5-11-2023

# GDPR Privacy Type Clustering: Motivational Factors for Consumer Data Sharing

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

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

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

# GDPR PRIVACY TYPE CLUSTERING: MOTIVATIONAL FACTORS FOR CONSUMER DATA SHARING

*Research Paper*

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

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

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

## Abstract

*The GDPR introduced restrictive privacy-preserving measures, affecting the daily life of (online) consumers. Moreover, literature shows that privacy preferences are constantly evolving. This is the first study introducing a GDPR exercising-oriented approach to identify consumer privacy types. Based on a representative sample of the German online population, we cluster consumers according to their privacy importance ("intention to act") and GDPR knowledge ("ability to act") and derive four consumer privacy type clusters: fundamentalists, amateurs, pragmatists, and unconcerned. We investigate motivational factors for changing privacy settings and find significant differences between consumers' intentions and actions for selected factors. This provides evidence for the privacy paradox. Contrarily, intentions and actions align for other factors, which supports the hypothesis that action-based consent might lower the privacy paradox. Finally, we suggest the development of standardized scales and corresponding clustering methodologies for consumer privacy type clustering to increase comparability over time and across populations.*

*Keywords: Privacy, General Data Protection Regulation, GDPR, Privacy Types, Privacy Personas, Clustering, Data Sharing.*

## 1 Introduction

The increasing Internet adoption and related use of consumer data have contributed to drawing public attention to (online) privacy issues (Westin, 2003). Lately, the introduction of the General Data Protection Regulation (GDPR) (European Parliament and the Council, 2016) and its new consumer privacy rights marks a peak of public attention to privacy topics. Since then, GDPR-related information obligations constantly remind (online) consumers of data privacy aspects, e.g., cookie consent management on websites or privacy settings in online profiles. In addition, many companies have recently started actively promoting privacy as a product or service feature (e.g., Apple, Samsung, Google, Meta). However, given the recent changes in the context of privacy and privacy awareness, there is little empirical research on how consumers execute their newly gained GDPR rights and how consumers' intentions and abilities to act influence this process.

Before the GDPR introduction, researchers already identified consumer privacy types and investigated motivational and contextual factors for data sharing (e.g., Acquisti et al., 2015; Goldfarb and Tucker, 2012; John et al., 2011; Brandimarte et al., 2013). We build upon this research and analyze in the context of the GDPR how online consumer privacy behavior differs across consumer privacy types and which motivational factors for data sharing prevail. For this purpose, we conduct a consumer survey with a representative sample of the German online population. The survey systematically gathers information

on the intention, action, and prevention of consumers' motivations to disclose, revoke and delete personal data in the hands of online providers. We suggest a novel GDPR exercising-oriented clustering approach by combining the privacy importance scale as an indicator of the consumer's *intention to act* and the GDPR knowledge scale as an indicator of the *ability to act.* This approach allows us to cluster consumers according to their privacy tendency and relate these findings to previous studies regarding consumer privacy types (Westin, 2003; Hoofnagle and Urban, 2014; Hann et al., 2007; Dupree et al., 2016). Furthermore, the results allow us to dissect potential differences between consumer privacy types and their respective intentions and actions, providing insights into the current state of the privacy paradox with online consumers (e.g., Norberg et al., 2007) and implications for the development and application of Information Systems for consumer privacy management or protection. To our knowledge, this is the first study after the GDPR introduction, applying a GDPR exercising-oriented approach to identify consumer privacy types in a representative sample of the German online population.

The paper is structured as follows: The next section provides an overview of related work. Afterward, we introduce our data and methodology, including our survey design. Then, we present our empirical results, followed by a discussion of the implications of our findings and potential limitations. We conclude by summarizing our findings.

# 2 Related Work

An overarching definition of privacy and information privacy is an ongoing discussion in the literature. As our work focuses solely on privacy in the context of the GDPR, we rely on the GDPR definition of privacy as being in control over the collection, storage, and use of personal information. This understanding has a long tradition and is in line with several authors, e.g., Altman (1975), Petronio (1991), Stone et al. (1983), Smith et al. (1996), and others. Following this concept, we refer to privacy as information privacy throughout this paper.

There are several studies on the measurement of privacy tendencies and the segmentation of similar consumers based on their privacy tendencies. Preibusch (2013) offers an overview of privacy-related instruments. More recently, Martin et al. (2017) suggest a scale for privacy importance, which we also employ in our survey. However, scales alone hardly capture the entire spectrum of relevant information regarding consumer privacy types and their characteristics. Further attempts to classify consumer privacy types are usually context-specific (regarding privacy regulation regimes, sub-populations, regionality, or intention to measure; see Westin, 2003; Dupree et al., 2016; Elueze and Quan-Haase, 2018); hence, generalizations are not readily possible but offer a starting point for our analysis. Westin (2003) provides one of the first consumer privacy type segmentations based on consumer opinion surveys in the United States. He segments consumers into three privacy categories: fundamentalists, unconcerned, and pragmatists. Fundamentalists (25% of their sample) are highly privacy-oriented, rejecting consumer benefits and seeking legal and regulatory privacy measures. Unconcerned (20%) willingly share personal data. Pragmatists (55%) take a balanced approach, weighing privacy risks and benefits. Westin updated this segmentation in the following years. Table 1 summarizes the privacy types over time, including results from selected authors (see Kumaraguru and Cranor (2005) for a detailed survey of Westin's studies).

Hoofnagle and Urban (2014) criticize Westin's segmentation for several reasons. Firstly, the surveys only consider stated preferences or levels of concern and do not include actual behaviors. Secondly, Westin assumes that pragmatists follow a rational choice model based on the idea of the theoretical homo economicus. Thirdly, pragmatists are a default category, e.g., if respondents do not fit into any other category. Based on a survey from 2012 and applying Westin's segmentation criteria, they report 19% fundamentalists, 56% pragmatists, and 16% unconcerned[1]. They conclude that Westin's fundamentalists are instead "privacy resilient" because their privacy knowledge is high or they are willing to engage in privacy protection activities. Furthermore, they describe Westin's *privacy*

[1] The remainder failed at least one screening question. The numbers do not add up to 100%, as the authors exclude these cases.

*pragmatists* as "privacy vulnerable" because these respondents are less knowledgeable and less likely to protect their privacy actively. We address these concerns by not focusing on preferences but on motivational factors for intention, action, and prevention and by considering all privacy types from these studies for interpreting our clustering results.

| **Authors** | | **Westin** | **Westin** | **Westin** | **Hoofnagle & Urban[1]** | **Dupree et al.** |
|---|---|---|---|---|---|---|
| **Year of the survey** | | 1995 | 1999 | 2001 | 2012 | 2016 |
| **Privacy types** | **Fundamentalists** | 25% | 25% | 34% | 19% | 6% |
| | **Unconcerned** | 20% | 22% | 8% | 16% | 16% |
| | **Pragmatists** | 55% | 53% | 58% | 56% | 78% |

*Table 1. Development of the share of privacy types over time in Westin's and related studies. Based on Kumaraguru and Cranor (2005) and Westin (2003).*

Elueze and Quan-Haase (2018) focus on the online privacy attitudes of older Canadian adults (65+ years). They take an interview-based approach (n = 40), identifying five privacy types: privacy fundamentalists (13%), intense pragmatists (15%), marginally concerned (25%), relaxed pragmatists (42%), and cynical experts (5%). This is in contrast to our approach based on empirical data. Dupree et al. (2016) propose to use security and privacy attitudes and behaviors to perform a cluster analysis for privacy personas. They identify five distinct privacy types: fundamentalists, lazy experts, technicians, amateurs, and marginally concerned. Our study uses a similar bottom-up clustering approach to identify privacy types and extends their work by adding the concept of consumers' intentions and abilities to act. Hann et al. (2007) perform a choice-based experiment deriving privacy types and respective dollar amounts for private data. They rely on a sample from the United States and Singapore, suggesting three privacy types: privacy guardians, information sellers, and convenience seekers. Their results are insightful regarding the tradeoff between privacy protection and financial gains.

Besides clustering or segmentation practices, privacy research offers insights into motivational factors and incentive systems to share personal data. On the one hand, motivational factors and incentive systems are highly relevant to companies relying on shared data and respective consumer behavior. On the other hand, this research is paramount in deriving conclusions concerning the regulation of privacy and data-gathering practices.

A major challenge for consumer privacy research is the observation of differing intended and actual privacy behaviors. Berendt et al. (2005) and Norberg et al. (2007) refer to this as the "privacy paradox". Furthermore, the abovementioned studies by Westin (2003) and others provide evidence that privacy preferences are evolving (see Table 1). Goldfarb and Tucker (2012) find that survey participants provided less information in 2008 compared to 2001. In the social media context, Stutzman et al. (2013) show a similar decreasing sharing effect among Facebook users. However, over time, Facebook users share more information with Facebook itself, third-party apps, and advertisers. The authors argue that this might indicate Facebook's capability of manipulating the contexts of privacy decisions in such a way that it is advantageous for Facebook.

From a practical perspective, the hypothesis of temporally evolving privacy preferences is intuitive, as consumers constantly adjust their behaviors to companies' privacy practices and vice versa. Additionally, general awareness of data privacy-related issues and corresponding public education might affect consumer behavior. Regarding the evolution of consumer privacy behaviors over time and the potential effects of the GDPR introduction, Presthus and Sørum conducted several consumer surveys in Norway. Presthus and Sørum (2019) find that consumers report an improved knowledge about information privacy because of GDPR. However, most participants do not show the need to execute new GDPR rights and trust companies with their personal data. Sørum and Presthus (2021) report that the GDPR introduction did not alter the level of consumer awareness or level of control over personal data. Most respondents in this study report that they might execute newly gained rights of personal data deletion, portability, and access. Studies by Presthus and Sørum provide valuable insights into the GDPR effects on consumers but do not derive consumer privacy types or clusters. We thus extend their

exercise-oriented approach with the differentiation between intention, action, and prevention and combine it with privacy type clustering based on consumers' intention and ability to act.

Summarizing this section, Acquisti et al. (2015) postulate the main challenges to the privacy debate. Firstly, consumers are uncertain about the potential consequences of privacy-related behaviors and their preferences regarding those consequences. Secondly, privacy is either context-specific or lacks context. Thirdly, privacy concerns are malleable and not static. Therefore, we suggest that privacy studies about consumer preferences can only provide a snapshot of privacy preferences in a respective context and population. Nevertheless, these snapshots provide valuable insights into privacy preferences, guiding practitioners, researchers, and regulators. In the following, we provide insights into the current state of privacy preferences of different consumer privacy types in the context of the GDPR in Germany.

# 3 Data and Methodology

## 3.1 Survey design and setup

Following Lowry et al. (2017), we implemented a quantitative online survey targeting the German online population to investigate privacy types and motivational factors for data sharing. Hence, we designed the survey in German and translated constructs used in the survey using the back-translation method by evaluating three translations (two native speakers and a machine translation tool) in both directions (Brislin, 1970; Douglas and Craig, 2007). In the first section of the survey, we queried standard demographic and sociographic questions like age, gender, level of education, occupational status, household income, and private Internet usage time. We followed good research practice by reusing established scales wherever suitable (Jenkins and Solomonides, 2000); e.g., we investigated the (online) shopping behavior of participants with the "involvement with shopping" scale by Albrecht et al. (2017). This scale consists of four seven-point Likert-type items that measure how important, engaging, and fun shopping is for respondents. Querying standard demographics and established scales allows us to control for them and establish a basis for future study comparisons (Lowry et al., 2017).

The main section of the survey focused on privacy behavior regarding consumers' *intentions* and *actions* to change privacy settings and share data. We reused two established scales measuring latent constructs, namely "Privacy importance" and "Knowledge of the product class", as the foundation for the privacy type clustering (see Section 3.3). The privacy importance scale consists of four seven-point Likert-type items and measures participants' sensibility, importance, and anxiety associated with the subject of privacy (Martin et al., 2017). We employed this scale as we expect consumers with higher privacy importance have a higher *intention to act* and to protect their privacy. Contrarily, consumers with lower privacy importance are less interested in protecting their privacy (e.g., Chai et al., 2009). We adopted the knowledge of the product class scale by Kelting et al. (2017), to ask for knowledge of the GDPR. The scale is generic and adaptable to different product classes. Our adopted instrument consists of three seven-point Likert-type items asking for familiarity with the GDPR, an assessment of the personal GDPR knowledge, and an estimate of the personal GDPR knowledge compared to the rest of the population. The scale aims to mitigate the effect of unrealistic optimism (Weinstein and Klein, 1996) through the population comparison item. We intentionally excluded the product attributes item from the original scale, as it does not fit in the context of the GDPR. We employed this scale as we expect that consumers with higher GDPR knowledge have a higher *ability to act* and to exercise their GDPR-given rights. Accordingly, consumers with lower GDPR knowledge are less able to execute their rights and protect their privacy.

The survey mimics the typical thought and action process of consumers handling their privacy settings and eventually deleting personal data in the context of an online service. Therefore, the structure of the survey follows the order of (1) intention and (2a) action or (2b) prevention of action. Regarding intentions (1), we asked participants if, how often, and why they intended to change privacy settings or request the deletion of personal data. Next, regarding the actions (2a), we queried if and how often participants actively changed privacy settings or requested the deletion of personal data. Additionally, we asked participants for their reasons for performing either action. Regarding the prevention of

action (2b), we asked participants which reasons prevented them from changing privacy settings or requesting the deletion of personal data.

To investigate motivational factors, we asked for reasons to relax privacy settings, which might involve sharing more personal data, using a seven-point Likert-type scale on six possible reasons. Using the same scale, we queried the trust in recommendations of four entities regarding privacy settings. Finally, we asked the participants to estimate the monthly time they are willing to spend adapting privacy settings for seven distinct incentive reasons.

Throughout the survey, we implemented two instructional manipulation checks to increase the quality of the results, one after the first section and one towards the end of the survey (Oppenheimer et al., 2009). We screened out participants who failed to answer one of those questions correctly and excluded their dataset from the following analysis. Implementing such instructional manipulation checks does not threaten the results' validity (Kung et al., 2018). For questions with predefined answers, we always asked for qualitative feedback by showing an "other"-option. Due to little response and simplicity, we do not present these results in the tables of Section 4.

## 3.2 Sample descriptive statistics and latent constructs

In cooperation with a market research company that acquired our representative sample, we ran the survey over 18 days from the 3rd to the 21st of March 2022. In total, 943 people started the survey; however, 354 either decided not to complete it or failed at least one attention check. Hence, we collected data from 589 successful participations. The final sample is representative of the German online population regarding age and gender distributions (see Table 9 in the Appendix). Additionally, we collected a diverse set of participants regarding other demographic and sociographic attributes. The mean age was 43.6 years, which is in line with the average German Internet user. The level of education was slightly higher than the population average, with 31.3% of participants having a university degree (18.5% in 2019; German Federal Statistical Office, 2020); 63% were regularly working, and 9.5% were students. In our sample, 40.7% were married, and 48.4% were single. Household sizes differed from 1 to 6 or more persons with a median size of 2 persons. In the sample, the median number of children in participants' households was 1. The household income varied from less than 20,000 euros to more than 150,000 euros, with a median range of 20,000 to 40,000 euros. Regarding the detailed results of the scales (i.e., involvement with shopping, privacy importance, and knowledge of the GDPR), aggregated categorical variables and statistics to other scales, refer to Table 3 in Section 4.1.

We computed Cronbach's alpha α to evaluate the reliability of the three latent constructs measured with the scales implemented in our survey. Although other measures exist to evaluate construct reliability, we took the path of comparability. Doing so allows for comparison with the original publications on these scales. Overall, Table 2 shows excellent levels (> .90) of α (Nunnally and Bernstein, 1994) for the constructs and similar levels compared to the original studies. Thus, we infer that the constructs can inform further analyses in our study.

| Latent construct | Cronbach's alpha in this study | Cronbach's alpha in the original study | Original study |
|---|---|---|---|
| Involvement with shopping | .95 | study 1a: .90<br>study 1b: .92 | Albrecht et al. (2017) |
| Privacy importance | .91 | .94 | Martin et al. (2017) |
| Knowledge of the GDPR (adopted from product class knowledge) | .92 | .89 | Kelting et al. (2017) |

*Table 2. Cronbach's alpha of latent constructs.*

## 3.3 Clustering and group differences

Following previous studies on privacy types (e.g., Dupree et al., 2016), we applied k-means clustering to identify our privacy types. We chose this method over other clustering approaches as, besides the

comparability with previous studies, k-means clustering has the benefit of requiring no prior assumptions about the clusters and the possibility of choosing different starting positions for cluster centers (which we did to assess the robustness of the clustering). We used the two latent constructs of privacy importance and knowledge of the GDPR as input vectors to retrieve distinct groups of participants with similar stated characteristics regarding the two scales. Unlike other studies (e.g., Roßnagel et al., 2014), we performed the analysis based on intention- and ability-related scales, not demographics. We treat the two scales as endogenous variables, allowing us to investigate differences between the clusters in participants' demographics and other variables. Further, it allows for verifying the coherence and robustness of the scale results by comparing them with other variables collected in the survey, e.g., variables regarding intention, action, and prevention.

We sequentially performed the k-means clustering with up to 8 clusters. Every time we calculated the mean distances of participants' input vectors to their respective cluster centers. We used the elbow criterion as a heuristic to determine the final number of clusters. We found a visible discontinuity at four clusters in the graph of mean distances and mean standard deviations of distances. In Figure 1, we marked this "elbow" in orange on both the mean distance and the standard deviation of distances. Hence, we decided to use the four-group clustering to determine the privacy types. The clustering allows testing for differences between the privacy types. For all tables in Section 4, we adhere to non-parametric tests and calculated independent samples Kruskal-Wallis 1-way ANOVAs to determine significance levels, including pairwise Mann-Whitney U tests. For the comparison of *intention* and *action*, we applied related-samples McNemar tests. We highlight significant results in Section 4 with asterisks.

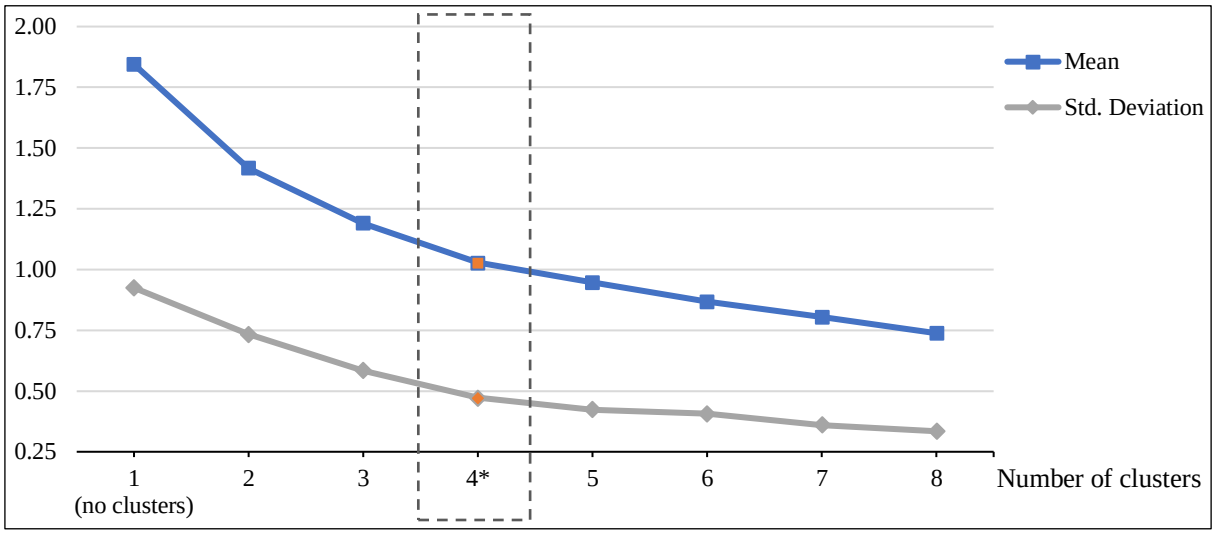



*Figure 1. Mean distances of observations from their cluster centers and within cluster mean standard deviations.*

# 4 Empirical Results

## 4.1 Consumer privacy types

Our clustering approach results in four distinct privacy types. The cluster criteria, i.e., the "privacy importance" scale as the *intention to act* and the "knowledge of GDPR" scale as the *ability to act*, exhibit significant differences between clusters. The clustering groups respondents according to low privacy importance and low knowledge (Cluster 1), high knowledge and relatively low privacy importance (Cluster 2), relatively low knowledge but high privacy importance (Cluster 3), and high knowledge and high privacy importance (Cluster 4). Given these observations, we derive privacy-related labels for each cluster in relation to the abovementioned studies from Westin (2003) and Dupree et al. (2016), e.g., we refer to Cluster 1 as "unconcerned" (n = 90; 15.3% of the sample), Cluster 2 as "pragmatists" (141; 23.9%), Cluster 3 as "amateurs" (157; 26.7%) and Cluster 4 as "fundamentalists" (201; 34.1%). A direct

comparison of the group sizes from our study to former studies is not feasible because the clustering method and the number of clusters differ. However, we find support for the fact that privacy is important or very important for most respondents in our sample, e.g., privacy importance is only neutral in Cluster 1, with a mean of 2.97. There are also significant differences between clusters for other descriptive factors. From Table 3, e.g., amateurs (Cluster 3) and fundamentalists (Cluster 4) exhibit a higher mean age than unconcerned (Cluster 1) and pragmatists (Cluster 2). Pragmatists (Cluster 2) and fundamentalists (Cluster 4) have a higher portion of respondents with university degrees, a higher portion of occupational status "working", and higher median income, e.g., fundamentalists (Cluster 4) are only slightly below the higher income bracket. In addition, these two clusters report higher GDPR knowledge. There are significantly more men in pragmatists (Cluster 2), whereas amateurs (Cluster 3) have a higher female proportion. We do not observe evidence for group differences regarding the scale "involvement with shopping" or private time spent on the Internet. The consumer privacy types allow us to investigate privacy behavior and motivational factors for data disclosure, revocation, and deletion in more detail in the following section.

| **Cluster demographics** | | **Cluster** | | | | **Total sample** |
|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | |
| Observations n (in %) | | 90 (15.3) | 141 (23.9) | 157 (26.7) | 201 (34.1) | 589 (100.0) |
| Knowledge of GDPR scale (cluster center) | Mean** | 2.06 | 4.49 | 2.33 | 4.91 | 3.69 |
| | Std. | .80 | .84 | .79 | .87 | 1.50 |
| Privacy importance scale (cluster center) | Mean** | 2.97 | 4.00 | 5.69 | 6.11 | 5.01 |
| | Std. | 1.01 | .75 | .75 | .68 | 1.42 |
| Age (in years) | Mean** | 36.4 | 40.1 | 47.1 | 46.6 | 43.6 |
| | Std. | 15.4 | 13.7 | 15.5 | 13.7 | 15.0 |
| Gender (in %) (** if excluding "diverse") | male | 50.0 | 58.2 | 38.5 | 54.7 | 50.5 |
| | female | 50.0 | 40.4 | 61.5 | 45.3 | 49.1 |
| | diverse | - | 1.4 | - | - | .4 |
| Education (in %)** | university degree | 18.9 | 39.3 | 23.1 | 37.8 | 31.3 |
| | no university degree | 81.1 | 60.7 | 76.9 | 62.2 | 68.7 |
| Occupational status (in %)** | working | 46.6 | 71.4 | 53.9 | 71.2 | 63.0 |
| | not working | 53.4 | 28.6 | 46.1 | 28.8 | 37.0 |
| Income range (in k euro) | Median | 20-40 | 40-60 | 20-40 | 20-40 | 20-40 |
| Involvement with shopping scale | Mean | 4.1 | 4.3 | 4.3 | 4.3 | 4.3 |
| | Std. | 1.63 | 1.55 | 1.82 | 1.71 | 1.69 |
| Private Internet time (in hours per day) | Mean | 4.2 | 3.9 | 3.6 | 3.7 | 3.8 |
| | Std. | 3.1 | 2.9 | 2.6 | 3.0 | 2.9 |

*Table 3. Demographics per identified cluster.*
*Cluster description 1: unconcerned, 2: pragmatists, 3: amateurs, 4: fundamentalists.*
*Between-group difference significance ** at $p < 0.01$, * at $p < 0.05$.*

## 4.2 Consumer privacy behavior and motivational factors

This section presents findings on consumer privacy behavior and motivational factors for data disclosure, revocation, and deletion. Thereby, overarching results for the entire sample and differences between clusters are of interest. Firstly, Table 4 presents the results for which reasons respondents intended to change their privacy settings (row I = intention) and for which reasons they changed their privacy settings (row A = action) in the past. It is possible and feasible that respondents did not have a prior intention to change but still acted. Hence, values from rows "A" might be higher than the corresponding values in rows "I". Overall, more than 85% of respondents have had the intention to change their privacy settings (question 7.I in Table 4), and over 68% have actively changed them (see

7.A in Table 4). This result supports the previous general claim of high privacy importance in our sample. Interestingly, the unconcerned (Cluster 1) show a significantly different pattern, displaying neither intention nor action. Amateurs (Cluster 3) had the intention but did not act. The underlying motivators for intention and action are various, the most common being "Fear/worry of unauthorized access to personal data" (3. in Table 4), especially amateurs (Cluster 3) and fundamentalists (Cluster 4) exhibit this fear. In contrast, a change in privacy policy (4. in Table 4) is foremost relevant for fundamentalists (Cluster 4). An improvement in service or convenience (5. and 6. in Table 4) did not trigger many intentions or actions, only pragmatists (Cluster 2) indicating slightly higher interest.

| **Reasons for privacy change action** (in % of respondents) | **Intention / Action** [a] | **Cluster** | | | | **Total sample** [b] |
|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | |
| 1. For the exclusive receipt of desired advertising. | I | 15.6 | 23.4 | 14.6 | 22.4 | 19.5* |
| | A** | 10.0 | 23.4 | 10.8 | 15.9 | 15.4* |
| 2. Fear/worry of unauthorized access to personal data. | I** | 33.3 | 27.7 | 59.2 | 49.8 | 44.5 |
| | A** | 24.4 | 33.3 | 51.0 | 56.2 | 44.5 |
| 3. Data protection incident, e.g., user data was stolen. | I* | 12.2 | 17.0 | 21.0 | 25.4 | 20.2** |
| | A | 7.8 | 16.3 | 12.1 | 14.9 | 13.4** |
| 4. Privacy policy was changed. | I** | 10.0 | 15.6 | 14.6 | 24.4 | 17.5 |
| | A** | 13.3 | 15.6 | 13.4 | 26.4 | 18.3 |
| 5. Improve the convenience of using the service, e.g., by customizing the service. | I | 11.1 | 16.3 | 7.0 | 10.0 | 10.9 |
| | A* | 7.8 | 17.0 | 7.0 | 12.9 | 11.7 |
| 6. Save time when using the service, e.g., by releasing certain personal data. | I | 13.3 | 18.4 | 12.7 | 15.4 | 15.1** |
| | A | 7.8 | 14.2 | 9.6 | 8.0 | 9.8** |
| 7.I. I have not yet had this intention. / 7.A. I have not actively changed my privacy settings yet. | I** | 30.0 | 14.9 | 14.6 | 8.5 | 14.9** |
| | A** | 60.0 | 24.1 | 36.9 | 20.4 | 31.7** |

*Table 4. Reasons for privacy change action, where I = intention, A = action. Cluster description 1: unconcerned, 2: pragmatists, 3: amateurs, 4: fundamentalists. [a] Between-group difference significance; [b] significance of difference between intention and action (** at p < 0.01, * at p < 0.05).*

For the entire sample, we examined the privacy paradox (e.g., Norberg et al., 2007) by looking at the significance of differences between intention and action for the underlying reasons using related-samples McNemar change tests. There is a significant discrepancy between intention (85%) and action (68%) (see 7. in Table 4), providing evidence for the privacy paradox. Participants show signs of the privacy paradox for better-targeted advertisements (1. in Table 4), data protection incidents (3. in Table 4), and service or convenience improvements (6. in Table 4). Contrarily, there are no signs of the privacy paradox for fear/worry of unauthorized access to personal data (2. in Table 4), a change in privacy policy (4. in Table 4), and an improvement of convenience (5. in Table 4). Though, there might be cluster-specific signs for the privacy paradox, e.g., the unconcerned act less than they intend to act out of fear of unauthorized access to personal data.

Table 5 presents the reasons why participants try to change their settings or delete their data entirely. Overall, almost 65% of respondents tried to delete their data in the past (6. in Table 5). These are fewer respondents than those who intend to change the privacy settings (68%, see Table 4). Thereby, the general protection of privacy is again the most important motivator. However, there are significant group differences in motivators. Interestingly, participants give little importance to data protection incidents for deleting data across all clusters. A reason might be that the deletion would be without effect if an incident has already happened. In addition, the deletion of data for reducing general advertising is of little relevance across clusters.

Additionally, participants reported the frequency of privacy change intentions and actions and the deletion of data over the last year. The median is 1-2 times yearly for privacy change intention and

action. The median for deleting data is 0. Again, the unconcerned (Cluster 1) show signs of the privacy paradox by reporting higher frequencies for intention (1-2 times) than action (0 times). Moreover, there are significant group differences for privacy change intention, action, and deletion frequencies.

| **Reasons for trying to delete data** (in % of respondents) | **Cluster** | | | | **Total sample** |
|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | |
| 1. Protect privacy.** | 30.0 | 27.0 | 45.9 | 53.7 | 41.6 |
| 2. For the exclusive receipt of desired advertising. | 12.2 | 14.9 | 8.3 | 15.9 | 13.1 |
| 3. Fear/worry of unauthorized access to personal data.** | 12.2 | 21.3 | 31.8 | 37.3 | 28.2 |
| 4. Data protection incident, e.g., user data was stolen. | 5.6 | 14.2 | 15.3 | 14.9 | 13.4 |
| 5. Ensure deletion of personal data after account deletion. | 16.7 | 23.4 | 26.1 | 27.9 | 24.6 |
| 6. I have never tried this before.** | 51.1 | 37.6 | 37.6 | 25.4 | 35.5 |

*Table 5. Reasons for trying to delete data.*
*Cluster description 1: unconcerned, 2: pragmatists, 3: amateurs, 4: fundamentalists.*
*Between-group difference significance ** at 0.01, * at 0.05.*

Table 6 presents factors preventing respondents from changing privacy settings (rows C) or deleting data (rows D). Overall, only 24% and 33% of respondents state that nothing prevents them from changing or deleting data (10. in Table 6). Hence, there are significant barriers to changing privacy settings or deleting data; however, with significant differences between clusters, e.g., pragmatists (Cluster 2) and fundamentalists (Cluster 4) encounter significantly fewer barriers than unconcerned (Cluster 1) and amateurs (Cluster 3).

| **Reasons for preventing privacy changes and deleting of data** (in % of respondents) | | **Cluster** | | | | **Total sample** |
|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | |
| 1. Fear of deterioration of service. | C | 4.4 | 14.2 | 14.0 | 13.4 | 12.4 |
| | D | 4.4 | 11.3 | 15.9 | 12.4 | 11.9 |
| 2. Without shared data, the service does not work. | C* | 20.0 | 33.3 | 38.9 | 34.8 | 33.3 |
| | D* | 12.2 | 22.7 | 28.0 | 24.4 | 23.1 |
| 3. Without shared data, the service becomes chargeable. | C | 5.6 | 13.5 | 16.6 | 16.9 | 14.3 |
| | D | 7.8 | 9.2 | 10.8 | 11.4 | 10.2 |
| 4. Time required to perform the action. | C* | 38.9 | 39.7 | 36.3 | 26.9 | 34.3 |
| | D* | 35.6 | 38.3 | 24.8 | 24.4 | 29.5 |
| 5. I am not aware of the subject. | C** | 22.2 | 5.0 | 11.5 | 8.0 | 10.4 |
| | D* | 12.2 | 6.4 | 10.2 | 3.5 | 7.3 |
| 6. I do not care about the subject. | C** | 20.0 | 5.0 | 2.5 | 4.5 | 6.5 |
| | D** | 17.8 | 4.3 | 3.8 | 6.0 | 6.8 |
| 7. Subject matter is too complicated for me. | C** | 20.0 | 17.0 | 32.5 | 11.4 | 19.7 |
| | D* | 18.9 | 14.2 | 22.9 | 10.4 | 16.0 |
| 8. I do not know how this works. | C** | 16.7 | 6.4 | 22.3 | 10.9 | 13.8 |
| | D** | 23.3 | 6.4 | 28.0 | 9.5 | 15.8 |
| 9. I have postponed or forgotten the assignment. | C | 6.7 | 5.0 | 5.7 | 7.0 | 6.1 |
| | D | 4.4 | 5.7 | 7.6 | 6.0 | 6.1 |
| 10. Nothing is preventing me. | C** | 24.4 | 22.0 | 15.9 | 31.3 | 23.9 |
| | D** | 31.1 | 35.5 | 22.3 | 40.8 | 33.1 |

*Table 6. Reasons for the inaction of privacy change or data deletion, where C = preventing change, D = preventing deletion.*
*Cluster description 1: unconcerned, 2: pragmatists, 3: amateurs, 4: fundamentalists.*
*Between-group difference significance ** at 0.01, * at 0.05.*

Also, participants report higher barriers to changing privacy settings than barriers to deleting personal data (10. in Table 6). There seem to be significant knowledge barriers preventing unconcerned (Cluster 1) and amateurs (Cluster 3) from performing described actions, as the subject matter is too complicated (7. in Table 6), and they do not know how this works (8. in Table 6). Additionally, unconcerned (Cluster 1) is the only cluster not interested in the subject (6. in Table 6). In general, respondents assume that without shared data, used services are not working (2. in Table 6), but also performing privacy actions requires time (6. in Table 6). Interestingly, potential fees for the service (3. in Table 6) or the deterioration of service (1. in Table 6) do not prevent respondents from acting.

Table 7 summarizes the reasons that motivate consumers to relax their privacy settings or to share more data. Table 6 shows that potential fees for using the service (3. in Table 6) or the deterioration of service (1. in Table 6) do not prevent respondents from acting. However, improved service (3. in Table 7) and monetary incentives in the form of discounts (5. in Table 7) or avoiding fees (6. in Table 7) might motivate consumers to relax privacy settings and share more data. Tailoring services (2. in Table 7) or tailoring advertisements (1. in Table 7) seem less effective. Only pragmatists (Cluster 2) seem to be generally inclined to persuasion regarding relaxation. In that sense, individuals from this group are also convenience seekers, as described by Hann et al. (2007). Also, unconcerned (Cluster 1) might be information sellers susceptible to monetary incentives (Hann et al., 2007).

| **Motivation to relax privacy settings and share more data** | | **Cluster** | | | | **Total sample** |
|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | |
| 1. Tailored advertising. | Mean** | 2.51 | 3.01 | 2.53 | 2.38 | 2.59 |
| | Std. | 1.67 | 1.70 | 1.81 | 1.80 | 1.77 |
| 2. Tailored services (better performance). | Mean* | 3.72 | 4.11 | 3.78 | 3.52 | 3.76 |
| | Std. | 1.87 | 1.74 | 1.90 | 2.00 | 1.90 |
| 3. Improved service (more services). | Mean* | 3.97 | 4.27 | 3.84 | 3.71 | 3.92 |
| | Std. | 1.91 | 1.79 | 1.90 | 1.95 | 1.90 |
| 4. Save time when using the service (improved convenience). | Mean** | 3.94 | 4.26 | 3.88 | 3.49 | 3.85 |
| | Std. | 1.82 | 1.71 | 1.94 | 1.98 | 1.90 |
| 5. Discounts/rebates (more favorable services). | Mean** | 4.59 | 4.72 | 4.29 | 3.74 | 4.25 |
| | Std. | 1.85 | 1.76 | 1.98 | 2.00 | 1.95 |
| 6. Avoid the obligation to pay for the service (free service) | Mean** | 4.76 | 4.65 | 4.55 | 3.81 | 4.35 |
| | Std. | 1.85 | 1.68 | 1.86 | 1.96 | 1.89 |

*Table 7. Motivation to relax privacy settings and share more data. Based on a Likert scale from (1) strongly disagree to (7) strongly agree. Cluster description 1: unconcerned, 2: pragmatists, 3: amateurs, 4: fundamentalists. Between-group difference significance ** at $p < 0.01$, * at $p < 0.05$.*

We asked participants how much time they are willing to invest regarding privacy changes or privacy management to receive certain benefits, such as tailored advertising or services, improved service, or monetary incentives (see 1. to 6. from Table 7). Overall, 36% of respondents are unwilling to invest any time, and 44% are willing to invest less than one hour per week. Only 20% are willing to invest more than one hour per week. Respondents are willing to invest the most time to improve privacy in general (45% less than one hour and 32.5% more than 1 hour). In addition, monetary incentives are potential motivators for participants to invest time; e.g., 46% of respondents are willing to invest less than an hour and 26% more than one hour per week to receive discounts/rebates. Avoiding fees for a service motivates 49% of respondents to invest less than one hour and 23% to invest more than one hour per week. However, there are significant differences between the clusters. In line with results from Table 7, respondents are not willing to invest time in tailored services and especially not in tailored advertising.

Table 8 summarizes respondents' trust towards privacy recommendations of different entities. Respondents place the highest trust in consumer protection organizations, whereas platform operators

are the least trusted. Interestingly, only fundamentalists (Cluster 4) trust their judgment more than the recommendation of independent data protection experts.

| Trusted entities' privacy recommendations | | Cluster | | | | Total sample |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | |
| Consumer protection organizations | Mean** | 4.91 | 5.35 | 5.64 | 5.69 | 5.48 |
| | Std | 1.76 | 1.40 | 1.47 | 1.39 | 1.50 |
| Platform operators | Mean | 2.98 | 3.31 | 3.22 | 3.13 | 3.17 |
| | Std | 1.61 | 1.34 | 1.71 | 1.68 | 1.60 |
| Independent data protection experts | Mean** | 4.28 | 4.96 | 5.05 | 5.18 | 4.95 |
| | Std | 1.70 | 1.33 | 1.67 | 1.56 | 1.58 |
| Own / self-defined settings | Mean** | 4.01 | 4.94 | 4.60 | 5.22 | 4.80 |
| | Std | 1.70 | 1.24 | 1.66 | 1.46 | 1.56 |

*Table 8. Trusted entities' privacy recommendations. Based on a Likert scale from (1) strongly disagree to (7) strongly agree.*
*Cluster description 1: unconcerned, 2: pragmatists, 3: amateurs, 4: fundamentalists.*
*Between-group difference significance ** at $p < 0.01$, * at $p < 0.05$.*

# 5 Discussion, Implications, and Limitations

Several years have passed since the GDPR introduction. We can assume that our results reflect a more mature state of consumer privacy understanding than previous studies, as the GDPR introduced more restrictive privacy-preserving measures that all European Union (online) consumers have been exposed to. Therefore, it is not surprising that our survey results indicate a high level of privacy awareness and a relatively high level of GDPR knowledge amongst German online consumers. However, convenience and monetary incentives remain important factors, e.g., consumers are unwilling to spend much time and effort dealing with privacy-related issues or the subject of privacy in general. On the one hand, we find notable differences between intentions to change and actual changes in privacy settings for some motivators. Generally, these observations might indicate the privacy paradox, i.e., the misalignment of intentions and actions. On the other hand, for other motivators, participants do not show signs of the privacy paradox. These findings might provide evidence for the hypotheses from Norberg et al. (2007) that action-based regulation or consent might lower the privacy paradox. By default, the GDPR regulates many data collection and usage permissions online consumers face. Therefore, the GDPR introduction might already show some effect, as consumers now indicate a high awareness of the topic and partially act accordingly. However, these mixed results reveal the need for a deeper understanding of motivators and contexts influencing the appearance and amplitude of the privacy paradox.

From a consumer's perspective, privacy systems should be effortless or private by default, as the low amounts of time consumers are willing to spend managing their privacy settings suggest; future research should investigate how to implement effortless management of GDPR-related rights. Firms should design services that do not strongly depend on private data. However, firms wanting to gather more consumer data should ensure that consumers understand its need, e.g., by offering services that specifically depend on the required data. Additionally, monetary incentives or the selling of personal information does work for some consumers. In contrast, tailoring existing services or tailored advertising does not justify more data gathering in the eyes of most consumers from our survey. This finding has implications, especially for practitioners, e.g., from social media. Social media advertises tailored advertisements and more tailored experiences as a value proposition (see Meta example, Figure 2 in the Appendix). However, this might not justify more data collection for most consumers. Generally, consumers place varying trust in privacy recommendations of third-party entities, trusting consumer protection agencies most. This observation might be a good indicator and starting point for practitioners to foster trust with consumers, e.g., how to incorporate trusted third parties in ecosystems to make data sharing more reliable and trustworthy for consumers.

Regarding consumer privacy type clustering, Westin's (2003) three groups are overly simplistic and do not offer enough differentiation. Moreover, we could not identify the five suggested clusters by Dupree et al. (2016). Combining these, we suggest four privacy clusters for our sample by confirming Westin's clusters and adding the amateur cluster suggested by Dupree et al. (2016). We derived our privacy clusters following a best-practice data science clustering methodology. Our sample has a relatively large proportion of fundamentalists and amateurs compared to previously mentioned studies. The applied clustering approach does not require any assumptions regarding potential consumer types or segments beforehand and provides much flexibility. This flexibility has the disadvantage of making comparisons over time and different samples less reliable, as cluster affiliation is relative and depends on the sample itself. We encourage developing and applying standardized scales and clustering approaches to increase comparability between studies, populations, and over time. The desired clustering methodology should offer enough flexibility to account for potential changes in the privacy context and require few prior assumptions. For this, future research should experiment with different clustering approaches to verify the robustness of the results across different approaches. In this regard, defining absolute levels of privacy knowledge and importance is the most crucial challenge. One step can be to replace self-reported scales on privacy knowledge, which we had to use due to a lack of alternatives, with objective scales measuring the knowledge of the GDPR or, more generally, of the privacy topic as objectively as possible. This approach might help generate more objective clustering results and address potential biases, such as the Dunning-Kruger effect (Dunning, 2011), overconfidence bias (Moore and Healy, 2008), unrealistic optimism (Weinstein and Klein, 1996) or social desirability bias (Fisher, 1993). Also, including standard personality trait tests from related research fields, such as psychology, might add further insights and increase comparability. Measuring and comparing privacy perception and preferences over time and across populations is necessary to guide practitioners, researchers, and regulators. On the one hand, a deeper understanding of consumer privacy types helps the understanding of consumer incentives regarding their use of data-sharing platforms and, on the other hand, helps to improve the design of privacy-protecting Information Systems.

Besides the potential limitations mentioned above (i.e., the use of only one clustering methodology and self-reported data, generally, the use of more standardized scales, and the cited biases), our research faces common limitations of research with similar methodology. First, the results are not inherently generalizable as the findings only apply to the current state of the German online population. Also, sample sizes could always be increased. Second, although from a representative sample regarding age and gender, the results might face sample selection biases as, for example, privacy-concerned people might not participate in anonymous online studies.

# 6 Conclusion

This is the first study introducing a GDPR exercising-oriented approach to identify privacy consumer types. Based on a representative sample of the German online population, we cluster consumers according to their privacy importance (*intention to act*) and GDPR knowledge (*ability to act*), deriving four privacy type clusters: fundamentalists, amateurs, pragmatists, and unconcerned. The GDPR introduced restrictive privacy-preserving measures affecting the daily life of (online) consumers. Therefore, we assume that our results reflect a more mature state of consumer privacy understanding than previous studies. We find strong evidence that consumers value privacy for our sample and consumer privacy types. However, convenience and monetary incentives remain essential requirements, as consumers do not want to invest too much time and effort into the privacy subject. We find mixed results regarding the presence and amplitude of the privacy paradox. The level of divergence between intention and action varies across motivational factors. Therefore, the current state of the privacy paradox remains inconclusive. The hypothesis that action-based regulation or consent (like the GDPR) weakens the privacy paradox requires further empirical investigation. Our clustering of privacy types reveals common patterns with existing research and generates new insights into consumer privacy types. Our privacy type clustering results provide valuable insights into implications and requirements for using or developing Information Systems for consumer privacy management or protection. Time will

tell how stable consumer preferences remain, especially as companies increasingly compete on privacy and engage in public privacy communication. We assume this might ultimately influence consumers' privacy perceptions and preferences. Therefore, we suggest the development of standardized scales and corresponding clustering methodologies to enable researchers, practitioners, and regulators alike to investigate consumer privacy perception and preferences over time and in different populations.

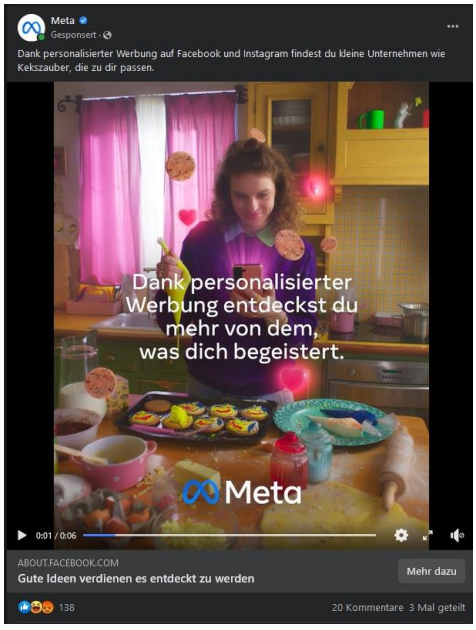
## Remarks and Acknowledgments

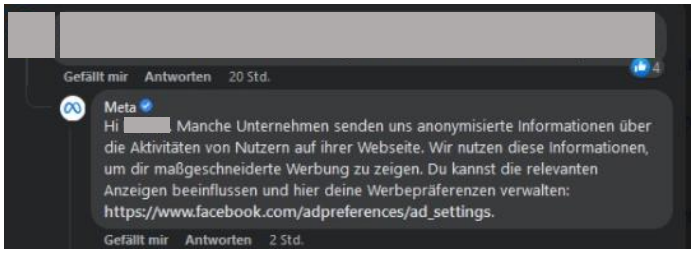
We want to express our sincere gratitude to the German Federal Ministry of Education and Research for their generous funding support through the PERISCOPE project (funding number: 16KIS1480). This support enabled us to conduct our research. We also extend our appreciation to our colleagues from the PERISCOPE project, who provided invaluable feedback and advice throughout the process of conducting this research. Their contributions were essential to the success of this study.

## Appendix

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

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




Translation of top screenshot:
Meta – Hi [username], some companies send us anonymized information about users' activity on their websites. We use this information to display tailored ads to you. You can influence the relevant ads and manage your advertising preferences here: *LINK*

Translation of left screenshot:
Thanks to personalized advertising, you discover more of what excites you.

*Figure 2. Meta advertisement example (retrieved on July 07, 2022, from personal Meta timeline). Note: The authors did not interact with the displayed Meta ad; however, other users did.*

## References

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). "Privacy and human behavior in the age of information", *Science (New York, N.Y.)* 347 (6221), 509–514.

Albrecht, C.-M., Hattula, S., and Lehmann, D. R. (2017). "The relationship between consumer shopping stress and purchase abandonment in task-oriented and recreation-oriented consumers", *Journal of the Academy of Marketing Science* 45 (5), 720–740.

Altman, I. (1975). "The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Monterey".

Berendt, B., Günther, O., and Spiekermann, S. (2005). "Privacy in e-commerce", *Communications of the ACM* 48 (4), 101–106.

Brandimarte, L., Acquisti, A., and Loewenstein, G. (2013). "Misplaced Confidences", *Social Psychological and Personality Science* 4 (3), 340–347.

Brislin, R. W. (1970). "Back-Translation for Cross-Cultural Research", *Journal of Cross-Cultural Psychology* 1 (3), 185–216.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., and Upadhyaya, S. J. (2009). "Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens", *IEEE Transactions on Professional Communication* 52 (2), 167–182.

Douglas, S. P. and Craig, C. S. (2007). "Collaborative and Iterative Translation: An Alternative Approach to Back Translation", *Journal of International Marketing* 15 (1), 30–43.

Dunning, D. (2011). "The Dunning–Kruger Effect", in: M. P. Zanna and J. M. Olson (eds.) *Advances in Experimental Social Psychology*. 1. Aufl., 247–296. s.l., Elsevier textbooks.

Dupree, J., Devries, R., Berry, D., and Lank, E. (2016). "Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices", in: J. Kaye and A. Druin (eds.) *CHI '16: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5228–5239. New York, NY, The Association for Computing Machinery.

Elueze, I. and Quan-Haase, A. (2018). "Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin's Privacy Attitude Typology Revisited", *American Behavioral Scientist* 62 (10), 1372–1391.

Federal Statistical Office (2020). *Educational attainment of the population in Germany*. URL: https://www.destatis.de/EN/Themes/Society-Environment/Education-Research-Culture/Educational-Level/Tables/educational-attainment-population-germany.html (visited on November 03, 2022).

Fisher, R. J. (1993). "Social Desirability Bias and the Validity of Indirect Questioning", *Journal of Consumer Research* 20 (2), 303.

Goldfarb, A. and Tucker, C. (2012). "Shifts in Privacy Concerns", *American Economic Review* 102 (3), 349–353.

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

Hoofnagle, C. J. and Urban, J. M. (2014). "Alan Westin's Privacy Homo Economicus", *Wake Forest Law Review* 49 (2), 261–318.

Jenkins, S. and Solomonides, T. (2000). "Automating Questionnaire Design and Construction", *International Journal of Market Research* 42 (1), 1–13.

John, L. K., Acquisti, A., and Loewenstein, G. (2011). "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information", *Journal of Consumer Research* 37 (5), 858–873.

Kelting, K., Duhachek, A., and Whitler, K. (2017). "Can copycat private labels improve the consumer's shopping experience? A fluency explanation", *Journal of the Academy of Marketing Science* 45 (4), 569–585.

Kumaraguru, P. and Cranor, L. F. (2005). "Privacy Indexes: A Survey of Westin's Studies".

Kung, F. Y., Kwok, N., and Brown, D. J. (2018). "Are Attention Check Questions a Threat to Scale Validity?", *Applied Psychology* 67 (2), 264–283.

Lowry, P. B., Dinev, T., and Willison, R. (2017). "Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda", *European Journal of Information Systems* 26 (6), 546–563.
Martin, K. D., Borah, A., and Palmatier, R. W. (2017). "Data Privacy: Effects on Customer and Firm Performance", *Journal of Marketing* 81 (1), 36–58.
Moore, D. A. and Healy, P. J. (2008). "The trouble with overconfidence", *Psychological review* 115 (2), 502–517.
Norberg, P. A., Horne, D. R., and Horne, D. A. (2007). "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", *Journal of Consumer Affairs* 41 (1), 100–126.
Nunnally, J. C. and Bernstein, I. H. (1994). *Psychometric theory*. 3rd Edition. New York, NY: McGraw-Hill.
Oppenheimer, D. M., Meyvis, T., and Davidenko, N. (2009). "Instructional manipulation checks: Detecting satisficing to increase statistical power", *Journal of Experimental Social Psychology* 45 (4), 867–872.
Petronio, S. (1991). "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples", *Communication Theory* 1 (4), 311–335.
Preibusch, S. (2013). "Guide to measuring privacy concern: Review of survey and observational instruments", *International Journal of Human-Computer Studies* 71 (12), 1133–1143.
Presthus, W. and Sørum, H. (2019). "Consumer perspectives on information privacy following the implementation of the GDPR", *International Journal of Information Systems and Project Management* 7 (3), 19–34.
(2016). *Regulation (EU) 2016/679 (General Data Protection Regulation). Regulation (EU) 2016/679*.
Roßnagel, H., Zibuschka, J., Hinz, O., and Muntermann, J. (2014). "Users' willingness to pay for web identity management systems", *European Journal of Information Systems* 23 (1), 36–50.
Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", *MIS Quarterly* 20 (2), 167.
Sørum, H. and Presthus, W. (2021). "Dude, where's my data? The GDPR in practice, from a consumer's point of view", *Information Technology & People* 34 (3), 912–929.
Stone, E. F., Gueutal, H. G., Gardner, D. G., and McClure, S. (1983). "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations", *Journal of Applied Psychology* 68 (3), 459–468.
Stutzman, F., Gross, R., and Acquisti, A. (2013). "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook", *Journal of Privacy and Confidentiality* 4 (2).
Weinstein, N. D. and Klein, W. M. (1996). "Unrealistic Optimism: Present and Future", *Journal of Social and Clinical Psychology* 15 (1), 1–8.
Westin, A. F. (2003). "Social and Political Dimensions of Privacy", *Journal of Social Issues* 59 (2), 431–453.