The market for privacy

Eggers, Felix; Beke, Frank T.; Verhoef, Pieter C.; Wieringa, Jaap E.

Published in:
Journal of Interactive Marketing

Publication date:
2022

The market for privacy: Understanding how consumers trade off privacy practices

Felix Eggers [a]

Frank T. Beke [b]

Peter C. Verhoef [c]

Jaap E. Wieringa [d]

[a] Professor, Department of Marketing, Copenhagen Business School, Solbjerg Plads 3, 2000 Frederiksberg, fe.marktg@cbs.dk (Corresponding author)

[b] PhD, Frank T. Beke, De Nieuwe Zaak, Hanzeallee 28, 8017 KZ Zwolle, Netherlands, frank@denieuwezaak.nl

[c] Professor, Department of Marketing, Faculty Economics and Business, University of Groningen, Nettelbosje 2, 9747 AE Groningen, +31 (0)50 363 3686, p.c.verhoef@rug.nl

[d] Professor, Department of Marketing, Faculty Economics and Business, University of Groningen, Nettelbosje 2, 9747 AE Groningen, j.e.wieringa@rug.nl

Acknowledgments: The authors acknowledge the Customer Insight Center from the University of Groningen for funding.

The market for privacy: Understanding how consumers trade off privacy practices

Abstract

In recent years, firms' privacy practices have received increasing attention from consumers. While firms largely see this development as a threat, as consumers might prohibit collection or use of data, we suggest that it can also represent an opportunity for firms. On the "market for privacy" firms can gain a competitive advantage by differentiation and actively promoting preferred privacy practices. In this context, we study how consumers trade off five privacy elements relating to distributive fairness (i.e., information collection, storage, use) and procedural fairness (i.e., transparency, control). Moreover, we analyze how the impact of these elements differs among four industries that vary in information sensitivity and interaction intensity. By using discrete choice experiments, we show that all privacy elements matter to consumers, even when in a trade-off with price. In highly sensitive industries differences in information collection and use matter more while storage matters less for differentiation. When consumers have less frequent interactions with companies, they require more transparency about their privacy practices. We demonstrate empirically that optimizing privacy practices can lead to robust changes in market shares (study 1) and higher revenues in equilibrium (study 2) when firms embrace the market for privacy.

Keywords: Privacy; information collection; information storage; information use; strategy

1. Introduction

Declining costs of gathering and storing consumer data and the growing necessity to harness this data to stay competitive leads to an erosion of consumer privacy (Rust, Kannan, and Peng 2002). The collection of personal information enables firms to understand the needs and preferences of consumers better, thereby generating potential positive consequences for consumers. Major tech firms, such as Google, Amazon and Netflix are now using personalization methods. Also, advertisers use specialized firms to target customers online and on social media. This is, however, not without a risk and can create strong negative publicity and debates, as shown, for example, in the analyses of Facebook profiles done by Cambridge Analytica for the campaign of Donald Trump targeting US voters in the 2016 elections (Cadwalladr and Graham-Harrison 2018). Controversial revelations about privacy and frequent negative publicity about privacy breaches are making consumers also increasingly concerned about the negative consequences of providing information. The potential negative consequences have also been debated when COVID-19 tracking apps have been introduced to monitor the pandemic and inform individuals at risk (Brough and Martin 2021). Accepting to share personal information with companies therefore requires a well-established trade-off of these positive and negative consequences from consumers (Rust and Huang 2014; Acquisti, Brandimarte, and Loewenstein 2015; Beke et al. 2022; Krafft, Arden, and Verhoef 2017).

This trade-off is managerially meaningful. When consumers consider the aforementioned trade-off as unfavorable, they are more likely to refrain from using products and services that are conditional on collecting information. As an example, a study by the Pew Research Center shows that 60% of consumers have chosen to not install a mobile app when the collection of information was too extensive, and 43% have uninstalled a mobile app after finding out about information collection (Olmstead and Atkinson 2015). This implies that consumers are more likely to choose an offer that protects their privacy better, i.e., has a less negative trade-off for consumers (Lee, Ahn, and Bang 2011).

If firms only address minimum legal requirements, e.g., complying to the General Data Protection Regulation (GDPR) in the EU, and offer the same privacy practices there is intense competition among firms in this "market for privacy" (Rust, Kannan, and Peng 2002). In this context, we argue and empirically demonstrate that firms should consider the growing attention for privacy as an opportunity to strategically differentiate from competitors (Goldfarb and Tucker 2013; Bleier, Goldfarb and Tucker 2020). Differentiating on privacy can segment the market effectively, e.g., among privacy unconcerned consumers who prefer lower prices instead and privacy fundamentalists who require more privacy (Hann et al. 2007; Lee, Ahn, and Bang 2011). In this case, differentiation lowers competition and can lead to markets with larger surplus among competitors, while also being beneficial for consumers. Large firms such as Apple and Google already embrace stricter privacy practices although not necessarily required by law to do so (Gurman and Grant 2021). To differentiate, firms need a better understanding of how their privacy practices affect consumers' decisions (Bolton and Saxena-Iyer 2009; Rust and Huang 2014). This trade-off is not trivial to capture as consumers would likely gain larger benefits, e.g., via personalization, when providing more or more sensitive information. This would make this option equally attractive in terms of net utility as sharing less information for smaller benefits.

We contribute to this research field as follows. First, we present an empirical study that measures consumers' trade-offs among options that vary in five privacy practices: 1) information collection, 2) information storage, 3) information use, 4) transparency, and 5) control. We show that each of these privacy practices matters to consumers and demonstrate how a negative utility of a privacy practice can be balanced by a more favorable element of another privacy practice. In a separate empirical study, we confirm that this trade-off also holds next to price, i.e., that consumers are willing to pay a higher price when offered with better privacy options and vice versa. Second, whereas prior work has predominantly assessed the privacy trade-off in one specific industry or context (Zhao, Lu, and Gupta 2012; Sutanto et al. 2013; Premazzi et al. 2010) we differentiate our findings for four industries (banks, insurances, news,

cinemas). These industries differ in terms of information sensitivity (referring to consumers' potential loss when information ends up in the wrong hands) and interaction intensity (referring to how often consumers interact or transact with a firm). For each industry, we highlight market scenarios in which differentiation on privacy can increase market shares and result in higher (equilibrium) market prices and revenues that benefit firms and consumers. In this regard, our results identify competitive privacy elements that have the potential to, at least, slow down privacy erosion.

2. Literature review

Privacy is relevant in a multitude of disciplines, including but not limited to marketing, information systems, management, human resources, medicine, or even transportation, e.g., in the context of autonomous driving. There are several summaries of the existing knowledge in these disciplines in systematic reviews, e.g., (Beke, Eggers, and Verhoef 2018; Bélanger and Crossler 2011; Martin and Murphy 2017; Smith, Dinev, and Xu 2011). In this chapter we focus on exemplary research that addresses the consumer perspective and the trade-off that consumers have to make between positive and negative aspects of sharing data, e.g., the benefit of personalization vs. sharing more personal information.

Already in the early days of Internet there has been attention for personalization and the development of recommender systems in, e.g., the news industry (e.g., Konstan et al. 1997; Resnick and Varian 1997). There is an extensive literature on how data and models can be used to personalize and how recommender systems can be developed in marketing, information systems and computer science (e.g., Verhoef, Kooge, and Walk 2016). Ansari and Mela (2003) develop a statistical and optimization approach for customization of information on the Internet. Chung, Rust and Wedel (2009) develop Bayesian models to personalize music playlist. Within computer science there is extensive attention for the development of models for online personalization (e.g., Adomavicius and Tuzhilin 2005). Beyond

studies considering the development of these systems, researchers have also considered if customer's willingness to use these systems and share data. For example, Kim and Kim (2018) study factors driving the willingness to provide personal information for recommender systems. Al-Natour et al. (2020) study how privacy uncertainty influences the use of mobile apps, which also frequently use personalization techniques. Beke et al. (2022) have developed the PRICAL scale to measure the trade-off between costs and benefits of data-sharing. This research has also gained importance during the Covid-19 epidemic in which Corona tracing apps require access to personal health and location data for a personal and societal benefit (Brough and Martin 2021). Lin (2022) separates a consumer's privacy preference into an intrinsic and an instrumental component and estimates the value of privacy to consumers and the value of consumer data to firms. In sum, there is an extensive amount of literature on privacy, online recommendation and personalization, or how privacy policies affect the attitude towards digital goods. Importantly, there is no research that shows how different privacy elements influence consumers' choices and how the importance of these elements changes depending on the industry of the firm. We address this research gap with our study.

3. Conceptual background

There has been much discussion on how informational privacy[1] should be defined. The most prevalent standpoint is that informational privacy is a matter of autonomy and control over the collection, storage, and use of information (Westin 1967; Petronio 1991; Smith, Milberg, and Burke 1996; Malhotra, Kim, and Agarwal 2004). Recent privacy laws and guidelines in the US and the EU have adopted this standpoint on privacy, as they aim to let consumers decide for themselves what happens with their information. According to this line of thinking, privacy is "*the ability of individuals to control the terms*

[1] Note that our focus is on informational privacy rather than physical privacy. For an extensive discussion on the conceptual nature of privacy, see Stewart (2017).

under which their personal information is acquired, stored, and used" (Culnan and Bies 2003; Smith, Milberg, and Burke 1996).

We refer to social justice theory and divide this definition into privacy elements that relate to privacy outcomes, i.e., distributive fairness (information collection, storage, use), and elements that take the procedures that cause these outcomes into account, i.e., procedural fairness (transparency, control) (Son and Kim 2008; Culnan and Bies 2003; Wirtz and Lwin 2009). In this context, we study how consumers trade off the positive and negative consequences of these five elements of a privacy strategy and how they influence the acceptance of information collection. Specifically, in study 1, we analyze how this trade-off is moderated by industry characteristics. We assess industry characteristics that could aggravate the risks for consumers (information sensitivity) and that could enhance their benefits (interaction intensity). In study 2, we add price to the model to analyze to what extent consumers trade off privacy elements with more salient benefits, i.e., lower prices. Figure 1 summarizes the conceptual model.

===== FIGURE 1 =====

3.1 Consumer trade-off among privacy elements

Many consumer decisions are based on trade-offs, for example between price and quality. When consumers evaluate offerings made by firms they make a trade-off between what they gain (positive consequences) and what they lose (negative consequences) in relation to their status quo (Bolton and Lemon 1999; Ostrom and Iacobucci 1995). Trade-offs among these consequences can be reflected by utility theory or the concept of customer value (Zeithaml 1988). Accordingly, a consumer might consider the loss of anonymity due to the collection, storage, and use of information as negative; while the same consumer could attach a positive utility to the consequence that a firm better understands her needs and preferences leading to better personalized content (Rust and Huang 2014; Acquisti, Brandimarte, and

Loewenstein 2015). Whether the balance of these consequences is positive or negative depends on how strong the consumers weigh the different privacy practices.

Moreover, consumers might compensate negative privacy elements by other benefits that are not related to the data collection, e.g., lower prices. In this regard, it has been shown that consumers are willing to give up their privacy even for small monetary benefits (Athey, Catalini, and Tucker 2017). We therefore also add price to the trade-off (in study 2).

3.1.1 Distributive Fairness

According to distributive fairness in social justice theory a consumer perceives an exchange as fair if the own input is commensurate with the outcomes that the consumer receives by the firm (Wirtz and Lwin 2009), i.e., if the perceived benefits are proportional to the provided personal information. Firms typically employ three type of privacy practices that affect distributive fairness, namely information collection, information storing (processing), and information use (dissemination) (Solove 2006). Information collection refers to a firm's gathering and recording of information about consumers. While prior work has shown that consumers are affected by the amount and type(s) of information a firm collects (Hui, Teo, and Lee 2007; Martin, Borah, and Palmatier 2017; Mothersbaugh et al. 2012), the type of information (and therefore information sensitivity) is often industry- or sector-specific and therefore difficult to change for a firm. Instead, firms have to make a strategic decision about where and how they collect information—that is, actively provided by consumers, passively tracked by firms, or inferred from other information.

Information storage refers to saving the collected information in the firm's database and keeping it available for future use. Consumers generally respond positively when a firm promises "*safer*" storage. For example, consumers are more inclined to choose firms when only authorized personnel has access to information about customers (Hann et al. 2007) and consumers use a personalized mobile app more

often when information about them is stored only locally (Sutanto et al. 2013). More generally, firms could influence consumers' privacy trade-off positively by storing information for a limited amount of time or by storing it anonymously, e.g., via k-anonymity or differential privacy (Jiang, Heng, and Choi 2013; Wieringa et al. 2021; Schneider et al. 2017).

Information use entails that firms process the information they have collected to generate knowledge about their customers. To create value firms can employ this knowledge to tailor their services or content to the needs and preferences of individual consumers (Adomavicius and Tuzhilin 2005; Montgomery and Smith 2009). Consumers generally respond positively to personalized websites (Hauser et al. 2009; Hauser, Liberali, and Urban 2014; Mothersbaugh et al. 2012), services (Chung, Rust, and Wedel 2009; Chung, Wedel, and Rust 2016), and even advertisements and direct mail (Urban et al. 2013).

However, consumers are not always convinced of the positive consequences of personalization. When explicitly asked, consumers oppose personalized marketing content such as banner ads or direct mail (Turow et al. 2009). Justifying personalized marketing content by pointing to increased relevance only convinces consumers to accept information collection in specific circumstances (Schumann, Von Wangenheim, and Groene 2014). Therefore, as consumers seemingly underestimate the added value of personalized content when it is made explicit, whether offering personalization prompts consumers to accept information collection remains unclear.

3.1.2 Procedural Fairness

Consumers also care about *how* distributive fairness is created in an exchange—that is, they require procedural fairness (Donaldson and Dunfee 1994). For example, while personalization might benefit consumers, they might still be dissatisfied when they believe they were not informed sufficiently about the data collection. In line with legislation and the aforementioned definition of privacy, firms can employ two privacy practices that affect procedural fairness: transparency and control (Wirtz and Lwin 2009).

Transparency requires that a firm informs consumers about the collection, storage, and use of personal information. Without transparency consumers cannot know whether their privacy is respected or violated, such that legislators have considered transparency fundamental for privacy. The Federal Trade Commission in the US has traditionally stressed the importance of transparency (Ohlhausen 2014), while transparency is also imposed by the GDPR in the EU. Even though governments enforce transparency, firms have remained reluctant to clearly inform consumers about privacy practices. Many Fortune 100 firms still rate below-average on transparency (Martin, Borah, and Palmatier 2018), and in the past most firms provide transparency by posting long and difficult-to-read privacy statements (McDonald and Cranor 2008). Prior research has shown that perceived transparency makes consumers more cooperative and committed to a firm in general (Son and Kim 2008), and that actual transparency makes consumers feel less vulnerable (Aguirre et al. 2015; Martin, Borah, and Palmatier 2017). Thus, a firm could potentially benefit from being considered proactively transparent about the collection, storage, and use of information. However, firms need to take into account that transparency might also raise awareness or arouse privacy concerns (LaRose and Rifon 2007). Over 70% of consumers are unaware of what information firms collect, and consumers who are aware are less willing to disclose information (Rose, Rehse, and Röber 2012), which implies that transparency could be a double-edged sword. Therefore, understanding whether promoting transparency about the collection, storage, or use of information truly affects consumers' trade-off and thus the acceptance of information collection positively is crucial.

Control implies that a consumer has the ability to regulate the collection, storage, or use of information. The importance of control is also reflected in the Federal Trade Commission's opinion on privacy, which has stressed that firms should ask consumers for consent (Ohlhausen 2014). In the EU, the GDPR mandates that besides control over data collection (consent of collection), firms should also provide consumers with control over data storage (ability to remove data) and data use (ability to prevent the use of data) (General Data Protection Regulation 2016). Moreover, providing control might also be in the

interest of firms. Prior research has shown that consumers are more cooperative and committed to firms they believe provide control (Son and Kim 2008). For example, giving consumers control over the collection of their information increases the effectiveness of personalized advertisements (Schumann, Von Wangenheim, and Groene 2014), while providing consumers control over storage by offering the opportunity to remove information increases their acceptance of information collection by firms in general (Röber et al. 2015). Moreover, control over the use of information makes consumers more willing to self-disclose information to a specific firm (Mothersbaugh et al. 2012). However, despite governmental pressure and the potential benefit for both firms and consumers, firms have remained reluctant to proactively communicate that consumers have influence over the collection, storage, and use of information. Firms might fear that actively promoting control would disrupt the collection, storage, and use of information. Therefore, they need to consider carefully whether promoting control affects consumers' trade-off and the acceptance of information collection positively. Additionally, firms need a better understanding of whether consumers' acceptance of information collection hinges more on having the ability to prevent information collection (control over collection), the ability to remove or alter information (control over storage), or the ability to determine how information is used (control over use).

3.2 Industries that affect information sensitivity and interaction intensity

Preferences for privacy could be affected by the industry a firm operates in. We assess the influence of one industry characteristic that could enhance the perceived negative consequences for consumers—information sensitivity—and another industry characteristic that could affect the perceived positive consequences for consumers—interaction intensity.

3.2.1 Information sensitivity

Information sensitivity reflects the potential loss (risk) consumers might experience when the information ends up in the wrong hands and is misused (Milne et al. 2017; Mothersbaugh et al. 2012).

As such, information sensitivity increases the subjective personal negative consequences or 'costs' of information disclosure (Premazzi et al. 2010). Consumers generally consider financial or medical information to be more sensitive than lifestyle or purchase habits (Mothersbaugh et al. 2012). While research has shown that consumers are less willing to disclose sensitive information (Lwin, Wirtz, and Williams 2007; Acquisti, John, and Loewenstein 2012; Mothersbaugh et al. 2012; Röber et al. 2015; Phelps, Nowak, and Ferrell 2000), these studies have manipulated information sensitivity by asking respondents to disclose a wide variety of types of information. However, firms generally have limited influence on which information is available for them to collect. For example, to provide personalized services a bank needs to process payment information, even though consumers might consider that information to be highly sensitive. Thus, information sensitivity is often under limited managerial control which implies that other elements might play a more important role in order to strategically differentiate from competitors. Not much is known from prior research how an increased risk (high information sensitivity) moderates the effect of distributive and procedural privacy practices on consumers' privacy trade-off.

3.2.2 Interaction intensity

Rather than only affecting risks and potential losses, the type of industry might also affect the positive consequences, i.e., benefits, consumers derive from the collection of information. Interaction intensity, which we define as the frequency with which consumers interact or transact with a firm, has been used to classify industries or firms by prior studies using comparable terms: usage level (Danaher, Conroy, and McColl-Kennedy 2008), high versus low contact (Bowen 1990), and visit frequency (Hann et al. 2007). The value consumers derive from improved services due to information collection can be enhanced when consumers interact more frequently with firms. For example, consumers benefit more from a more efficient checkout process due to stored financial information when they transact more often with that firm. Similarly, consumers consider personalized feedback or marketing content more

valuable when they use the firm's products and services more often (Mothersbaugh et al. 2012). Also, consumers are more open to relationship programs they interact frequently with (Ashley et al. 2011). However, prior research has not yet addressed the effect of interaction frequency on the influence of specific elements of a firm's privacy strategy on the acceptance of information collection.

4. Study 1: Consumer trade-off among privacy practices

4.1 Experimental design and procedure

To measure the moderating role of industry characteristics on the influence of a firm's privacy strategy, we employed a discrete choice experiment to a 2 x 2 between-subjects design, varying the industry's information sensitivity (high vs. low) and interaction intensity (high vs. low). We selected specific industries on the basis of a pre-test (N = 50), in which respondents rated 16 industries on information sensitivity and interaction intensity, among other characteristics. All characteristics were rated on 7-point Likert scales. We identified banks (high information sensitivity, high interaction intensity), health insurance (high, low), news providers (low, high), and cinemas (low, low) as the four industries covering the four experimental conditions (details are available upon request).

We allocated respondents randomly to one of the four conditions. In each condition respondents had to indicate the firm with which they normally transacted within the industry. All questions were then adjusted to that specific firm, so that we assess the acceptance of information collection for a specific purpose by a specific firm within a specific industry (see Appendix A for the scenario). Respondents who did not interact with a firm from the industry were screened out, as these respondents would not be able to relate the subsequent choice experiment to a specific, realistic context.

Before the choice experiment started, the respondents answered several questions with regard to their perceived privacy practice of their current firm. These questions were structured into the privacy

practices of information collection, storage, use, transparency, and control. These questions served to provide a benchmark for the status quo and, using the same terminology as in the choice experiment, to make respondents familiar with the attributes and levels used in the subsequent choice tasks.

4.2 Discrete choice experiment

In the discrete choice experiment, we assess whether consumers accept a personalization program that varies in the way data is collected, stored, and used, and the amount of transparency and control over these elements provided by a firm. For each of these elements we generated levels based on realistic combinations of sub-dimensions of each element, which resulted in seven to nine levels per element.[2] Specifically, for information collection we used seven combinations of whether the data were provided voluntarily (default), tracked within the channels of the firm (internally), tracked outside the channels of the firm (externally), or inferred. Storage was represented by nine combinations of two sub-dimensions; one that captured storage time (unlimited, one year, or one month) and another that captured storage type (anonymized, identifiable by ID, or identifiable by email address). Information use consisted of eight combinations of personalization of insights, personalization of marketing content, and secondary disclosure. Finally, transparency and control both featured all eight combinations for which element (collection, storage, use) the firm provides transparency and control, if any (see Appendix B for the list of attributes and levels). Throughout the experiment, respondents were able to get more information about the meaning of the attribute levels by moving their pointer over each level's text, which opened a popup box with additional information and examples.

We used a computer-generated design to allocate randomized sets of profiles to choice sets with two options each. The resulting factorial design was balanced and orthogonal (Huber and Zwerina 1996). Moreover, as we are interested in whether consumers accept information collection or would rather

[2] We made sure that each of the elements matter in a pre-test using banks as the research context (N = 100).

reject information collection and not use the service, we included a no-choice option using a dual-response format (Brazell et al. 2006; Wlömert and Eggers 2016). Figure 2 depicts an exemplary choice set. Each respondent completed 14 choice sets, including an initial training set and a holdout set for checking predictive validity so that twelve decisions remained for the estimation. Please refer to the Web Appendix where we address potential concerns about the validity of a conjoint choice experiment in the field of privacy.

===== FIGURE 2 =====

5. Results

5.1 Sample

We invited respondents to our experiment via a Dutch research panel provider that has sent out invitations to participate in our study. The panel is representative on six socio-demographic characteristics: gender, age, education, region, household composition and employment. Respondents received standard panel incentives for their participation. The median time to complete the survey was about 13 minutes (790 seconds). From the 1,285 consumers who completed the survey, 100 respondents were removed because they answered the survey in an unrealistically short time (less than 5 minutes), while another 344 respondents were removed because they failed an attention check.[3] The remaining sample of 841 consumers showed no signs of adverse quality, such as straightlining. Respondents were equally divided over the four industries: Banks (N = 211), insurance firms (N = 223), news (N = 202), and cinemas (N = 205). Figure 3 shows the industry classification and a manipulation

[3] The 29% failure rate is substantial but in line with studies using similar instructional manipulation checks (Paas and Morren 2018). Nonetheless, it is a cause for concern. However, using a choice experiment with randomized stimuli, inattentive respondents are less likely to systematically bias the answers but would rather increase the error variance. Accordingly, not excluding the inattentive respondents and using the full sample for the estimation only has a minor effect on the results. Utility estimates are highly correlated ($\rho = .99$) but, in general, scaled lower (closer to zero) in the full sample, which is consistent with a higher amount of random answers in logit models (Hauser, Eggers, and Selove 2019). Consequently, consumers appear slightly less sensitive in simulations. However, no major implications change. Please refer to Appendix C for a comparison of the results.

check based on perceived industry characteristics and confirms that the four industries were appropriately represented.

Because target groups in the four industries differed, the samples had minor structural differences. Specifically, the cinema sample was slightly younger and contained more married people than the other industries. Within the specific industries, we found that age and marital status only had a minor effect on the results. Preferences did not differ significantly depending on marital status in any of the industries and there are only six significant differences out of 68 depending on the age category (α = 5%) so that we do not discuss these differences further (details are available upon request).

===== FIGURE 3 =====

5.2 Status quo

Table 1 shows that the perceived status quo of current privacy strategies differs between industries. According to the respondents' classification, news providers rely on all forms of data collection whereas banks, insurance companies, and cinemas depend mainly on volunteered and internally collected information. Interestingly, news providers use volunteered information substantially less often and consumers believe they substitute this information with automatically collected or inferred data. Regarding storage, information is largely kept for an unlimited time in all industries. Moreover, all industries are perceived to store identifiable information, either by ID (banks and news) or by email address (cinemas and insurance companies). In terms of information use, banks and insurance firms rely mostly on providing recommendations and insights into their own behavior, whereas news providers and cinemas use more personalized marketing content. Over 40% of the respondents believe their news provider disseminates information to third parties. Finally, across all industries most respondents believe their firm is not transparent (avg. 67%) and provides no control (avg. 58.7%).

===== TABLE 1 =====

5.3 Estimation

We estimated consumers' preferences for the privacy elements using a standard multinomial logit (MNL) model within a hierarchical Bayes (HB) procedure. Since HB provides individual-level utility estimates, we account for heterogeneity between consumers. Accordingly, at the lower level, the probability that respondent *h* chooses alternative *i* from choice set *J* can be written as follows (Rossi and Allenby 2003):

(1) $$\mathrm{P}(i)_h = \frac{\exp\,(\beta_h{}' x_i)}{\sum_{j\in J}\exp\,(\beta_h{}' x_j)},$$

with x_i being a vector for privacy elements for alternative *i* and β_h being a vector of the part-worth utilities for respondent *h*. As the scale of the utilities is affected by the error variance we normalize the scale by setting the error variance to one (Hauser, Eggers, and Selove 2019).

At the upper level, we assume a normal distribution of the partworths with different means according to the two industry characteristics:

(2) $$\beta_h = \theta' z_h + \varepsilon_h,$$

with θ being a matrix of parameters, z_h being a vector of covariates (information sensitivity, interaction intensity), and ε_h representing normally distributed random effects with covariance matrix D, i.e., $\varepsilon_h \sim Normal(0, D)$. We assume a diffuse prior with a variance of 2.0 and 5 degrees of freedom in addition to the number of parameters for the prior covariance matrix. After a burn-in period of 10,000 iterations we used 10,000 iterations to draw posterior partworths.

The process converged well and the model fit was acceptable, outperforming a chance (null) model 2:1 in terms of root likelihood (RLH improvement over chance = 1.955, standard deviation across

draws = 0.015). Similarly, the holdout sample predictions among three alternatives (two privacy alternatives and no-choice) showed high predictive validity with a hit rate of 0.712 (compared to 0.33 chance). Since we found no substantial improvement in model fit when considering interaction effects, we report only main effects.

5.4 Estimation results

Table 2 provides the sample means and standard deviations across consumers to indicate the level of heterogeneity in preferences. We present the results as contrasts between the two industry characteristics

===== TABLE 2 =====

Collecting more information than voluntarily provided has a negative effect. However, the negative effect of internal information collection is close to zero. The standard deviations indicate that in all industries a proportion of the consumers consider internal information collection and (to a lesser extent) inferred information as beneficial. In contrast, collecting information externally has a substantial negative effect on the acceptance of information collection. The absolute magnitude of the mean effect exceeds the standard deviation in all industries, particularly in information-sensitive industries.

On average, consumers react in a neutral way regarding the use of information for personalization of insights. Again, the standard deviations indicate that across all industries some consumers perceive a utility of this use while others perceive a disutility. Personalized marketing content has a negative influence, although some consumers are indifferent or even perceive such content as beneficial. Respondents are consistently averse to disseminating information to third parties (e.g., other firms).

While consumers respond in a positive manner to both transparency and control, effect sizes are lower for transparency. Standard deviations often exceed the means such that some consumers

consider transparency as negative in low information-sensitivity industries (e.g., News). Overall, transparency is most preferred in industries that consumers interact less frequently with. Among collection, storage, and use of information, storage has the lowest effect sizes for both transparency and control. Nevertheless, across all industries it is most beneficial from a consumer perspective to provide control over all elements, while the worst strategy is to allow no control.

Table 3 shows the mean relative importance rates based on the difference between best and worst strategies per element depending on the industry characteristics (calculated for each individual in each posterior draw, then averaged). Storage type matters most in almost all industries, while storage time is less important. Storage type and time are less important for information-sensitive industries, while information collection and use gain in importance weight. Differences in transparency and control depending on information sensitivity are only marginally significant according to the posterior distribution.

Regarding interaction intensity, importance weights are more balanced. We see significant differences only in terms of transparency, which is more relevant in industries that are characterized by less frequent interactions (here, insurance companies and cinemas).

===== TABLE 3 =====

5.5 Simulation and sensitivity analysis

The previous analyses focus on the effect of privacy elements on consumers' preferences—that is, utility estimates. However, the analyses do not consider whether the differences in utilities are meaningful in terms of their effect on choice probabilities. To analyze these effects, we create a scenario in which we predict the share of consumers that would adopt the personalization program rather than

not accept the data collection that goes along with it. Specifically, we use the logit model (Equation 1) to predict choice probabilities between two alternatives: (1) the current status quo within the industry and (2) the no-choice option. To determine the current status quo, we consider all privacy elements that more than 33%[4] of the consumers indicated as currently being used by the firm within the industry (see Table 1).

The status quo privacy strategy has an average choice probability of less than 50% in all industries. That is, on average it is more likely that consumers do not consent to the data collection. The highest probability of 0.45 is achieved by the insurance industry in which only internal information is collected, which is stored by email address for unlimited time and used for personalized insights and marketing content. Cinemas and banks follow thereafter with 0.44 and 0.39 choice probability. News providers have the lowest choice probability (0.26) because their strategy contains more negative elements—that is, internal and external data plus inferred information, all of which are used for personalized insights, marketing content, and dissemination to third parties.

===== TABLE 4 =====

Our sensitivity analysis compares to what extent the shares of the status quo scenario change when privacy elements are added (+) or removed (-) from the current strategy ("0" represents the status quo element). Table 4 depicts the relative change in choice probabilities. Accordingly, firms should be reluctant to collect information externally, as the share of consumers accepting information collection would drop by 9% (cinema) to 12% (bank) when firms start collecting information externally. For news, the influence of removing external information collection is less profound (6%), as consumers believe

[4] We use one-third because this value implies differences between industries while still considering only frequently employed strategies.

most news providers already collect information externally. Foregoing inferred data collection has less substantial effects but the resulting changes compared to the status quo remain robust.

Storing information for a shorter period would also be a promising strategy, which seems to especially increase the acceptance of information collection by news providers (+23%) and cinemas (+18%). However, firms need to consider whether this positive effect offsets the usage constraint of shortening the storage time. Our experiment suggests that the most influential lever to increase choice probabilities is to save personal information only in an anonymous form, e.g., at an aggregated level. In this case, shares would increase by 24% (banks) to 54% (news).

With regard to the use of information, the largest negative impact has the dissemination of information to third parties, as 19% (insurance firms) to 23% (banks) of the current share would be lost when adding this element to the strategy. Also, news providers who are currently using this strategy would benefit largely from removing this element, resulting in a 19% share increase. Removing other elements of information use only has a marginal effect, probably because they are already being used.

A firm could also maintain its current strategies and add transparency and control elements to increase choice probabilities. Adding all transparency or control elements would make the personalization program substantially more attractive. Shares would increase by 13% (news) to 19% (cinema) when adding full transparency. Offering control leads to 20% (insurances) to 28% (news) higher shares. In these cases, choice probabilities would exceed those of the no-choice option, except for news providers given the low choice probability of the status quo. Overall, these results confirm that consumers are sensitive to optimizing the privacy strategy—that is, focusing on specific privacy elements matters.

6. Study 2: Competing on privacy vs. price

The first study showed that consumers are sensitive to privacy practices and trade-off positive and negative privacy elements. In practice, companies could also balance privacy practices with price, e.g., by giving a rebate for providing personal information. This second study adds price as a benchmark attribute, which allows calculating willingness-to-pay for privacy practices (see also Lin, 2022, who estimates valuations for personal information). Moreover, we estimate price equilibria that would result when firms compete on the market for privacy. In this regard, the study can be seen as an empirical extension to Rust, Kannan, and Peng (2002) who derive equilibrium solutions in a monopoly and to Lee, Ahn, and Bang (2011) who provide a game theoretical model.

6.1 Experimental design and sample

We nested the second study in the bank scenario, similar as in Study 1. We used the same privacy attributes and levels (see section 3.2) and added price as an additional attribute. This price attribute referred to the monthly maintenance fee for the bank account and varied between 'no fee' (€0) and €1.50 per month, which captured the price range employed by most banks at the time of the data collection. Although the maintenance fee is not the primary revenue driver for banks it is, arguably, most accessible for consumers in our survey context. All remaining settings remained consistent to Study 1.

A total of 302 consumers completed the study. After filtering respondents who did not pass the attention check (see Study 1), 238 respondents remained for the estimation. The sample's most frequently paid monthly maintenance fee was €1.50. The status quo regarding the most frequently employed privacy practices was consistent to Study 1 (see Table 1).

6.2 Estimation

Having price as an attribute in the study setup, we are able to normalize the scale to monetary units and estimating a separate scaling parameter, γ_h, as in Sonnier, Ainslie, and Otter (2007). Accordingly, the utility that respondent *h* receives from alternative *i* can be expressed as $u_{ih} = \gamma_h(\beta_h{}'x_i - p_i)$, with x_i being a vector of privacy practices for alternative *i* and p_i is the monthly maintenance fee (i.e., price). In this model, the estimated part-worth utilities for the privacy practices, β_h, can be interpreted directly in terms of incremental willingness-to-pay. We constrained γ to positive values by assuming a log-normal distribution in the prior, while all β parameters were assumed to be normally distributed as in Study 1. We increased the number of burn-in iterations to 20,000 to ensure convergence and kept another 10,000 posterior draws. All other estimation settings remained consistent to Study 1. The estimation process converged well and showed an acceptable fit, indicated, for instance, with a posterior average hit rate of 0.694 (vs. 0.712 in Study 1).

6.3 Willingness-to-pay for privacy

When collecting external information banks would have to charge a consumer €0.62 per month less (SD = 0.33), on average, compared to asking for voluntary information only. This implies banks would have to provide a rebate of -59% of the base price of €1.50. The most negative element is to disseminate information to third parties for which consumers would request a monetary compensation of, on average, €1.46 per month (SD = €1.15). Given the status quo of €1.50 maintenance fee per month, this result implies that banks would have to waive the fee entirely when using this privacy practice. Consumers are willing to pay €0.47 (SD = 0.43) per month more for storing information for shorter time periods, €0.89 (SD = 0.32) more for storing it in anonymized form, and up to €0.70 for offering transparency and €1.05 when adding control of information collection, storage, and use. (See Appendix D for detailed results). Overall, all privacy elements remain relevant to consumers despite including

price. On average, price has a relative importance weight of 15.7% (posterior SD = 0.8%) such that the privacy elements comprise more than 80% importance in comparison.

6.4 Price equilibria

The willingness-to-pay estimates do not translate directly into revenue or profit gains as they do not consider competitive reactions. To show the impact of the privacy elements on equilibrium revenues we simulate a market with two competitors in a market of ten million consumers that exhibit the empirically derived distribution of preferences and privacy trade-offs. Other, static competitors are considered in an outside option, represented by the no-choice utility.

As a benchmark, we use the competitive scenario in which both firms offer the same privacy practices of the status quo situation, i.e., internal data collection and collection of inferred information, storage by ID for an unlimited time, used for personalized insights and content, providing neither transparency, nor control. When both firms offer the bank accounts for €1.50 per month, they would achieve a market share of 20.7% each (SD = 0.7%). As in the simulations in Study 1, the majority of consumers would choose neither of these two competitors. This configuration would lead to expected revenues of €3,100,146 (SD = €107,684).[5] However, this solution is not a Nash equilibrium as increasing the price would allow one firm to make larger revenues. If one firm increases its price to €1.76 per month its market share would drop to 17.7% (SD = 0.8%) but revenues would increase to €3,119,042 (SD = €146,975). In this case, the optimal reaction of the competitor is to also increase prices. The Nash equilibrium is achieved if both firms offer the bank account for €1.76 per month as neither increasing or decreasing the prices further would yield higher revenues for any of the firms; both would generate €3,482,660 (SD = €132,180) at 19.8% (SD = 0.8%) market share.

[5] These calculations show the mean across posterior draws. Standard deviations are given in parentheses.

Compared to this benchmark we analyze how the equilibria change when one firm differentiates and offers a different privacy practice than in the status quo scenario. Specifically, we assume that firm 1 keeps the privacy practice of the status quo scenario and firm 2 differentiates. We use the root-finding method of Allenby et al. (2014) to estimate Nash price equilibria for each posterior draw and calculate the mean revenue change to the benchmark scenario of having no differentiation. Equilibria exist in the majority of draws (96.6%, on average). Table 5 presents the results.

===== TABLE 5 =====

Overall, the results show that if firm 2 implements a more favorable privacy practice (not collecting data internally or by inference, storing it for shorter periods or in anonymous form, providing transparency or control), it is able to significantly increase its revenue compared to the status quo. This is due to appealing to a segment of consumers that care about privacy, which was previously untargeted (drawing from the outside option), and those who are willing to pay a higher price per month. At the same time, firm 1 might, on average, also benefit from the differentiation of firm 2 because of lower competition. At least, firm 1 is not performing significantly worse in any of the scenarios if firm 2 decides to optimize the different privacy elements. Similarly, if firm 2 offers a privacy practice that is less appealing to consumers (collecting data externally, disseminating data to third parties, or not providing personalized insights or content), it largely benefits the competitor that is able to increase revenues significantly.

7. Discussion

We study how the main elements of a firm's privacy strategy affect consumers' privacy trade-off and thus their acceptance of information collection. Moreover, we assess whether the importance of each privacy element differs between industries that vary in information sensitivity and interaction intensity. Thereby, we have executed two choice experiments in a total of four industries using a

conjoint design. Overall, we see that each of the privacy elements (information collection, storage, use, transparency, and control) matter to consumers and lead to changes in choice shares. In addition, we show that these effects differ systematically between industries. Before discussing our findings more in-depth, it is important to note that we assume that the trade-offs consumers make in an experimental situation would also transfer to real-life choices. Although conjoint studies have been used to test theory with more abstract attributes (e.g., Wuyts et al. 2004), we would call for future studies in field-settings to confirm our findings how data-sharing and data-control practices affect consumer choice. We show the most important findings in Table 6, which we subsequently discuss, that can be used as propositions to guide future research.

===== TABLE 6 =====

We observe that using more ways to collect information negatively affects the acceptance of information collection. This finding corresponds with prior work (e.g., (Martin, Borah, and Palmatier 2017)) that showed that consumers feel more vulnerable when a firm requests access to more types of information. Although interaction intensity increases the negative impact of internal information collection, the sensitivity analysis shows this effect to be negligible because all industries already collect information internally. Hence, owing to the status quo, removing this element only marginally affects the choice probabilities. Moreover, we show that consumers are more responsive to information collection in industries that handle sensitive information, such as banks and insurance companies. The risks are intensified in information-sensitive industries, which suggests that consumers focus more on ways to avoid these risks altogether.

In line with risk theory, our findings show that promoting a shorter period for storing information and storing it anonymously or in a non-identifiable way each increases consumers' acceptance of

information collection. Remarkably, however, information storage seems to be less important in information-sensitive industries (banks, insurances). While these importance rates are relative and thus do not necessarily imply that storage is less important on an absolute level, consumers might understand that to provide reliable services, banks and insurance firms need to store identifiable information for an extended period. In industries in which information is less sensitive consumers might doubt the need to store identifiable information for an unlimited period. However, storing information for shorter periods or in anonymous form also reduces the usage opportunities for firms and might therefore not be a sensible alternative for many firms, such as Google or Amazon, that heavily rely on data in their marketing and operations. However, for banks that might rely less on personalization in their marketing communication, and given that for banks it is of utmost importance to be trusted, aggregation might be a good option. For example, there has been strong negative publicity for the Dutch bank ING when sharing their intentions to use payment data to personalize offers (Verhoef and Baake 2019). Moreover, methodologies are evolving that allow to make managerial inferences even if data is available in privacy preserving form (Holtrop et al. 2017).

With regard to information use, we show that on average, consumers are neither expecting large benefits nor disadvantages from personalized insights or personalized marketing content. Prior studies show that consumers are more committed and cooperative when confronted with personalization (e.g., (Chung, Wedel, and Rust 2016; Hauser, Liberali, and Urban 2014; Urban et al. 2013)). In our research, we give consumers an evident choice. Describing personalization in the choice context makes it explicit, which could result in reactance. In the context of ads we have already seen that reactance might cause consumers to resist personalization (Van Doorn and Hoekstra 2013; Bleier and Eisenbeiss 2015; Goldfarb and Tucker 2011; Aguirre et al. 2015). On the other hand, removing personalized marketing content only has a marginally positive impact on choice probabilities, so firms that are currently using personalized marketing content are not forced to act. Moreover, the benefits of information use are not enhanced by

interaction intensity. Thus, even in industries in which consumers interact often with firms, they are not expecting large benefits from personalized insights or personalized marketing content. Furthermore, our findings confirm that consumers strongly oppose external dissemination of information in any industry (e.g., Wirtz and Lwin 2009). Combining the considerable loss of disclosing sensitive information with the uncertainty of sharing information with third parties repels consumers even more. As a caveat, our results represent the consumer perspective such as when given a choice between personalization or not. It does not reflect whether personalization is effective which also needs to be factored in when deciding to offer these options to consumers.

Besides privacy elements that affect distributive fairness, we also show that enhancing procedural fairness by offering control and transparency over the collection, storage, or use of information has a positive effect on consumers. Transparency and control are more important in industries that are considered sensitive (marginally significant at a 10% level). Transparency matters less when consumers interact more frequently with the firm. We believe that when consumers interact less often with a firm they might recall the privacy settings less well, so that transparency becomes more valuable. Nevertheless, stressing transparency and control is beneficial in all industries because most consumers believe that their current firm provides neither transparency nor control. As consumers believe they are “being kept in the dark” and “have lost all control” (TNS 2011), promoting transparency and control represents a promising option for strategic differentiation, which is confirmed by our sensitivity analysis and equilibria estimation. Arguably, adding control is more consequential for firms, so they might not be able to collect, store, or use the information as intended if consumers interfere. Although the decision to allow control needs to consider this trade-off, preliminary evidence suggests that consumers become more cooperative when they feel they are in control (Brandimarte, Acquisti, and Loewenstein 2013). Future research should assess whether consumers are indeed not interested in disruption, and thus whether firms would benefit from offering only control.

8. Limitations

Consumers might not always pay attention to their privacy. Reviewing privacy statements or terms and conditions is a complex task that consumers typically avoid. Especially in low-involvement ("low-effort") situations, such as when consumers search online or use their mobile phone, a privacy paradox might occur such that consumers accept information collection in spite of their concerns (Dinev, McConnell, and Smith 2015; Acquisti, Brandimarte, and Loewenstein 2015). In our study, we cannot rule out that consumers might have used heuristics to decide which option to prefer instead of carefully considering all information. We are convinced that our setting mimicked reality, in which consumers also do not necessarily process all the available information about privacy. In this realm, our study identifies which cues consumers attend to primarily in deciding whether to accept data collection. Relatedly, our study could have used more concrete attributes or stressed the potential consequences of the privacy element, such as a specific risk of a data breach. However, as we study multiple industries a high level of concreteness could become problematic. Individual companies would want to replicate our study with more specific privacy and marketing elements that are dedicated to their business.

Moreover, while we searched for the optimal privacy strategy (the "what"), we did not assess how a firm can promote this strategy to consumers, for example, without raising privacy concerns by making privacy more salient (the "how"). Specifically, we do not assess whether or how the way firms explain their privacy strategy affects our results. Relatedly, we purposefully used a wording that applies to all four experimental cells in order to compare the effects. We cannot rule out that a more specific wording that is tailored to each of the four industries might affect the results. Future research should therefore assess in more detail the "how" of communicating and promoting privacy.

A high level of heterogeneity between individuals remains unexplained. Future research should assess cognitive drivers that affect preferences. It would also be interesting to see if or how consumers

translate the privacy elements to a perceived probability of negative events taking place (e.g., a data breach), for instance as a mediator. Cultural differences should also be considered. Prior research has not only suggested that consumers from different countries and cultures worry about different issues (e.g., Miltgen and Peyrat-Guillard 2014) but also that privacy elements are valued differently between countries. As an example, US consumers considered unauthorized secondary use to be a minor issue, whereas Singaporean consumers felt unauthorized use was the most important privacy violation when dealing with online retailers (Hann et al. 2007). Our study is based on a sample from the Netherlands and does not allow these inferences. Given that our findings are consistent with the pre-test results from a US sample, we believe that the focus on a single nation is a minor limitation.

9. Conclusion

Firms are hesitant in aligning their privacy strategy with consumer preferences and tend to stick to legal requirements only. In this context, we analyze how consumers trade-off different privacy elements. We show that consumers take all elements into account (information collection, storage, use, transparency, control) when deciding to accept information collection. We also analyze how industry characteristics affect the influence of these elements and how their relevance is affected when compared to price. In this regard, our results provide insights how data collection strategies affect consumers' acceptance of information collection. The experimental conjoint study is a first of its kind that provides relevant insights that need to be tested further in future research with field data. This is especially relevant, as many technology giants, such as Amazon, as well as traditional firms, such as ING, are investing in data science assuming that consumes will keep sharing their data.

Rust et al. (Rust, Kannan, and Peng 2002) analyzed a monopolistic market scenario and projected that a market for privacy will emerge but privacy will continue to erode if the market is left unregulated. Regulation is effective in protecting consumers, however, it also creates fierce competition among firms

on the market for privacy if no firm exceeds the legal requirements. We demonstrate empirically that differentiation on privacy can effectively segment the market among privacy unconcerned consumers who are price sensitive and those who are willing to purchase a higher degree of privacy, leading to lower overall competition. While Lee et al. (2011) already showed using a game-theoretic approach that optimizing privacy practices could be a viable business model, our simulations imply that optimizing privacy practices can lead to a pareto optimum for the differentiating firm, the competitor, and consumers. Thus, we propose that competitive market forces can counteract the erosion of privacy if companies put the market for privacy on their strategy map.

References

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein (2015), "Privacy and Human Behavior in the Age of Information," *Science*, 347, 6221, 509–14.

———, Leslie K. John, and George Loewenstein (2012), "The Impact of Relative Standards on the Propensity to Disclose," *Journal of Marketing Research*, 49, 2, 160–74.

Adomavicius, Gediminas and Alexander Tuzhilin (2005), "Personalization Technologies," *Communications of the ACM*, 48, 10, 83–90, doi:10.1145/1089107.1089109.

Aguirre, Elizabeth, Dominik Mahr, Dhruv Grewal, Ko de Ruyter, and Martin Wetzels (2015), "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness," *Journal of Retailing*, 91, 1, 34–49, doi:10.1016/j.jretai.2014.09.005.

Al-Natour, Sameh, Hasan Cavusoglu, Izak Benbasat, and Usman Aleem (2020), "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps," *Information Systems Research*, 31, 4, 1037–63, doi:10.1287/isre.2020.0931.

Allenby, Greg M., Jeff D. Brazell, John R. Howell, and Peter E. Rossi (2014), "Economic Valuation of Product Features," *Quantitative Marketing and Economics*, 12, 4, 421–56, doi:10.1007/s11129-014-9150-x.

Ansari, Asim and Carl F Mela (2003), "E-Customization," *Journal of Marketing Research*, 40, 2, 131–45.

Ashley, Christy, Stephanie M. Noble, Naveen Donthu, and Katherine N. Lemon (2011), "Why Customers Won't Relate: Obstacles to Relationship Marketing Engagement," *Journal of Business Research*, 64, 7, Elsevier Inc., 749–56, doi:10.1016/j.jbusres.2010.07.006.

Athey, Susan, Christian Catalini, and Catherine E. Tucker (2017), "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," *Working Paper*,.

Beke, Frank T, Felix Eggers, and Peter C Verhoef (2018), "Consumer Informational Privacy: Current Knowledge and Research Directions," *Foundations and Trends in Marketing*, 11, 1, doi:10.1561/1700000057.

———, ———, ———, and Jaap E Wieringa (2022), "Consumers' Privacy Calculus: The PRICAL Index Development and Validation," *International Journal of Research in Marketing*, 39, 1, Elsevier.

Bélanger, France and Robert E. Crossler (2011), "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly*, 35, 4, 1017–41.

Bleier, Alexander and Maik Eisenbeiss (2015), "The Importance of Trust for Personalized Online Advertising," *Journal of Retailing*, 91, 3, 390–409, doi:10.1016/j.jretai.2015.04.001.

Bolton, Ruth N. and Katherine N. Lemon (1999), "A Dynamic Model of Customers' Usage of Services: Usage as an Antecedent and Consequence of Satisfaction," *Journal of Marketing Research*, 36, 2, 171–86.

——— and Shruti Saxena-Iyer (2009), "Interactive Services: A Framework, Synthesis and Research Directions," *Journal of Interactive Marketing*, 23, 1, Direct Marketing Educational Foundation, Inc., 91–104, doi:10.1016/j.intmar.2008.11.002.

Bowen, John (1990), "Development of a Taxonomy of Services to Gain Strategic Marketing Insights," *Journal of the Academy of Marketing Science*, 18, 1, 43–49, doi:10.1007/BF02729761.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein (2013), "Misplaced Confidences: Privacy and the Control Paradox," *Social Psychological and Personality Science*, 4, 3, 340–47,

doi:10.1177/1948550612455931.

Brazell, Jeff D., Christopher G. Diener, Ekaterina Karniouchina, William L. Moore, Válerie Séverin, and Pierre-Francois Uldry (2006), "The No-Choice Option and Dual Response Choice Designs," *Marketing Letters*, 17, 4, 255–68, doi:10.1007/s11002-006-7943-8.

Brough, Aaron R. and Kelly D. Martin (2021), "Consumer Privacy During (and After) the COVID-19 Pandemic," *Journal of Public Policy and Marketing*, 40, 1, 108–10, doi:10.1177/0743915620929999.

Cadwalladr, Carole and Emma Graham-Harrison (2018), "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, 17, 22.

Chung, Tuck Siong, Roland T. Rust, and Michel Wedel (2009), "My Mobile Music: An Adaptive Personalization System for Digital Audio Players," *Marketing Science*, 28, 1, 52–68, doi:10.1287/mksc.1080.0371.

———, Michel Wedel, and Roland T. Rust (2016), "Adaptive Personalization Using Social Networks," *Journal of the Academy of Marketing Science*, 44, 1, 66–87, doi:10.1007/s11747-015-0441-x.

Culnan, Mary J. and Robert J. Bies (2003), "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, 59, 2, 323–42, doi:10.1111/1540-4560.00067.

Danaher, Peter J., Denise M. Conroy, and Janet R. McColl-Kennedy (2008), "Who Wants a Relationship Anyway?," *Journal of Service Research*, 11, 1, 43–62.

Dinev, Tamara, Allen R. McConnell, and Jeff H. Smith (2015), "Informing Privacy Research through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box," *Information Systems Research*, 26, 4, 639–55.

Donaldson, Thomas and Thomas W. Dunfee (1994), "Towards a Unified Conception of Business Ethics: Integrative Social Contracts Theory," *Academy of Management Review*, 19, 2, 252–84, doi:10.5465/AMR.1994.9410210749.

General Data Protection Regulation (EU) (2016), *General Data Protection Regulation*, European Commission.

Goldfarb, Avi and Catherine E. Tucker (2011), "Online Display Advertising: Targeting and Obtrusiveness," *Marketing Science*, 30, 3, 389–404, doi:10.1287/mksc.1100.0583.

——— and ——— (2013), "Why Managing Customer Privacy Can Be an Opportunity," *MIT Sloan Management Review*, 54, 3.

Gurman, Mark and Nico Grant (2021), "Google Explores Alternative to Apple's New Anti-Tracking Feature," *Bloomberg*, https://www.bloomberg.com/news/articles/2021-02-04/google-explores-alternative-to-apple-s-new-anti-tracking-feature.

Hann, Il-Horn, Kai-lung Hui, Tom S. Lee, and Ivan P. L. Png (2007), "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems*, 24, 2, 13–42, doi:10.2753/MIS0742-1222240202.

Hauser, John R., Guilherme Liberali, and Glen L. Urban (2014), "Website Morphing 2.0: Switching Costs, Partial Exposure, Random Exit, and When to Morph," *Management Science*, 60, 6, 1594–1616.

———, Glen L. Urban, Guilherme Liberali, and Michael Braun (2009), "Website Morphing," *Marketing Science*, 28, 2, 202–23, doi:10.1287/mksc.1080.0459.

Hauser, John R, Felix Eggers, and Matthew Selove (2019), "The Strategic Implications of Scale in Choice-Based Conjoint Analysis," *Marketing Science*, 38, 6, 1059–81.

Holtrop, Niels, Jaap E Wieringa, Maarten J Gijsenberg, and Peter C Verhoef (2017), "No Future Without the Past ? Predicting Churn in the Face of Customer Privacy," *International Journal of Research in Marketing*, 34, 1, 154–72.

Huber, Joel and Klaus Zwerina (1996), "The Importance of Utility Balance in Efficient Choice Designs," *Journal of Marketing Research*, XXXIII, August, 307–17, http://www.jstor.org/stable/3152127.

Hui, Kai-Lung, Hock-Hai Teo, and Tom S. Lee (2007), "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly*, 31, 1, 19–33.

Jiang, Zhenhui (Jack), Cheng Suang Heng, and Ben C. F. Choi (2013), "Research Note - Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research*, 24, 3, 579–95, doi:10.1287/isre.1120.0441.

Kim, Min Sung and Seongcheol Kim (2018), "Factors Influencing Willingness to Provide Personal Information for Personalized Recommendations," *Computers in Human Behavior*, 88, December 2017, Elsevier, 143–52, doi:10.1016/j.chb.2018.06.031.

Konstan, Joseph A, Bradley N Miller, David Maltz, Jonathan L Herlocker, Lee R Gordon, and John Riedl (1997), "GroupLens: Applying Collaborative Filtering to Usenet News," *Communications of the ACM*, 40, 3, 77–87, http://portal.acm.org/citation.cfm?id=245108.245126.

LaRose, Robert and Nora J. Rifon (2007), "Promoting I-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior," *Journal of Consumer Affairs*, 41, 1, 127–50.

Lee, Dong-joo, Jae-Hyeon Ahn, and Youngsok Bang (2011), "Protection in Personalization : A Strategic Analysis of Privacy Protection," *MIS Quarterly*, 35, 2, 423–44, http://www.jstor.org/stable/pdf/23044050.pdf.

Lee, Dong-Joo, Jae-Hyeon Ahn, and Youngsok Bang (2011), "Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection," *MIS Quarterly*, 35, 2, 423–44.

Lin, Tesary (2022), "Valuing Intrinsic and Instrumental Preferences for Privacy," *Marketing Science*, 41, 4, 235–53, doi:10.1287/mksc.2022.1368.

Lwin, May O., Jochen Wirtz, and Jerome D. Williams (2007), "Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective," *Journal of the Academy of Marketing Science*, 35, 4, 572–85, doi:10.1007/s11747-006-0003-3.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, 15, 4, 336–55, doi:10.1287/isre.1040.0032.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier (2017), "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing*, 81, 1, 36–58.

———, ———, and ——— (2018), "Research: A Strong Privacy Policy Can Save Your Company Millions," *Harvard Business Review*,.

——— and Patrick E. Murphy (2017), "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science*, 45, 2, Journal of the Academy of Marketing Science, 135–55, doi:10.1007/s11747-016-0495-4.

McDonald, Aleecia M. and Lorrie Faith Cranor (2008), "The Cost of Reading Privacy Policies," *Journal of Law and Policy for the Information Society*, 4, 3, 540–65.

Milne, George R., George Pettinico, Fatima M. Hajjat, and Ereni Markos (2017), "Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing,"

Journal of Consumer Affairs, 51, 1, 133–61, doi:10.1111/joca.12111.

Miltgen, Caroline Lancelot and Dominique Peyrat-Guillard (2014), "Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries," *European Journal of Information Systems*, 23, 2, 103–25, doi:10.1057/ejis.2013.17.

Montgomery, Alan L. and Michael D. Smith (2009), "Prospects for Personalization on the Internet," *Journal of Interactive Marketing*, 23, 2, 130–37, doi:10.1016/j.intmar.2009.02.001.

Mothersbaugh, David L., William K. Foxx, Sharon E. Beatty, and Sijun Wang (2012), "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information," *Journal of Service Research*, 15, 1, 76–98, doi:10.1177/1094670511424924.

Ohlhausen, Maureen K. (2014), "Privacy Challenge and Opportunities: The Role of the Federal Trade Commission," *Journal of Public Policy & Marketing*, 33, 1, 4–9, doi:10.1509/jppm.33.1.4.

Olmstead, Kenneth and Michelle Atkinson (2015), "Apps Permissions in the Google Play Store," *Pew Research*,.

Ostrom, Amy and Dawn Iacobucci (1995), "Consumer Trade-Offs and the Evaluation of Services," *Journal of Marketing*, 59, January, 17–28, doi:10.2307/1252011.

Paas, L.J. and M. Morren (2018), "Please Do Not Answer If You Are Reading This: Respondent Attention in Online Panels," *Marketing Letters*, 29, 1, 13–21.

Petronio, Sandra (1991), "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples," *Communication Theory*, 1, 4, 311–35, doi:10.1111/j.1468-2885.1991.tb00023.x.

Phelps, Joseph E., Glen J. Nowak, and Elizabeth Ferrell (2000), "Privacy Concerns and Consumer

Willingness to Provide Personal Information," *Journal of Public Policy & Marketing*, 19, 1, 27–41.

Premazzi, Katia, Sandro Castaldo, Monica Grosso, Pushkala Raman, Susan Brudvig, and Charles F. Hofacker (2010), "Customer Information Sharing with E-Vendors: The Roles of Incentives and Trust," *International Journal of Electronic Commerce*, 14, 3, 63–91, doi:10.2753/JEC1086-4415140304.

Resnick, Paul and Hal R. Varian (1997), "Recommender Systems," *COMMUNICATIONS OF THE ACM*, 39, 4, 401–4.

Röber, Björn, Olaf Rehse, Robert Knorrek, and Benjamin Thomsen (2015), "Personal Data: How Context Shapes Consumers' Data Sharing with Organizations from Various Sectors," *Electronic Markets*, 25, 2, 95–108, doi:10.1007/s12525-015-0183-0.

Rose, John, Olaf Rehse, and Björn Röber (2012), "The Value of Our Digital Identity."

Rossi, Peter E. and Greg M. Allenby (2003), "Bayesian Statistics and Marketing," *Marketing Science*, 23, 3, 304–28.

Rust, Roland T. and Ming-Hui Huang (2014), "The Service Revolution and the Transformation of Marketing Science," *Marketing Science*, 33, 2, 206–21.

Rust, Roland T, P K Kannan, and Na Peng (2002), "The Customer Economics of Internet Privacy," *Journal of the Academy of Marketing Science*, doi:10.1177/009207002236917.

Schneider, Matthew J., Sharan Jagpal, Sachin Gupta, Shaobo Li, and Yan Yu (2017), "Protecting Customer Privacy When Marketing with Second-Party Data," *International Journal of Research in Marketing*, In Press, 1–11, doi:10.1016/j.ijresmar.2017.02.003.

Schumann, Jan H., Florian Von Wangenheim, and Nicole Groene (2014), "Targeted Online Advertising:

Using Reciprocity Appeals to Increase Acceptance among Users of Free Web Services," *Journal of Marketing*, 78, 1, 59–75.

Smith, H Jeff, Tamara Dinev, and Heng Xu (2011), "Information Privacy Research: An Interdisciplinairy Review," *MIS Quarterly*, 35, 4, 989–1015.

Smith, Jeff H., Sandra J. Milberg, and Sandra J. Burke (1996), "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly*, 20, 2, 167–96.

Solove, Daniel J. (2006), "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, 154, 1291, 477–564.

Son, Jai-Yeol and Sung S. Kim (2008), "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly*, 32, 3, 503–29.

Sonnier, Garrett, Andrew Ainslie, and Thomas Otter (2007), "Heterogeneity Distributions of Willingness-to-Pay in Choice Models," *Quantitative Marketing and Economics*, 5, 3, 313–31.

Stewart, David A. (2017), "A Comment on Privacy," *Journal of the Academy of Marketing Science*, 45, 2, 156–59.

Sutanto, Juliana, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang (2013), "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *MIS Quarterly*, 37, 4, 1141–64.

TNS (2011), "Attitudes on Data Protection and Electronic Identity in the European Union."

Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy (2009), "Americans Reject Tailored Advertising and Three Activities That Enable It," *Working Paper*,.

Urban, Glen L., Guilherme (Gui) Liberali, Erin MacDonald, Robert Bordley, and John R. Hauser (2013), "Morphing Banner Advertising," *Marketing Science*, 33, 1, 27–46, doi:10.1287/mksc.2013.0803.

Van Doorn, Jenny and Janny C. Hoekstra (2013), "Customization of Online Advertising: The Role of Intrusiveness," *Marketing Letters*, 24, 4, 339–51, doi:10.1007/s11002-012-9222-1.

Verhoef, Peter and Merle Baake (2019), "Vertrouwen in Banken Afgelopen Jaren Licht Gestegen," *Economische Statistische Berichten*, 104, 4778, Economisch Statistische Berichten, 482–83.

———, Edwin Kooge, and Natasha Walk (2016), *Creating Value with Big Data Analytics: Making Smarter Marketing Decisions*, Routledge.

Westin, Alan F. (1967), *Privacy and Freedom*, New York, New York, USA: Atheneum.

Wieringa, Jaap, P. K. Kannan, Xiao Ma, Thomas Reutterer, Hans Risselada, and Bernd Skiera (2021), "Data Analytics in a Privacy-Concerned World," *Journal of Business Research*, 122, May 2019, Elsevier, 915–25, doi:10.1016/j.jbusres.2019.05.005.

Wirtz, Jochen and May O. Lwin (2009), "Regulatory Focus Theory, Trust, and Privacy Concern," *Journal of Service Research*, 12, 2, 190–207, doi:10.1177/1094670509335772.

Wlömert, Nils and Felix Eggers (2016), "Predicting New Service Adoption with Conjoint Analysis: External Validity of BDM-Based Incentive-Aligned and Dual-Response Choice Designs," *Marketing Letters*, 27, 1, 195–210, doi:10.1007/s11002-014-9326-x.

Zeithaml, Valarie A. (1988), "Consumer Perceptions of Price, Quality, and Value: A Means-End Model and Synthesis of Evidence," *Journal of Marketing*, 52, 3, 2–22.

Zhao, Ling, Yaobin Lu, and Sumeet Gupta (2012), "Disclosure Intention of Location-Related Information in Location-Based Social Network Services," *International Journal of Electronic Commerce*, 16, 4,

53–89, doi:10.2753/JEC1086-4415160403.

Tables

Table 1.

Status quo of privacy strategy per industry (across respondents).

Current privacy strategy	Bank	Insurance	News	Cinema
Collection[a]				
Volunteered information	87.7%	91.5%	56.9%	81.0%
Internally collected information	71.6%	60.1%	64.4%	65.4%
Externally collected information	24.7%	20.6%	42.1%	28.3%
Inferred information	33.2%	26.0%	45.6%	36.1%
None of the above	1.9%	2.7%	9.9%	6.3%
Storage (Time)				
One month	4.3%	1.8%	11.8%	5.9%
One year	23.2%	21.5%	24.8%	34.6%
Unlimited	68.3%	71.8%	54.0%	53.7%
None of the above	4.3%	4.9%	9.4%	5.9%
Storage (Type)				
Anonymized	22.8%	26.0%	12.4%	16.6%
Identifiable on ID	53.6%	27.4%	66.3%	12.7%
Identifiable on email address	21.8%	41.7%	19.8%	67.3%
None of the above	1.9%	4.9%	1.5%	3.4%
Information Use[a]				
Insights into firm's own behavior	73.0%	60.5%	41.1%	55.6%
Personalized marketing content	58.8%	52.9%	70.3%	75.6%
Dissemination with third parties	13.3%	16.6%	40.1%	26.8%

None of the above	10.0%	17.0%	12.9%	13.3%
Transparency[a]				
Insight in collection	19.9%	20.6%	20.8%	16.6%
Insight in storage	16.1%	16.6%	11.9%	13.2%
Insight in use	13.7%	12.1%	16.3%	15.6%
None of the above	67.2%	65.0%	66.3%	69.8%
Control[a]				
Control over collection	21.3%	24.7%	26.2%	29.3%
Control over storage	16.1%	10.3%	14.4%	15.1%
Control over use	23.2%	16.6%	19.8%	23.9%
None of the above	59.2%	63.7%	58.4%	53.2%

[a] Options are not mutually exclusive, i.e., firms could employ a combination of them.

Table 2.

Estimation results contrasts.

	Information sensitivity				Interaction intensity			
	Low		High		Low		High	
	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Collection								
Voluntary	(0.00)		(0.00)		(0.00)		(0.00)	
Internal	-0.02	0.20	-0.06	0.20	0.01	0.20	-0.10	0.20
External	-0.33	0.28	-0.51	0.27	-0.44	0.28	-0.39	0.29
Inferred	-0.19	0.27	-0.22	0.27	-0.17	0.27	-0.24	0.27
Storage (Time)								
Unlimited	(0.00)		(0.00)		(0.00)		(0.00)	
One year	0.48	0.32	0.39	0.32	0.46	0.32	0.41	0.32
One month	0.79	0.51	0.48	0.51	0.58	0.52	0.69	0.54
Storage (Type)								
Anonymous	(0.00)		(0.00)		(0.00)		(0.00)	
ID number	-1.82	1.09	-0.97	1.04	-1.39	1.10	-1.36	1.20
Email address	-1.30	0.88	-1.05	0.79	-1.10	0.80	-1.24	0.88
Use								
None	(0.00)		(0.00)		(0.00)		(0.00)	
Personalized insights	-0.02	0.12	0.03	0.12	0.00	0.13	0.01	0.12
Marketing content	-0.17	0.15	-0.17	0.15	-0.20	0.15	-0.14	0.15
Dissemination	-0.85	0.78	-1.00	0.81	-0.96	0.81	-0.89	0.79
Transparency								
None	(0.00)		(0.00)		(0.00)		(0.00)	

Collection	0.21	0.23	0.22	0.23	0.27	0.22	0.16	0.23
Storage	0.19	0.15	0.19	0.15	0.20	0.15	0.18	0.15
Use	0.19	0.24	0.26	0.23	0.30	0.23	0.15	0.22
Control								
None	(0.00)		(0.00)		(0.00)		(0.00)	
Collection	0.28	0.14	0.31	0.16	0.28	0.15	0.32	0.15
Storage	0.26	0.18	0.21	0.18	0.26	0.18	0.21	0.18
Use	0.38	0.27	0.46	0.27	0.42	0.26	0.42	0.28
No choice	-0.73	2.59	-0.56	2.74	-0.88	2.59	-0.39	2.72

Reference category in italics.

Mean = mean across respondents, SD = standard deviation across respondents (level of heterogeneity).

Table 3.

Moderating effect of industry characteristics on average relative importance rates.

	Information sensitivity				Interaction intensity			
	Low	High	Difference	p^a	Low	High	Difference	p^a
Collection	0.141	0.160	14%	0.003	0.150	0.152	1%	0.381
Storage (Time)	0.123	0.111	-10%	0.018	0.114	0.120	5%	0.131
Storage (Type)	0.250	0.205	-18%	0.000	0.224	0.230	3%	0.180
Use	0.199	0.216	9%	0.007	0.211	0.204	-3%	0.146
Transparency	0.136	0.145	6%	0.082	0.146	0.135	-7%	0.036
Control	0.152	0.163	7%	0.071	0.155	0.159	2%	0.326

[a] *p*-values are based on the distribution of posterior draws.

Table 4.

Sensitivity analysis.

	Bank			Insurance			News			Cinema		
Collection												
Internal	-	2%	(2%)[n.s.]	-	0%	(1%)[n.s.]	-	0%	(2%)[n.s.]	-	-1%	(2%)[n.s.]
External	+	-12%	(2%)	+	-11%	(1%)	-	6%	(2%)	+	-9%	(2%)
Inferred	-	8%	(2%)	+	-4%	(1%)	-	5%	(2%)	-	4%	(2%)
Storage (Time)												
Unlimited	0	0%	(n.a.)	0	0%	(n.a.)	0	0%	(n.a.)	0	0%	(n.a.)
One year	+	8%	(2%)	+	9%	(2%)	+	11%	(3%)	+	13%	(2%)
One month	+	11%	(3%)	+	9%	(2%)	+	23%	(4%)	+	18%	(3%)
Storage (Type)												
Anonymous	+	24%	(3%)	+	25%	(3%)	+	54%	(6%)	+	31%	(3%)
ID number	0	0%	(n.a.)	+	1%	(2%)[n.s.]	0	0%	(n.a.)	+	-14%	(2%)
Email address	+	-5%	(2%)	0	0%	(n.a.)	+	7%	(3%)	0	0%	(n.a.)
Use												
Insights	-	-1%	(2%)[n.s.]	-	0%	(1%)[n.s.]	-	1%	(2%)[n.s.]	-	1%	(2%)[n.s.]
Content	-	3%	(2%)	-	4%	(1%)	-	3%	(2%)[n.s.]	-	5%	(2%)
Dissemination	+	-23%	(2%)	+	-19%	(2%)	-	19%	(3%)	+	-21%	(2%)
Transparency												
Collection	+	4%	(2%)	+	5%	(1%)	+	6%	(2%)	+	7%	(2%)
Storage	+	5%	(2%)	+	4%	(1%)	+	4%	(2%)	+	5%	(2%)

Use	+	4%	(2%)	+	6%	(2%)	+	3%	(2%) [n.s.]	+	7%	(2%)
All of the above	+	14%	(3%)	+	16%	(3%)	+	13%	(4%)	+	19%	(4%)
Control												
Collection	+	9%	(2%)	+	6%	(1%)	+	8%	(2%)	+	7%	(2%)
Storage	+	5%	(2%)	+	5%	(1%)	+	7%	(2%)	+	7%	(2%)
Use	+	12%	(2%)	+	9%	(2%)	+	12%	(3%)	+	10%	(2%)
All of the above	+	26%	(4%)	+	20%	(3%)	+	28%	(5%)	+	24%	(3%)

Privacy element added (+), removed (-), or status quo (0).

Numbers represent posterior means and posterior standard deviations (in parentheses).

[n.s.] represents non-significant changes compared to the status quo based on the distribution of posterior draws ($\alpha = 0.05$).

Table 5.

Relative revenue changes in equilibrium in differentiated markets

	Added (+) or removed (-) by Firm 2	Firm 1 (Status quo)		Firm 2 (Differentiated)	
Collection					
Internal	-	2.0%	(3.4%)$^{n.s.}$	12.9%	(6.4%)
External	+	15.8%	(5.2%)	-8.4%	(5.2%)$^{n.s.}$
Inferred	-	3.4%	(5.3%)$^{n.s.}$	21.8%	(6.7%)
Storage					
Time: One year	+	2.5%	(6.5%)$^{n.s.}$	28.9%	(12.1%)
Type: Anonymous	+	-0.0%	(5.5%)$^{n.s.}$	26.4%	(7.5%)
Use					
Insights	-	15.8%	(6.1%)	-3.8%	(5.8%)$^{n.s.}$
Content	-	18.9%	(5.0%)	-4.9%	(6.8%)$^{n.s.}$
Dissemination	+	27.7%	(7.0%)	-10.0%	(7.4%)$^{n.s.}$
Transparency					
Collection	+	0.6%	(5.1%)$^{n.s.}$	17.9%	(6.6%)
Storage	+	-5.5%	(4.7%)$^{n.s.}$	26.7%	(6.6%)
Use	+	-2.8%	(3.7%)$^{n.s.}$	22.0%	(5.7%)
All of the above	+	-13.0%	(9.3%)$^{n.s.}$	65.3%	(13.5%)
Control					
Collection	+	-0.7%	(4.4%)$^{n.s.}$	19.0%	(7.3%)
Storage	+	1.9%	(4.4%)$^{n.s.}$	14.5%	(5.8%)

Use	+	-1.0%	(4.8%)[n.s.]	20.7%	(5.8%)
All of the above	+	-5.4%	(8.1%)[n.s.]	50.1%	(13.2%)

Numbers represent posterior means and posterior standard deviations (in parentheses).

[n.s.] represents non-significant changes compared to the status quo based on the distribution of posterior draws ($\alpha = 0.05$).

Table 6.
Main findings of study and resulting propositions for future research

Construct	**Main Findings: Propositions for future research**
Information Collection	- Number of ways to collect information negatively affects the acceptance of information collection
Information Storage	- Shorter time of storing data positively affects the acceptance of information collection. - The effect of time of storing data is weaker in information intensive industries
Information Usage	- No effect of information usage on acceptance of information collection
Control	- Giving control to consumers positively accepts the acceptance of information collection - The effect of control is stronger in information intensive industries.
Transparency	- Providing more transparency on data collection positively accepts the acceptance of information collection. - The effect of transparency is stronger in information intensive industries. - The effect of transparency is weaker in industries where there are frequent interactions between firms and customers

Figures

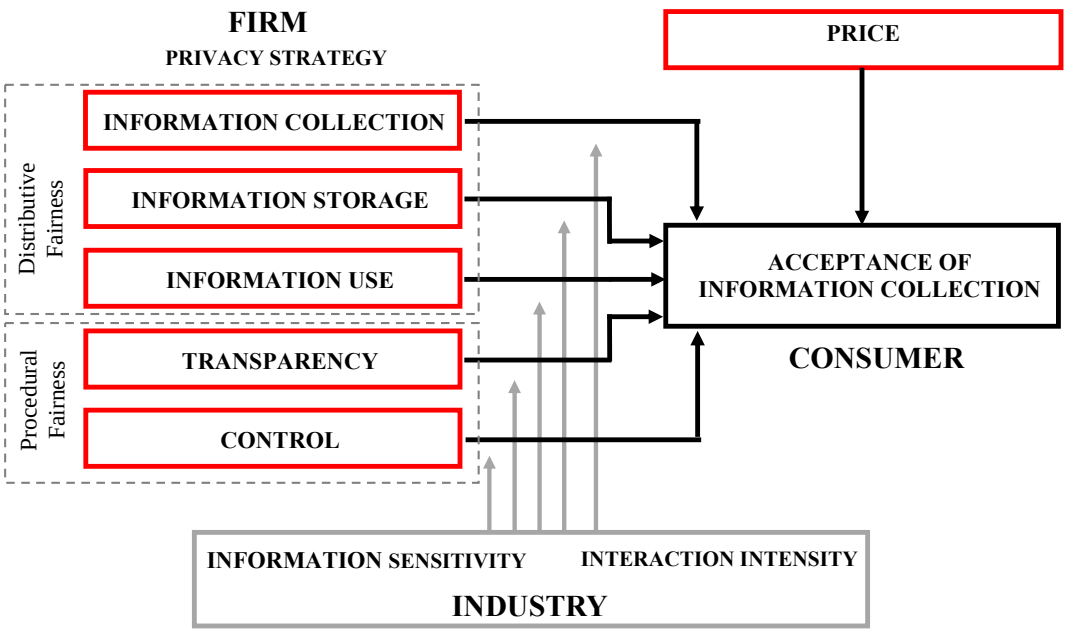
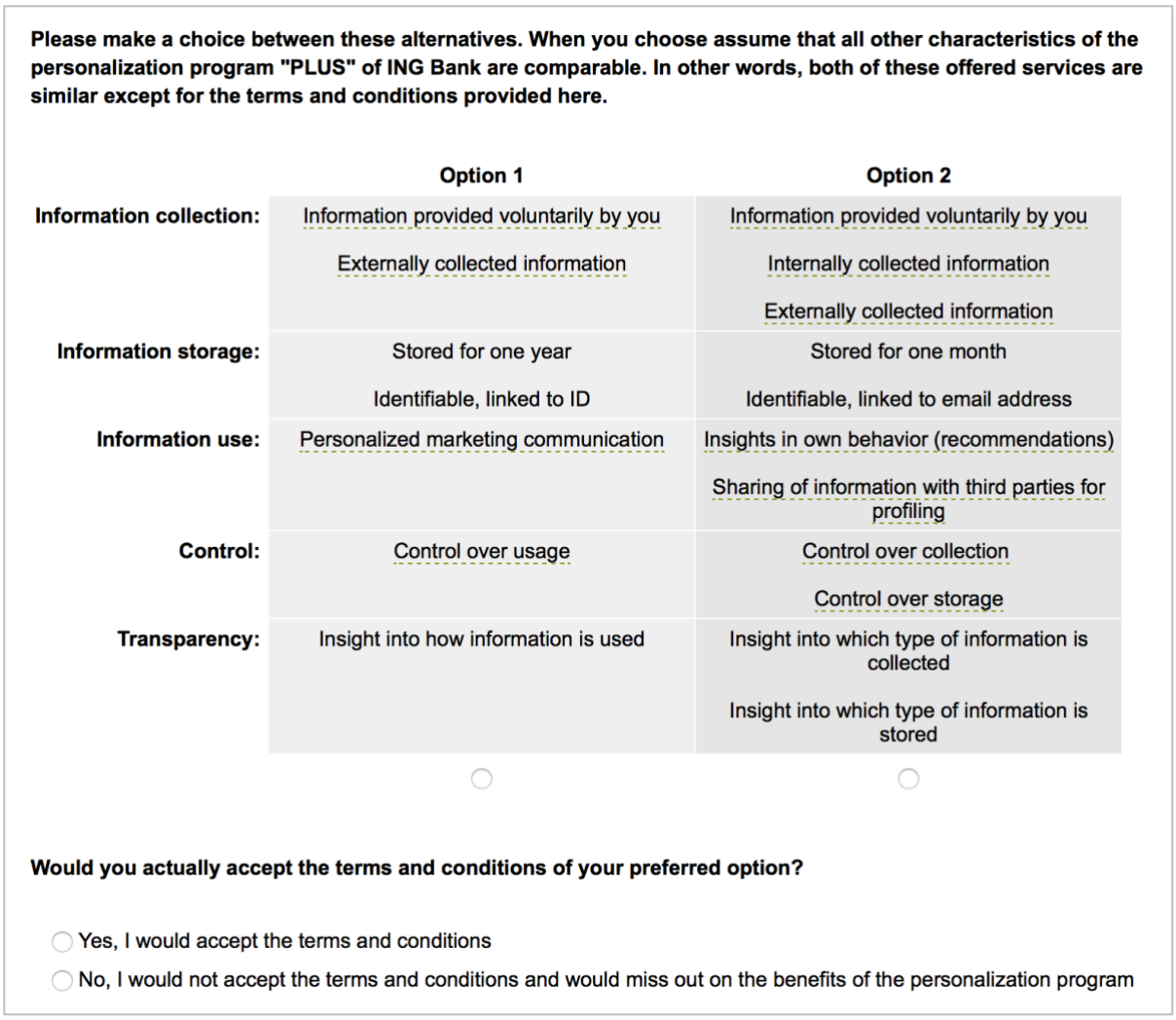


Fig. 1. Conceptual model.



Please make a choice between these alternatives. When you choose assume that all other characteristics of the personalization program "PLUS" of ING Bank are comparable. In other words, both of these offered services are similar except for the terms and conditions provided here.

	Option 1	Option 2
Information collection:	Information provided voluntarily by you Externally collected information	Information provided voluntarily by you Internally collected information Externally collected information
Information storage:	Stored for one year Identifiable, linked to ID	Stored for one month Identifiable, linked to email address
Information use:	Personalized marketing communication	Insights in own behavior (recommendations) Sharing of information with third parties for profiling
Control:	Control over usage	Control over collection Control over storage
Transparency:	Insight into how information is used	Insight into which type of information is collected Insight into which type of information is stored

Would you actually accept the terms and conditions of your preferred option?

- Yes, I would accept the terms and conditions
- No, I would not accept the terms and conditions and would miss out on the benefits of the personalization program

Fig. 2. Illustrative choice set (bank setting, translated).

		Interaction Intensity: High	Interaction Intensity: Low
Information Sensitivity	High	*Bank* (4.13; 4.95)	*Health insurance* (3.52; 2.69)
	Low	*News provider* (3.03; 4.09)	*Cinema* (2.41; 1.96)

Numbers in parentheses on the left indicate the perceived mean rating of information sensitivity, numbers on the right represent the mean rating of interaction intensity in study 1.

Fig. 3. Industry classification and manipulation check

Appendix A: Scenario Descriptions

Now [Your Firm] is thinking about introducing a new personalization program called “PLUS.” This program is free of charge and aims to augment the current service of [Your Firm].

At this moment [Your Firm] uses information about its customers only to improve their products and services at a general level. By introducing the personalization program “PLUS” [Your Firm] aims to adapt its products and services to the needs of individual customers. Therefore “PLUS” ensures that the products and services of [Your Firm] better fit you. Although most decisions with regard to “PLUS” have already been made there is still uncertainty about some of the terms and conditions.

On the following pages you are repeatedly asked to choose between two alternatives of “PLUS.” These alternatives differ on the terms and conditions that have been mentioned before. Please select the alternative that you prefer. After this decision you are asked whether you would truly adopt the new personalization program “PLUS” and the corresponding terms and conditions. When choosing between both alternatives, please assume all other characteristics of the personalization program “PLUS” are the same. In other words, both alternatives are identical except for the terms and conditions mentioned here.

Appendix B: List of Attributes and Levels (Translated)

Information Collection 1 – Volunteered information (forms) 2 – Volunteered + Internally collected information (click-stream) 3 – Volunteered + Externally collected information (search behavior) 4 – Volunteered + Inferred information (needs based on click-stream) 5 – Volunteered + Internally + Externally 6 – Volunteered + Internally + Inferred 7 – Volunteered + Internally + Externally + Inferred
Information Storage (type) and Information Storage (time) 1 – Anonymous + Unlimited 2 – Anonymous + One year 3 – Anonymous + One month 4 – Identifiable on ID + Unlimited 5 – Identifiable on ID + One year 6 – Identifiable on ID + One month 7 – Identifiable on email address + Unlimited 8 – Identifiable on email address + One year 9 – Identifiable on email address + One month
Information Use 1 – Insights in own behavior (recommendations) 2 – Personalized marketing content 3 – Dissemination with third parties 4 – Insights + Personalized marketing 5 – Insights + Dissemination with third parties 6 – Personalized marketing + Dissemination 7 – Insights + Personalized marketing + Dissemination
Transparency 1 – None 2 – Insight in collection 3 – Insight in storage 4 – Insight in use 5 – Insight in collection and storage 6 – Insight in collection and use 7 – Insight in storage and use 8 – Insight in collection and storage and use
Control

1 – None
2 – Control over collection
3 – Control over storage
4 – Control over use
5 – Control over collection and storage
6 – Control over collection and use
7 – Control over storage and use
8 – Control over collection and storage and use

In the estimation we considered the subdimensions of these levels and report their marginal effects in Table 3. For example, instead of estimating effects for the eight levels of transparency, we considered the three binary sub-dimensions separately: 1) transparency about collection (yes/no), 2) transparency about storage (yes/no), and 3) transparency about use (yes/no).

Appendix C: Sensitivity Analysis Comparing Full and Filtered Samples

		Bank			Insurance			News			Cinema	
		Filtered	Full		Filtered	Full		Filtered	Full		Filtered	Full
Status quo		0.39	0.41		0.45	0.46		0.26	0.30		0.44	0.45
Collection												
Internal	-	2%	1%	-	0%	0%	-	0%	0%	-	-1%	-1%
External	+	-12%	-9%	+	-11%	-9%	-	6%	5%	+	-9%	-8%
Inferred	-	8%	7%	+	-4%	-3%	-	5%	3%	-	4%	3%
Storage (Time)												
Unlimited	0	0%	0%	0	0%	0%	0	0%	0%	0	0%	0%
One year	+	8%	7%	+	9%	6%	+	11%	9%	+	13%	8%
One month	+	11%	6%	+	9%	6%	+	23%	17%	+	18%	14%
Storage (Type)												
Anonymous	+	24%	18%	+	25%	21%	+	54%	39%	+	31%	27%
ID number	0	0%	0%	+	1%	0%	0	0%	0%	+	-14%	-11%
Email address	+	-5%	-2%	0	0%	0%	+	7%	3%	0	0%	0%
Use												
Insights	-	-1%	-1%	-	0%	-1%	-	1%	0%	-	1%	0%
Content	-	3%	3%	-	4%	3%	-	3%	2%	-	5%	3%
Dissemination	+	-23%	-19%	+	-19%	-14%	-	19%	13%	+	-21%	-15%
Transparency												

Collection	+	4%	3%	+	5%	3%	+	6%	4%	+	7%	6%
Storage	+	5%	4%	+	4%	4%	+	4%	2%	+	5%	4%
Use	+	4%	4%	+	6%	6%	+	3%	1%	+	7%	5%
All of the above	+	14%	11%	+	16%	13%	+	13%	8%	+	19%	15%
Control												
Collection	+	9%	8%	+	6%	5%	+	8%	6%	+	7%	3%
Storage	+	5%	6%	+	5%	5%	+	7%	4%	+	7%	5%
Use	+	12%	10%	+	9%	8%	+	12%	7%	+	10%	7%
All of the above	+	26%	24%	+	20%	18%	+	28%	18%	+	24%	15%

Privacy element added (+), removed (-), or status quo (0).

Numbers represent posterior means and posterior standard deviations (in parentheses).

$^{n.s.}$ represents non-significant changes based on the distribution of posterior draws ($\alpha = 0.05$).

Appendix D: Incremental Willingness-to-pay for Privacy

	Sample mean	Sample SD
Collection		
Voluntary	(€0.00)	
Internal	-€0.21	€0.15
External	-€0.62	€0.33
Inferred	-€0.53	€0.32
Storage (Time)		

Unlimited	(€0.00)	
One year	€0.47	€0.39
One month	€0.47	€0.43
Storage (Type)		
Anonymous	(€0.00)	
ID number	-€0.58	€0.31
Email address	-€0.89	€0.32
Use		
Insights	€0.19	€0.35
Content	€0.07	€0.27
Dissemination	-€1.46	€1.15
Transparency		
Collection	€0.18	€0.20
Storage	€0.16	€0.17
Use	€0.36	€0.19
Control		
Collection	€0.29	€0.18
Storage	€0.40	€0.15
Use	€0.36	€0.18
No choice	-€0.54	€3.50
Gamma	1.05	0.47

Reference category in italics.