49 (32%)	-	54 (36%)	-	48 (32%)	-
English	15 (10%)	-	4 (8%)	-	6 (11%)	-	5 (10%)	-
German	136 (90%)	-	45 (92%)	-	48 (89%)	-	43 (90%)	-
Female	96 (64%)	-	32 (65%)	-	34 (63%)	-	30 (63%)	-
Male	54 (36%)	-	17 (35%)	-	20 (37%)	-	17 (35%)	-
Divers	1 (0.7%)	-	0 (0%)	-	0 (0%)	-	1 (2%)	-
Age	28.36	11.66	28.55	11.69	27.30	8.71	29.38	14.35
General Privacy Concerns	5.12	1.10	5.27	1.04	4.81	1.27	5.31	0.96

Table 3: Descriptive Survey Information

5.5.2 Manipulation Check

People within the different groups were manipulated regarding data sensitivity. It was expected that group one (no transparency features and no information about sensitivity) has a medium perceived sensitivity, while group two (transparency features and low sensitivity) has a low perceived sensitivity, and group three (transparency features and high sensitivity) a high perceived sensitivity. To compare the perceived sensitivity of the three groups, a Kruskal-Wallis test was conducted. The result shows a p-value of $4.32e^{-5}$. This confirms that the groups are significantly different regarding the perceived sensitivity. This can also be seen in Table 4. However, in contrast to the expectations, group one perceived the lowest sensitivity, followed by group two and group three. Therefore, it

seems that the transparency features raised the perceived sensitivity, even though low sensitivity data was collected in group two. Table 4 additionally shows the descriptive statistics of trust, benefits of information disclosure, risks of information disclosure, and the willingness to disclose data for personalization. It can be seen that people have higher trust in the company when it offers transparency features. Especially in group two (transparency features, low sensitivity) the average trust is the highest with a value of 4.11. The benefits of information disclosure remain similar over all groups. However, the high sensitivity group has slightly higher values than the other two groups. Another, interesting finding of this table is that people in the high sensitivity group perceived the risks of information disclosure as high as people without transparency features. Group two (transparency features, low sensitivity), in contrast, has the lowest perceived risk in average. Lastly, the willingness to disclose data for personalization shows that group two has the higher value (3.88), followed by group one (3.00) and group three (2.69). Thus, this numbers indicate that effect of transparency features can have either a positive effect, for example with low sensitivity, or a negative effect, for example with very high data sensitivity, compared to the non-usage of transparency features.

	Total		Group 1 (No transparency)		Group 2 (Transparency, low sensitivity)		Group 3 (Transparency, high sensitivity)	
	Mean	sd	Mean	sd	Mean	sd	Mean	sd
Perceived Sensitivity	3.89	1.74	3.06	1.33	3.91	1.57	4.71	1.91
Trust	3.85	1.13	3.53	0.96	4.11	1.08	3.89	1.27
Benefits of Information Disclosure	4.72	1.20	4.69	1.18	4.70	1.26	4.76	1.16
Risks of Information Disclosure	4.24	1.35	4.39	1.23	3.98	1.36	4.38	1.43
Willingness to Disclose	3.22	1.68	3.00	1.51	3.88	1.75	2.69	1.53

Table 4: Descriptive Survey Information Part 2

5.5.3 Model Test

To validate the structural model shown earlier, partial least squares modelling was conducted (PLS-PM). The advantage of this method is that it is also working with relatively small sample sizes (Hair, Hult, Ringle, & Sarstedt, 2017). Regarding Hair et al. (2017), the sample size of the presented model must at least have 20 participants. Additionally, PLS is known to be more robust for misspecifications within the model (Henseler et al., 2014).

The PLS-PM function was conducted with the software R, using the “plspm” package provided. Additionally, bootstrapping is used to better verify the significance of the constructs. The PLS-PM function is performed with 5,000 bootstrapping resamples. In total, the model has a goodness of fit of 0.42. The R^2 of the goal variable willingness to disclose data for personalization is 0.45. Therefore, the model explains 45% of the variances.

The results show that the hypotheses regarding the privacy calculus are significant. Perceived benefits of information disclosure has a positive impact on the willingness to disclose data for personalization (path coefficient: 0.35), while perceived risks of information disclosure have a negative, and significant impact (path coefficient: -0.48). This result also shows that perceived risks have a stronger impact, compared to the perceived benefits. It can also be measured that trust has a negative impact on the perceived risks (path coefficient: -0.59). This means, people who have more trust in the service provider, perceive less risks in context of the data collection for personalization. Trust also has a positive and significant impact on the perceived benefits of information disclosure (path coefficient: 0.39). It can also be seen that the use of transparency features positively and significantly increases the trust perception of individuals (path coefficient: 0.20). However, there are also some hypotheses which cannot be supported. It cannot be supported that the use of transparency features has a direct impact on the perceived risks of information disclosure. The same holds for the effect of the transparency features on the perceived benefits of information disclosure. Additionally, the moderating effect of data sensitivity on the effect of transparency features and perceived risks cannot be supported. Table 5 summarizes these outcomes.

Hypotheses	Coefficient	P-Value	Supported
H1: Perceived benefits of information disclosure have a positive impact on the willingness to disclose data for personalization.	0.35	$1.73e^{-7}$	Yes
H2: Perceived risks of information disclosure have a negative impact on the willingness to disclose data for personalization.	-0.48	$6.06e^{-12}$	Yes

H3: The usage of transparency features has a negative impact on the perceived risks of information disclosure.	-0.10	0.29	No
H4: Data sensitivity negatively moderates the effect of transparency features on perceived risks of information disclosure.	-0.02	0.81	No
H5: The usage of transparency features has a positive impact on the perceived benefits of information disclosure.	-0.05	0.56	No
H6: Trust has a negative impact on the perceived risks of information disclosure.	-0.59	8.16e ⁻¹³	Yes
H7: Trust has a positive impact on the perceived benefits of information disclosure.	0.39	1.66e ⁻⁶	Yes
H8: Transparency features have a positive impact on trust.	0.20	0.013	Yes

Table 5: Path Model Estimation and Hypothesis Evaluation

Therefore, in this survey, transparency features had no direct impact on the perceived risks and perceived benefits of information disclosure. However, the effect is mediated by trust. Following that, transparency features have an indirect positive impact on perceived benefits, and an indirect negative impact on perceived risks. This concludes, that in this survey, the use of transparency features has the ability to increase the users' willingness to disclose data for personalization. This is shown by Table 6. This Table also highlights the importance of trust, having a total effect on the willingness to disclose data for personalization of 0.42. Over this avenue, via trust, transparency features have a total effect of 0.08 on the willingness to disclose data. However, note that this result includes the high sensitivity group as well.

Relationship	Direct effect	Indirect effect	Total effect
transparency -> trust	0.20	0.00	0.20
transparency -> disclosure	0.00	0.08	0.08
trust -> benefits	0.39	0.00	0.39
trust -> risks	-0.59	0.00	0.39
trust -> disclosure	0.00	0.42	0.42

Table 6: Total Effects of Transparency Features and Trust

5.5.4 Effect of Data Sensitivity

The model, however, does not explain which role data sensitivity plays in this context, even though the descriptive statistics showed that the willingness to disclose data for personalization is higher when low sensitivity data is used. Comparing the two transparency settings shows that the low sensitivity group has an average willingness to disclose of 3.88, while the high sensitivity group has one of 2.69.

As the effect of transparency features was already shown in this work, this chapter only compares the groups two and three. Both of them have transparency features, with the one difference of the data sensitivity. Therefore, this comparison allows to evaluate the effect of data sensitivity when transparency features are implemented. To test the model, the privacy calculus frame is taken, as well as the paths from trust to perceived benefits and perceived risks. Moreover, to have a holistic understanding of the working mechanism of data sensitivity, this construct is connected to the construct of perceived benefits, perceived risks, and trust. The following Figure 4 shows the model, as well as the outcome of the PLS analysis.

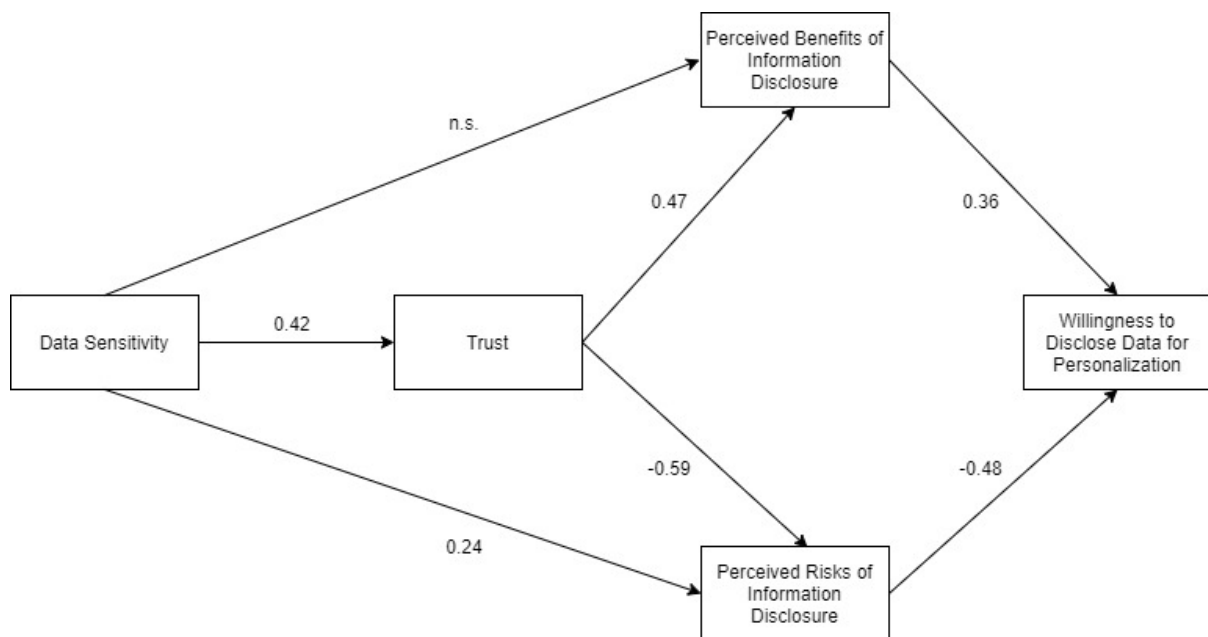


Figure 4: Comparing the Two Transparency Groups

This model confirms most of the outcomes which were shown in the previous PLS analysis. Perceived risks, as well as perceived benefits of information disclosure, are impacting the willingness to disclose data for personalization. Trust has a strong impact on perceived benefits, as well as on perceived risks. These outcomes indicate that transparency features and data sensitivity do not significantly change this working mechanism of the personalization privacy paradox, but are impacting some variables.

For example, the earlier analysis has shown that transparency features generally increase the perception of trust.

Data sensitivity has no significant impact on the perceived benefits of information disclosure. The effect of the perceived risks is significant and positive, meaning that a higher perceived data sensitivity leads to a higher risk perception. As the risks have a negative impact on the willingness to disclose data, data sensitivity has an indirect negative impact on the data disclosure. However, this model also gives other interesting insights. The path from data sensitivity to trust is significant and positive. Therefore, this shows that people who perceive data sensitivity to be higher, have a higher trust in the personalization provider. This is surprising, as this outcome contradicts with the descriptive statistics shown in the beginning. Remember that, when comparing the two transparency groups, the one with lower sensitive data has a higher trust perception, compared to the high sensitivity group (4.11 versus 3.89). The outcomes, however, would predict it the other way round. Table 7 shows the direct, the indirect, and the total effects of data sensitivity on the other constructs in the model. It also shows that a higher data sensitivity results in a higher willingness to disclose data for personalization when calculating the total effect of all paths. This, again, does not go in line with the descriptive statistics, which shows that the high sensitivity group comes with a lower willingness to disclose data for personalization compared with the low sensitivity group (2.69 versus 3.88). However, especially the total effects of data sensitivity on perceived risks and willingness to disclose data for personalization are quite low.

Relationship	Direct effect	Indirect effect	Total effect
sensitivity -> trust	0.42	0.00	0.42
sensitivity -> benefits	-0.09	0.20	0.11
sensitivity -> risk	0.24	-0.25	-0.01
sensitivity -> disclosure	0.00	0.04	0.04

Table 7: Total Effects of Data Sensitivity when Group 2 and 3 are compared

Those results show that it is hard to explain the effect of data sensitivity on the willingness to disclose data for personalization with the help of this privacy calculus model. This means, the effect can only be explained with measures, which are not included in this model. One option is for example that including affective and less cognitive constructs makes it possible to give better understanding of the effect of data sensitivity. However, note that this experiment was able to measure a difference between the low sensitivity and high sensitivity group when transparency features are used. It is only possible to explain the effect by the used model.

5.5.5 Effect of Different Privacy Personalities

As already explained, to control if the groups have similar people regarding their privacy personality, the general privacy concerns are measured. The result of the ANOVA analysis was that no significant difference can be found in the three groups. However, as the different personalities have a high attention within the personalization privacy paradox literature, the effect can also be analyzed in this context as well. To do so, each of the three groups is divided into two groups again. This is done by using the median of the general privacy concerns (GPC) of all participants. Therefore, the 50% of people, which belong to those with lower GPC, are in the low GPC group, while the people equal and greater belong to the high GPC group. By using the median of all participants and not dividing every group by its own median, makes it possible to set a status quo which is group independent. Thus, the results between the groups can be better compared. The following Table 8 shows these results.

	Total		Group 1 (no transparency features)		Group 2 (transparency features, low sensitivity)		Group 3 (transparency features, high sensitivity)	
	Low GPC	High GPC	Low GPC	High GPC	Low GPC	High GPC	Low GPC	High GPC
Number	68	83	20	29	27	27	21	27
Average GPC	4.13	5.92	4.24	5.97	3.80	5.82	4.45	5.97
Average Age	26.32	30.04	25.95	30.34	24.56	30.04	28.95	29.70
Average Sensitivity	3.94	3.84	2.95	3.14	3.74	4.07	5.14	4.37
Average Trust	4.09	3.65	3.54	3.52	4.30	3.92	4.34	3.53
Average Risks	3.88	4.54	4.07	4.62	3.56	4.40	4.11	4.59
Average Benefits	5.01	4.47	5.10	4.40	4.88	4.53	5.10	4.49
Average Disclosure	3.85	2.70	3.48	2.67	4.63	3.13	3.19	2.30

Table 8: Group Differences in the Context of Privacy Personalities

The table also shows that most of the GPC groups have a higher number of participants, even though the median was used. This can be explained as those who are exactly on the 50% quantile are allocated to this group.

A look at the average age indicates that people with a higher age are more likely to have higher general privacy concerns than younger people. The trust perception is similar, but slightly higher for the high GPC group in the transparency, low sensitivity group setting. The high GPC groups generally rates perceived risks higher than the low GPC groups, while the perceived benefits are rated lower. In line with that, the high GPC Groups are less willing to disclose data for personalization. However, both groups have the highest willingness in the transparency and low sensitivity setting. This is followed by the non-transparency setting, and the transparency, high sensitivity variant. Therefore, both privacy groups would disclose less data when transparency features are offered, and high sensitivity data is collected at the same time.

Moreover, a look at the average sensitivity gives interesting insights. The numbers show that the sensitivity is perceived to be the lowest in the first group, while it is the highest in the third. In the first two groups, people with higher GPC have a slightly higher sensitivity perception than people with lower GPC. However, in the third group, which is the one with transparency features and high data sensitivity, people with low GPC perceive the data to be higher than people with higher GPC. Therefore, it is also visible that the fluctuation between the groups is higher in the low GPC groups. This is visualized in the following Figure 5.

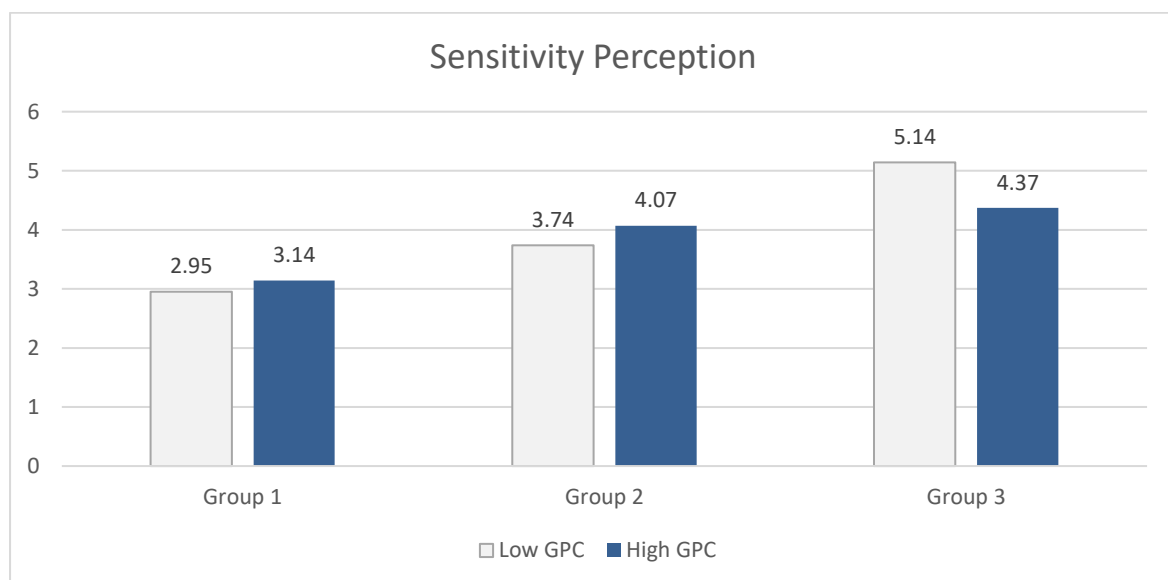


Figure 5: Differences in the Sensitivity Perception

To further validate the results, the first hypothesis model is tested again. However, in this case not the whole data is used, but two groups are tested separately. The first is the low GPC group, and the second is the high GPC group. The results can be found in Figure 6.

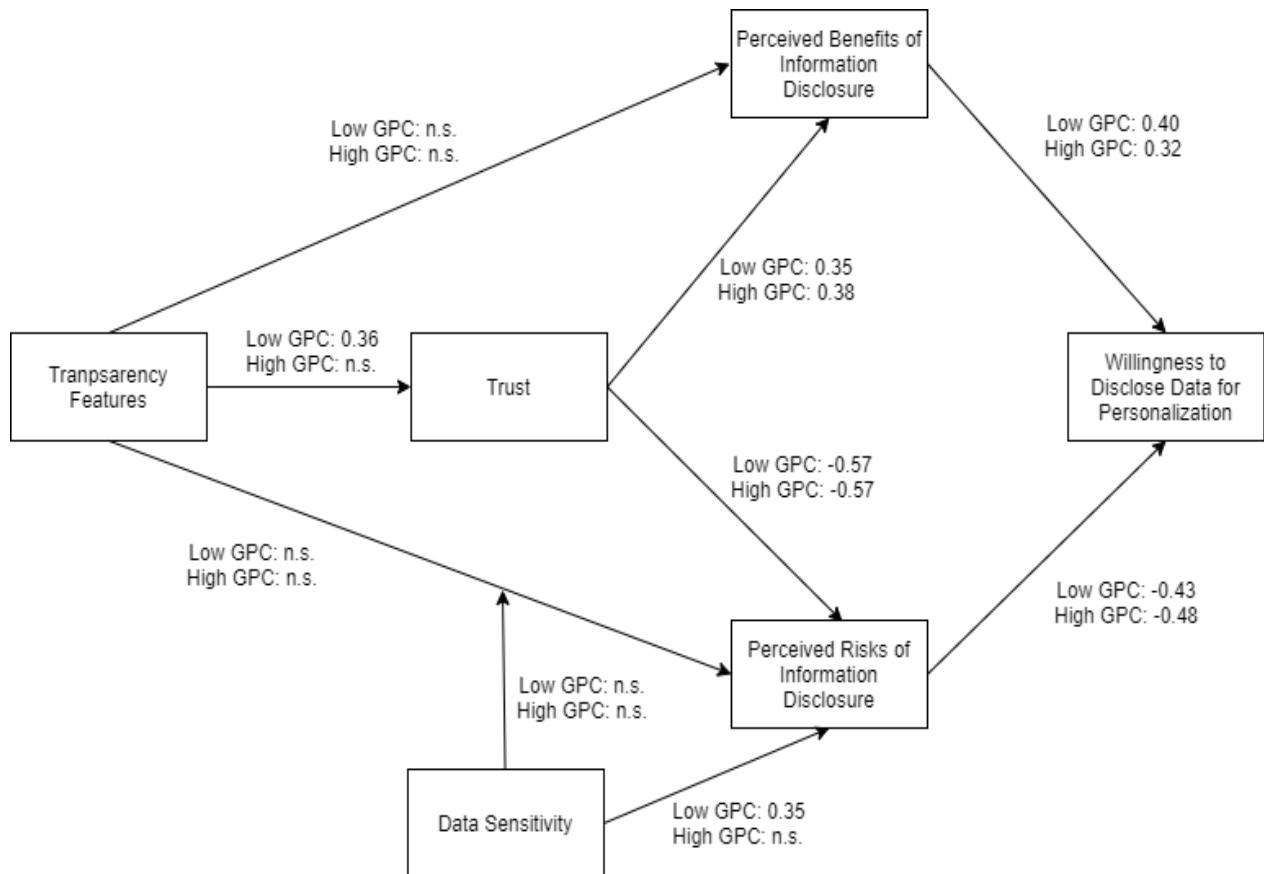


Figure 6: Hypothesis Model with Privacy Group Separation

The model reveals three main differences between the two groups. First, the effect of transparency features on trust is only significant in the low GPC group, but not in the high one. As the path coefficients of transparency features on perceived risks and perceived benefits are not significant, the effect on trust is the only path which has an impact on the willingness to disclose data for personalization. However, the insignificance in the high GPC group indicates that this model is not able to find an impact of transparency features in this group.

Second, data sensitivity has a positive and significant impact on the perceived risks of information disclosure in the low GPC group. Therefore, a higher perceived data sensitivity has the ability to reduce the willingness to disclose data for personalization. However, this effect is not significant in the high GPC group. Note that data sensitivity was perceived especially high in the low GPC group

when the online pharmacy indicates to use more sensitive data. Therefore, they perceive the data to be more sensitive and additionally include the data sensitivity in their decision model, compared to the high GPC group. This points out that data sensitivity has an important role in the low general privacy concerns group.

Third, the path coefficients from the perceived benefits and risks to the willingness to disclose data for personalization indicate that the decision weight is slightly different for both groups. For the path between perceived risks and the willingness to disclose data, the high GPC group has the stronger negative impact. This means this group is including the risk perception stronger in their decision-making process compared to the low GPC group. In contrast, the path between perceived benefits and willingness to disclose data is stronger for the low GPC group. This indicates that this group is stronger focusing on the benefits when deciding to disclose data or not. However, these differences should not be overinterpreted.

5.5.6 Demographic Effects

Table 3 already showed that more females (64%) than men (34%) participated in the survey. Therefore, it is interesting to know if different genders have different perceptions in the study. As only one diverse person participated, this one is excluded in this context, as it is not possible to state any statistical relevant outcomes. The following Table 9 shows the differences between females and males across all groups. Males rated all items slightly higher, except for the willingness to disclose data for personalization. However, the t-test only shows significance for the perceived sensitivity. Therefore, men significantly perceive data sensitivity higher than females.

	Perceived Sensitivity	Trust	Perceived Benefits	Perceived Risks	Willingness to disclose data	General Privacy Concerns
Females	3.64	3.75	4.64	4.18	3.28	5.06
Males	4.37	4.04	4.84	4.32	3.15	5.19
P-value (t-test)	0.01	0.15	0.32	0.55	0.66	0.49

Table 9: Gender Differences Across Groups

Besides the gender, the age is another demographic aspect, which is not equally distributed in this survey. This was earlier visible in Figure 3. Most of the participants are between 18 and 33 years old. Therefore, it can be necessary to analyze which effect age has on different factors. To do so, two groups are created. One is the young age group, in which all participants are allocated which are younger than the 50% quantile. The old age group includes all participants which are equal or greater to the 50% quantile of the age across all groups. The results can be seen in the following Table 10.

	Perceived Sensitivity	Trust	Perceived Benefits	Perceived Risks	Willingness to disclose data	General Privacy Concerns
Young Age	4.01	3.92	4.98	3.90	3.59	4.91
Old Age	3.78	3.79	4.49	4.53	2.90	5.30
P-value (t-test)	0.41	0.50	0.01	< 0.01	0.01	0.04

Table 10: Age Differences Across Groups

It shows that older people perceive data sensitivity slightly lower and have less trust in the online pharmacy. However, conducting a t-test shows that the differences are not significant. In contrast, significant differences between perceived benefits, perceived risks, the willingness to disclose data for personalization, and the general privacy concerns exist. That older people have higher general privacy concerns was already visible in the previous chapter, as the average age for the high GPC group was higher than for the low GPC group. Moreover, older people perceive less benefits and higher risks due to personalization. As a result, the willingness to disclose data for personalization is lower than for young people. These results indicate that the evaluation of personalization can be dependent on the age. These data show that young people are more open to use personalized services, independent of transparency features and data sensitivity.

6 Discussion

The literature review has shown that the personalization privacy paradox is a multidimensional and complex research field. To better understand the paradox, this work distinguishes two different dimensions. The first is the context. This includes all surrounding aspects, which people experience when they enter a personalized environment. Those aspects are the same for all users, but still can be perceived differently by them. This includes the types of personalization, pull versus push based personalization, information security, transparency features, the situation, personalization intensity, and data sensitivity.

The comparison of different personalization types has shown that perceived value can be greater for service personalization, compared to advertisement personalization (Awad & Krishnan, 2006). The use of push and pull based personalization approaches has different advantages and disadvantages. While push based can come with positive aspects like higher spontaneous purchases, or higher

perceived benefits, it also raises privacy concerns (Xu et al., 2011). Therefore, to overcome the personalization privacy paradox, pull based personalization can be helpful, as this approach can mitigate privacy concerns (Aguirre et al., 2015; Xu et al., 2011). Another variant to overcome the paradox is by offering high information security approaches and communicate those to the users (Sutanto et al., 2013). The effect of transparency features, however, is not solved in literature so far. While Awad and Krishnan (2006) claim that transparency features are only important for people who have a strong valuation for privacy, Karwatzki et al. (2017) were not able to support these outcomes and found no significant effect of transparency features. In contrast, Bleier and Eisenbeiss (2015) showed that transparency features can be important to overcome the personalization privacy paradox when personalization intensity is high. This indicates that transparency features must be set in further context. Sheng et al. (2008) showed that the situation in which the personalization is offered can be essential when dealing with the personalization privacy paradox. They showed that people are more willing to adapt personalization when they are in an emergency situation. Literature has also shown that personalization intensity has a positive impact on perceived benefits (Hayes et al., 2021; Xu et al., 2011). In contrast, higher personalization intensity can come with negative aspects, like increased perceived risks or higher perceived vulnerability. However, these negative aspects can be overcome, for example by pull based personalization, or if only people are targeted with low privacy valuation (Aguirre et al., 2015; Karwatzki et al., 2017; Xu et al., 2011). The last context specific aspect is data sensitivity. Even though little research was done in this context, research agrees that data sensitivity is negatively correlated with the willingness to disclose data for personalization over different paths (Hayes et al., 2021; Sutanto et al., 2013).

The second dimension is the users' inner working mechanism of their decision-making process when they experience personalization. This dimension considers for example the benefits versus risk trade-off, different privacy personalities, happiness, and trust. The trade-off between benefits and risks is a commonly used, cognitive approach to explain data disclosure or willingness to use personalized services (Chellappa & Sin, 2005; Hayes et al., 2021; Sheng et al., 2008; Sutanto et al., 2013; Xu et al., 2011). As already described, benefits can be risen, as well as risks, due to personalization. However, the risks can be mitigated, for example by implementing information security technology or by offering pull based personalization (Hayes et al., 2021; Xu et al., 2009). Whether people are willing to use the personalization is dependent on the outcome of this trade-off. When the benefits exceed the risks, it is likely that users are willing to use personalized offerings (Chellappa & Sin, 2005). Other, well discussed aspects are the different privacy personalities. Several studies show that people have different valuation for privacy and thus are reacting different within the personalization privacy paradox (Awad & Krishnan, 2006; Karwatzki et al., 2017; Lee et al., 2011; Xu et al., 2022; Zhu et al., 2017). On the one side, there are people for who privacy is essential. Those are unlikely to use personalized offerings. On the other side, there are people for who privacy is not important. Those are

more likely to use personalization, especially when it comes with benefits (Westin, 2003). Therefore, personalization providers should know their customers and target group (Xu et al., 2022). One option to offer the services to a broad variety of users, is by personalize the personalization, which means that individuals can choose their settings regarding personalization (Lee et al., 2011). Moreover, happiness and trust were found to be two main constructs in the personalization privacy paradox. While research regarding happiness is limited, but indicates that happiness leads to a higher personalization usage rate, the importance of trust was shown in several studies (Bleier & Eisenbeiss, 2015; Chellappa & Sin, 2005; Cloarec et al., 2022). Trust is able to have a positive impact on the perceived benefits of personalization, as well as to lower negative impact factors, for example the perceived risks (Aguirre et al., 2015; Bleier & Eisenbeiss, 2015; Chellappa & Sin, 2005; Cloarec et al., 2022).

On the basis of the literature review, an own experiment was conducted. The goal of this experiment was to set transparency features into a new context by manipulating the participants with different data sensitivities. This experiment provides several outcomes.

First, the use of transparency features has a positive and significant impact on the trust perception of the users. Over this avenue, transparency features can increase the willingness to disclose data for personalization. Even though the model is not able to explain the effect of data sensitivity, it is visible that the low sensitivity group with transparency features has a higher willingness to disclose data compared to the high sensitivity group or the non-transparency group. Thus, this experiment shows that transparency features can have a positive impact for data disclosure and supports prior literature (Bleier & Eisenbeiss, 2015). However, it also shows that this advantage disappears when data sensitivity of data, which is collected and communicated with the help of transparency features, is perceived as too high. Moreover, the willingness to disclose data in the experiment is lower in the transparency and high sensitivity setting compared to the non-transparency setting. This shows that transparency features have to be set into context, as the effect can change from context to context. This can explain why for example Karwatzki et al. (2017) did not find a significant impact of transparency features.

Moreover, using transparency can also increase the perceived data sensitivity of users. Therefore, people perceived data more sensitive in the low sensitive setting, compared to the one with no information about that. It is probable, that by using transparency features and naming the data, which is collected, the awareness rises, as proposed by Karwatzki et al. (2017).

By investigating the different privacy groups, the outcome from Awad and Krishnan (2006) cannot be supported. In the low general privacy concerns group, the effect of transparency features on trust is significant, while it is not in the high general privacy concerns group. This also implies that the model is not able to find any connection between transparency features and willingness to disclose data for

personalization for the high general privacy concerns group. Therefore, the effect of transparency features is only present in the low general privacy concerns group.

Moreover, the analysis shows that data sensitivity can raise the perceived risks in the low GPC group. Additionally, people in this group perceive highly sensitive data as especially sensitive, compared to the high GPC group. Surprisingly, in the high sensitivity variant, the sensitivity perception of the low GPC group is higher than in the high GPC group. One possible explanation is that people in the low GPC group generally do not expect that companies collect such data. By using transparency features and showing them that such data is used, they are negatively surprised with this information. It is possible that this triggers an affective reaction, which has an impact on the sensitivity evaluation. However, this speculation needs further evaluation by research.

The last interesting insight is that older people tend to have higher general privacy concerns. This is relevant, as the literature has shown that the differentiation into different privacy personalities is important in the context of the personalization privacy paradox (Awad & Krishnan, 2006; Lee et al., 2011; Xu et al., 2009; Zhu et al., 2017). Moreover, younger people are more open to use personalized services in this survey.

Practical Implications

Using transparency features can increase the user's trust into the service, which is personalized. This is especially important, as increased trust can lead to higher adoption rates of personalization. However, the survey also indicates that transparency should only be used when low sensitivity data is used. Therefore, every personalization provider should evaluate case by case if transparency features are beneficial. Moreover, especially for customers who do not value privacy to a high extent, companies should be careful using transparency features, as those people perceive highly sensitive data as especially sensitive, and data sensitivity additionally raises the perceived risks. Therefore, it is necessary for companies to know their customer group. However, as the high sensitivity setup did not come with significantly lower data disclosure rates compared to the no-transparency variant, companies should tend to use transparency features more often.

Theoretical Implications

The first theoretical insight is that the willingness to disclose data was shown to be lower in the high sensitivity setup compared to the low sensitivity one. Therefore, data sensitivity can play a role in the personalization privacy paradox and should therefore be further considered in research. Moreover, it can be seen that transparency features can have a different impact, dependent on the data sensitivity. This makes it visible that transparency features cannot be analyzed independent of different contexts. However, data sensitivity is only one example of those context specific aspects, which matter when the effect of transparency features is measured. The model, however, was not able to explain the

effect of data sensitivity in this context. This shows that research should also focus on more affective approaches, which do not only consider cognitive decision making.

Limitations

This work also comes with some limitations. The first is that only intentional willingness to disclose data for personalization is measured, and not real behavior. However, the privacy paradox has shown that there can be a gap between intentional and actual data disclosure (Norberg, Horne, & Horne, 2007).

Moreover, the model mainly includes cognitive constructs of the data disclosing process. Therefore, affective and non-cognitive aspects are missing. The survey also does not perfectly replicate the real world. This again includes affective stimuli, as the survey description tried to minimize those effects, but also other. For example, people can have the feeling to be observed and thus reacting differently than normal.

Another limitation is the sample. The age distribution earlier showed that mainly young people participated in the survey, which makes it not representative for the whole population. Additionally, more females than men participated. However, this survey also showed that the gender differences are not as strong as the differences of different ages. Moreover, most of the participants were German speaking, which makes it impossible to exclude country specific characteristics.

Moreover, implementing transparency features can be done differently. This work only used one formulation, which was the same for the two transparency groups. The only exception was the selection of the data used for personalization, to be able to manipulate the data sensitivity. However, transparency features can for example concentrate more on highlighting the benefits or mitigating the risks. In this work, a mix of both is taken. Nevertheless, it is possible that the design of the transparency features has an impact on the outcomes.

Last, this study focused on the personalization privacy paradox in the context of service personalization. Therefore, other personalization types are not taken into account. Literature has shown that different personalization types, for example service and advertisement personalization have different outcomes (Awad & Krishnan, 2006). Moreover, the same holds for the context of the online pharmacy. This is a very concrete example, which does not mean that the outcomes are the same with other service providers.

Future Research

Future research should further set transparency features into context. This can include data sensitivity, but also other context specific settings. Moreover, this can be connected with exploring different types of transparency features. This can for example include the formulation, but also the type of the presentation, as transparency features in literature mainly focus on written statements. Additionally, research can include more emotional and affective constructs to better understand the working mechanism of sensitivity when transparency features are used.

References

- Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: Examining user scenarios and privacy preferences, *Proceedings of the 1st ACM Conference on Electronic Commerce*, 1–8.
- Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclosure. *Journal of Marketing Research*, 49, 160–174.
- Aguirre, E., Mahr, D., Grewal, D., Ruygter, K., & Wetzels, M. (2015). Unraveling the Personalization Paradox: The Effect of Information Collection on Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing*, 91(1), 34–49.
- Albashrawi, M., & Motiwalla, L. (2019). Privacy and Personalization in Continued Usage Intention of Mobile Banking: An Integrative Perspective. *Information Systems Frontiers*, 21(5), 1031–1043. <https://doi.org/10.1007/s10796-017-9814-7>
- Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, 30(1), 13–28.
- Bleier, A., & Eisenbeiss, M. (2015). The Importance of Trust for Personalized Online Advertising. *Journal of Retailing*, 91(3), 390–409. <https://doi.org/10.1016/j.jretai.2015.04.001>
- Boersenblatt (2021). Ein Drittel mehr Umsatz für Amazon in Deutschland. Retrieved from <https://www.boersenblatt.net/news/ein-drittel-mehr-umsatz-fuer-amazon-deutschland-163619>
- Brandt, M. (2021). Die Top 10 Online-Apotheken in Deutschland. *Statista*. Retrieved from <https://de.statista.com/infografik/15489/die-top-10-online-apotheken-in-deutschland-nach-umsatz/>
- Chellappa, R. K., & Sin, R. (2005). Personalization versus privacy: an empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2), 181–202.
- Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting and Social Change*, 161, 120299.
- Cloarec, J., Meyer - Waarden, L., & Munzel, A. (2022). The personalization-privacy paradox at the nexus of social exchange and construal level theories. *Psychology & Marketing*, 39(3), 647–661.
- Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10, 104–115.
- Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323–342.
- Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking

- Outside the “APCO” Box. *Information Systems Research*, 26(4), 639–655.
<https://doi.org/10.1287/isre.2015.0600>
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (2nd). SAGE Publications.
- Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021). The Influence of Consumer–Brand Relationship on the Personalized Advertising Privacy Calculus in Social Media. *Journal of Interactive Marketing*, 55, 16–30.
- Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., . . . Calantone, R. J. (2014). Common Beliefs and Reality About PLS: Comments on Rönkkö and Evermann (2013). *Organizational Research Methods*, 17(2), 182–209.
- Hui, K., Teo, H. H., & Lee, S. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, 31(1), 19–33.
- Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, 5(2).
- Karwatzki, S., Dytnko, O., Trenz, M., & Veit, D. (2017). Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems*, 34(2), 369–400.
<https://doi.org/10.1080/07421222.2017.1334467>
- Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6), 607–635.
- Kim, W. (2002). Personalization: Definition, status, and challenges ahead. *Journal of Object Technology*, 1(1), 29–40.
- Kobsa, A. (2007). Privacy-enhanced personalization. *Communications of the ACM*, 50(8), 24–33.
<https://doi.org/10.1145/1278201.1278202>
- Lee, D. J., Ahn, J. H., & Bang, Y. (2011). Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection. *MIS Quarterly*, 35(2), 423–444.
- Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, 51(3), 434–445. <https://doi.org/10.1016/j.dss.2011.01.017>
- Li, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, 21(6), 621–642.
<https://doi.org/10.1057/ejis.2012.13>

- Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, 27(4), 161–200.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUPIC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355.
- Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. *American Marketing Association*, 36(1), 79–96.
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58.
- Norberg, P., Horne, D., & Horne, D. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, 41(1), 100–128.
- Ong, C. S., Chang, S. C., & Lee, S. M. (2015). Development of WebHapp: Factors in predicting user perceptoins of website-related happiness. *Journal of Business Research*, 68(3), 591–598.
- Personalization Consortium (2003). What is Personalization. *Personalization Consortium*.
- Rognehaugh, R. (1999). The Health Information Technology Dictionary. *Aspen*.
- Sheng, H., Nah, F., & Siau, K. (2008). An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns. *Journal of the Association for Information Systems*, 9(6), 344–376.
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35, 989–1015.
- Sutanto, J., Palme, E., Tan, C., & Phang, C. W. (2013). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly*, 37(3), 1141–1164.
- Tam, K. Y., & Ho, S. Y. (2006). Understanding the Impact of Web Personalization on User Information Processing and Decision Outcomes. *MIS Quarterly*, 30(4), 865–890.
- Thirumalai, S., & Sinha, K. K. (2013). To personalize or not to personalize online purchase interactions: Implications of self-selection by retailers. *Information Systems Research*, 24(3), 683–708.
- Treiblmaier, H., & Pollach, I. (2007). Users' Perceptions of Benefits and Costs of Perrsonalization. *International Conference on Information Systems*, 28, 1–15.
- Unni, R., & Harmon, R. (2007). Perceived Effectiveness of Push vs. Pull Mobile Location Based Advertising. *Journal of Interactive Advertising*, 7(2), 28–40.

- Vesanen, J. (2007). What is personalization? A conceptual framework. *European Journal of Marketing*, 41(5/6), 409–418.
- Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2), 8–23.
- Westin, A. F. (1967). Privacy and Freedom. *Athenaeum*.
- Westin, A. F. (1991). How the American Public Vies Consumer Privacy Issues in the Early 90s - and Why. *Committee on Government Relations, U.S. House of Representatives*. (54-68).
- Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), 431–453.
- Xie, E., Teo, H.-H., & Wan, W. (2006). Volunteering personal information on the internet: Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Springer Science and Business Media*, 17.
<https://doi.org/10.1007/s11002-006-4147-1>
- Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1), 42–52.
- Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems*, 26(3), 135–174. <https://doi.org/10.2753/MIS0742-1222260305>
- Xu, L., Li, Y., & Yao, Q. (2022). Information security investment and purchase decision for personalized products. *Managerial and Decision Economics*.
- Zeng, F., Ye, Q., Yang, Z., Li, J., & Song, Y. A. (2019). Which Privacy Policy Works, Privacy Assurance or Personalization Declaration? An Investigation of Privacy Policies and Privacy Concerns. *Journal of Business Ethics*, 176(4), 781–798. <https://doi.org/10.1007/s10551-020-04626-x>
- Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure Intention of Location-Related Information in Location-Based Social Network Services. *International Journal of Electronic Commerce*, 16(4), 53–90. <https://doi.org/10.2753/JEC1086-4415160403>
- Zhu, H., Ou, C. X.J., van den Heuvel, W.J.A.M., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management*, 54(4), 427–437. <https://doi.org/10.1016/j.im.2016.10.001>

Appendix

Authors	Year	Mechanism			Context			
		Measured Constructs/Constructs involved	Role of personalization	Types of personalization	Push- vs. Pulled based personalization	Data collection Environment	Theoretical Framework used	Definition of Personalization Privacy Paradox
Aguirre et al.	2015	Personalization, Trust, Click through intentions, information collection, Perceived vulnerability	Different Personalization groups	Advertisement Personalization	Push-and Pull approach	Social Media Field Experiments	Psychological ownership theory	Tradeoff between higher customer adoption and relevance for customers versus increased customers' vulnerability and lower adoption rates
Albashrawi and Motiwalla	2019	Personalization, privacy, perceived usefulness, perceived ease of use, customer satisfaction, continued usage intention of mobile banking	Measured construct	Service Personalization	Push	Experiment	Technology acceptance model	Tradeoff between privacy and personalization
Awad and Krishnan	2006	Transparency Features, General Privacy Concerns, Previous Online Invasion, Differentiation in Privacy Groups, Willingness to be profiled	As boundary condition/as fixed environment	Advertisement and Service Personalization	Pushed (covert)	Survey	Utility Maximization Theory	consumers who value information transparency features are less willing to be profiled online for personalized service and advertising
Bleier and Eisenbeiss	2015	More and less trusted retailer, Ad personalization depth and breadth, usefulness, reactance, privacy concerns, click-through intentions	fixed environment, but different sorts are measured	Advertisement Personalization	Push	Scenario-based online experiment	Stimulus Organism Response Model	Not directly mentioned, but positive and negative aspects of personalization are measured
Chellappa and Sin	2005	Value for Personalization, Concerns for Privacy, Trust Building Factors, Likelihood of Using personalization Services	fixed environment	Service Personalization	Push	Survey	Privacy Calculus	Personalization versus Privacy, but Paradox not directly mentioned
Clarec	2020	Trust, Privacy Concerns, Risks/ Costs, Benefits, Level of Attention, Information Disclosure	fixed environment	Not specified	No information	No data collection	Privacy Calculus (enhanced APCO Model)	Tension between value of personalization and privacy concerns
Clarec et al.	2022	Information collection concerns, Risk beliefs, Happiness, Trust beliefs, willingness to disclose information for personalization, internet literacy	Integrated into the goal variable: willingness to disclose information for personalization	Marketing Personalization (Social Media), but in a general context	No information	Online Survey	Social exchange and construal level theory	Benefits of personalization are constrained by privacy concerns
Hayes et al.	2021	Personalization, Brand Relationship Strength, Perceived Benefits, Perceived risk, Perceived Value of information disclosure, Willing to have personal information used, purchase intention, perceived vulnerability	Antecedent/ As exogenous construct	Advertisement Personalization	Push-and Pull approach	Social Media Experiment	Privacy Calculus	Tension between Personalization Benefits and Perceived risk, which arises due to personalization
Karwatzki et al.	2017	Personalization, Transparency Features, Information Disclosure, Differentiation in Privacy Groups, Disposition to value privacy, experience with the internet, experience with online personalization, Willingness to disclose information	As boundary condition/as fixed environment	Service Personalization	Pushed (covert)	Website	Information Boundary Theory	Definition of Awad and Krishnan (2006)
Kobsa	2007	Trust, Privacy Concerns, Value of Personalization, individual privacy attitudes, type of information to be disclosed, awareness and control over the use of personal information	fixed environment	Not specified	No information	No data collection	Privacy Calculus	Tension between personalization and privacy (but paradox not specifically mentioned)
Lee et al.	2011	Privacy Protection, Social Welfare, Privacy Regulation	fixed environment	Service Personalization	No information	No data collection	Game theory, Privacy Calculus	Personalization-privacy tradeoff

Table 11: Concept Matrix Part 1

		Mechanism				Context			
Authors	Year	Measured Constructs/Constructs involved	Role of personalization	Types of personalization	Push- vs. Pulled based personalization	Data collection Environment	Theoretical Framework used	Definition of Personalization Privacy Paradox	
Li and Unger	2012	Privacy Concerns, Privacy Protection, Perceived Quality of Personalization, Industry Domain, Past Experience, Likelihood of Using Online Personalization, Willingness to Pay a Premium, Willingness to Provide Information	fixed environment	Service Personalization	Push	Quasi-experimental approach	none	Expectation of consumers that a service provider will provide personalized services based on their profiles and trust that the provider will not indiscriminately share their personal information	
Sheng et al.	2008	Personalization, Context (Emergency versus non-Emergency), Privacy Concerns, Intention to adopt	Antecedent	Service Personalization	Push	Experiment Study	Privacy Calculus	Personalization comes with benefits, but also arises privacy concerns for the customers	
Sutanto et al.	2013	Personalization, Perceived Sensitivity, Information Privacy Concerns, Psychological Comfort, Perceived intrusion of Information Boundaries, benefits of personalization, perceived effectiveness of privacy-safe feature, intention to save adverts to the application, trust	As boundary condition/as fixed environment	Advertisement Personalization	Pushed (covert)	Mobile Phone Application	Gratification theory and information boundary theory	Tension between how the developers and marketers of IT applications exploit users' information to offer them personalized services, and those users' growing concerns about the privacy of that information	
Unni and Hamon	2007	privacy concerns about location tracking, perceived benefits, value, and intentions to try location-based advertising	Different Personalization groups (pull vs. push)	Advertisement Personalization (location aware)	Pushed and pulled approach	Survey	none	Does not directly name the Personalization Privacy Paradox, but deals with the tension between personalization benefits and privacy concerns	
Xu et al.	2011	Personalization, Previous Online Invasion, Perceived Benefits, Perceived Risks, Perceived Value of Disclosure, Willingness to have personal information used in LAM, Purchase Intention	As Antecedent	Advertisement Personalization (location aware)	Pushed (covert) and pulled (overt)	Mobile Phone Application	Privacy Calculus	Personalization and the resulting benefits versus perceived risks of information disclosure	
Xu et al.	2022	No measured constructs. Game Theory about security investments	fixed environment	Not specified	Push	No data collection	Simultaneous game, Firm-led Stackelberg game, and firm-led Stackelberg game with punishment	Tradeoff between personalization and information security for consumers	
Xu et al.	2009	Information Delivery Mechanisms, Privacy-Related Interventions, Privacy Benefits, Privacy Risks, Intention to Disclose Personal Information in LBS	fixed environment	Service Personalization	Push-and Pull approach	Quasi-experimental survey method	Privacy Calculus	Tension between personalization Benefits and Perceived risk	
Zeng et al.	2019	Privacy assurance, Personalization declaration, Act of self-disclosure, Intensity of self-disclosure, Purchase	fixed environment	Service Personalization	Push	Survey	none	Tradeoff between personalization benefits and privacy concerns	
Zhao et al.	2012	Incentives provision, interaction promotion, extrinsic and intrinsic benefits personalization, privacy control, privacy policy, privacy concerns, awareness of legislation, previous privacy invasions, personal innovativeness, intention to disclose location-based information	fixed environment	Service Personalization (location aware)	Push	Survey	Privacy Calculus, Justice Theory	Not directly mentioned, but benefit-privacy concerns tradeoff is measured	
Zhu et al.	2017	Privacy Benefits, Privacy Concerns/Risks, company reputation, different privacy groups, use of personalized services	fixed environment	Service Personalization	Push	Simulation data	Multi-attribute utility theory, Privacy Calculus	Balance between customers' enjoyment of personalization, but also risk perception due to personalization	

Table 12: Concept Matrix Part 2