Research Center
Finance & Information Management

Fraunhofer FIT
Project Group
Business & Information
Systems Engineering

The Upside of Data Privacy – Delighting Customers by Implementing Data Privacy Measures

by

Henner Gimpel, Dominikus Kleindienst, Niclas Nüske, Daniel Rau, Fabian Schmied

in: Electronic Markets, 2018, p. 1-16

University of Augsburg, D-86135 Augsburg
Visitors: Universitätsstr. 12, 86159 Augsburg
Phone: +49 821 598-4801 (Fax: -4899)

University of Bayreuth, D-95440 Bayreuth
Visitors: Wittelsbacherring 10, 95444 Bayreuth
Phone: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

WI-686

Electronic Markets – The International Journal on Networked Business

[Manuscript Template]

Full Title of Article:	The Upside of Data Privacy
Subtitle (optional):	Delighting Customers by Implementing Data Privacy Measures
Preferred Abbreviated Title for Running Head (maximum of 65 characters including spaces)	The Upside of Data Privacy
Key Words (for indexing and abstract services – up to 6 words):	privacy concerns, privacy measures, customer data, customer satisfaction, survey research
JEL classification	M3

Abstract

The targeted analysis of customer data becomes increasingly important for data-driven business models. At the same time, the customers' concerns regarding data privacy have to be addressed properly. Existing research mostly describes data privacy as a necessary evil for compliance and risk management and does not propose specific data privacy measures which address the customers' concerns. We therefore aim to shed light on the upside of data privacy. In this paper, we derive specific measures to deal with customers' data privacy concerns based on academic literature, legislative texts, corporate privacy statements, and expert interviews. Next, we leverage the Kano model and data from two internet-based surveys to analyze the measures' evaluation by customers. From a customer perspective, the implementation of the majority of measures is obligatory as those measures are considered as basic needs of must-be quality. However, delighting measures of attractive quality do exist and have the potential to create a competitive advantage. In this, we find some variation across different industries suggesting that corporations aiming to improve customer satisfaction by superior privacy protection should elicit the demands of their specific target customers.

Introduction

In the future, the ability to analyze customer data will be a growing source of competitive advantage (Morey, Forbath, & Schoop, 2015). With the growing amount of data generated worldwide, digital business models emerge which are based on insights gained from customer data (Matthing, Sandén, & Edvardsson, 2004; Saarijärvi, Grönroos, & Kuusela, 2014). At the same time, trust in data privacy is becoming more relevant for customers (Berendt, Günther, & Spiekermann, 2005; Preibusch, Kübler, & Beresford, 2013) which is amplified by several data privacy scandals in the recent past. For instance, a serious incident occurred when the credit card information of 56 million Home Depot customers was stolen (Inman & Nikolova, 2017; Morey et al., 2015). Other examples are Ashley Madison, an online dating portal which lost user data of 37 million registered married men and women to the public (BBC, 2015); Apple which was accused of collecting location data on iPhones and iPads without authorization from and without notifying their customers (The Guardian, 2011); and Facebook which was discovered to be collecting data from user profiles and transmitting these data to advertising companies and others (The Telegraph, 2010). For companies, such publicly exploited scandals cause economic damage (Acquisti, Friedman, & Telang, 2006; Muntermann & Roßnagel, 2009) and competitive disadvantages in brand image and customer satisfaction. Conversely, it might be possible that companies which perform well in terms of data privacy could increase customer satisfaction and gain a competitive advantage. For instance, companies such as DuckDuckGo or Silent Circle already try to differentiate themselves by providing privacy friendly services (Tanner, 2013). DuckDuckGo is a search engine which differs substantially from many conventional search engines. The company collects neither personal information nor behavioral data about its users. Silent Circle is a company which provides solutions for secure communication. For instance, the company developed a smartphone which ensures private and encrypted communication. However, many companies see data privacy as necessary evil. As such, data privacy limits the opportunities to gain valuable customer insights and its implementation binds valuable resources (Culnan & Armstrong, 1999). In addition to this downside perspective, an integrated management of data privacy requires an upside perspective. Moreover, practitioners should be aware of specific available data privacy measures which go beyond the mere application of laws and regulations and, thus, enable their companies to differentiate themselves from their competitors.

Also in academic literature, data privacy management is mostly seen from a risk perspective which focusses on corporate data (e.g., from internal research departments) without considering customers' concerns regarding the protection of their personal information. For instance, Buhl (2013) states that privacy protection measures which

address threats such as technology spying and obstruction should be implemented only if the risk-reducing effects outweigh the related costs. Acquisti et al. (2006) link a company's privacy incidents to the negative impacts on its market value. Only to a small extent does the literature consider an upside perspective on data privacy, such as Preibusch et al. (2013) who found that customers who bought a DVD at a privacy-friendly but more expensive online retailer are more satisfied than customers of cheaper but privacy-unfriendly online retailers. Even so, specific data privacy measures which might be implemented to generate customer delight are yet to be considered in the literature. Thus, we raise the following two research questions:

RQ1: Which data privacy measures can companies take?

RQ2: Are some of these measures perceived as attractive measures that delight customers?

To answer these research questions, we first develop an overview of data privacy measures by investigating and consolidating academic literature, legislative texts, company privacy statements, and findings from expert interviews. Second, using the Kano model, we evaluate the customers' perception of these different measures, that is, whether measures are considered to be of must-be, one-dimensional, attractive, or indifferent quality. This paper is organized as follows: We discuss the context of the problem and related work. We outline our methodical approach, derive measures which can be taken by companies to address data privacy concerns and analyze the customers' perceptions of these measures on the basis of the results of two surveys. The discussion provides an overview of the theoretical contribution and managerial implications as well as the paper's limitations. Lastly, we conclude with a summary and an outlook on potential areas of future research.

Problem Context

As previously motivated, public attention regarding data privacy issues is growing. This attention is reflected in different scientific disciplines, such as philosophy, psychology, economics, marketing, law, and information systems (Ahmad & Mykytyn, 2012; Pavlou, 2011). Moreover, privacy incidents such as the scandals previously mentioned as well as their prevention are the subject of numerous research projects[a]. Privacy incidents appear regularly and have consequences for both companies and customers. They are defined by Acquisti et al. (2006) as

[a] Examples: Acquisti et al., 2006; Ahmad & Mykytyn, 2012; Campbell, Gordon, Loeb, & Zhou, 2003; Cavusoglu, Mishra, & Raghunathan, 2004; Dhasarathan, Thirumal, & Ponnurangam, 2015; Hovav & D'Arcy, 2003; Mamonov & Koufaris, 2014; Moshki & Barki, 2016; Nicholas-Donald, Matus, Ryu, & Mahmood, 2011; Nofer, Hinz, Muntermann, & Roßnagel, 2014.

events “involving misuses of individuals’ personal information.” Consequently, customers might become victims of fraud or identity theft (Acquisti et al., 2006). Furthermore, the misuse of personal information might have negative effects on personal relationships, job applications, insurance contracts, and credit decisions.

Smith, Milberg, and Burke (1996) elaborated seven major data privacy concerns of customers relating to Data Collection (storage of large amounts of personal customer data), Data Combination (combination of customer data from different databases to gain additional information about a customer), Internal Secondary Usage (usage of customer data for an unauthorized secondary purpose within the company), External Secondary Usage (disclosure of customer data for an unauthorized secondary purpose outside the company), Errors (deliberate or accidental errors in customer data), Improper Access (unauthorized views and edits of customer data), and Reduced Judgment (automated decision-making based on customer data). The work of Smith et al. (1996) is described as the first and most influential work in the field of data privacy concerns (Preibusch, 2013). Though some publications adapt the concerns (e.g., Hong & Thong, 2013; Malhotra, Kim, & Agarwal, 2004), mostly to better measure the concerns with multi-item survey scales and factor analysis, recent publications also refer to Smith et al. (1996) without any modification of the privacy concerns (e.g., Eastin, Brinson, Doorey, & Wilcox, 2016; Keith, Thompson, Hale, Lowry, & Greer, 2013).

Academic literature provides recommendations for customers themselves as well as public authorities responsible for protecting customers’ privacy rights through laws and regulations (Buchmann, Böhm, & Raabe, 2008; Klingspor, 2016). From a company perspective, privacy incidents may be caused by technical, managerial, organizational, or human failures (Acquisti et al., 2006). Companies might suffer direct economic damage, such as punishment by penalties or loss of market value, as well as indirect effects, such as increasing insurance fees or decreasing customer satisfaction (Acquisti et al., 2006; Nicholas-Donald et al., 2011). The effect of privacy breaches on a firm’s market value is considered in several papers. Cavusoglu et al. (2004) investigate the effect of internet security breach announcements on the market value of publicly traded US firms. A similar study was conducted by Campbell et al. (2003). The authors investigate the effect of public announcements of information security breaches on the market value of publicly traded US firms. Within their analysis, Campbell et al. (2003) differentiate between security breaches which involve unauthorized access to confidential data and security breaches which do not involve confidential data. Interestingly, significant effects can only be shown in the case of the involvement of confidential data (Campbell et al., 2003). In contrast, Nofer, Hinz, Muntermann, and Rossnagel (2014) investigate the direct effect of privacy violations and security breaches on consumers’ investment behavior, which was examined in a laboratory experiment.

Consequently, companies must decide on how to deal with data privacy issues and the related risks. In line with this issue, articles which address companies' handling of data privacy focus on potential threats and how to avoid their occurrence. Occasionally, the management of data privacy is considered as a part of corporate data governance which can be seen as a "framework for assigning decision-related rights and duties in order to be able to adequately handle data as a company asset" (Otto, 2011). As an example, Khatri and Brown (2010) propose to define the role of a data security officer as a part of the data governance in order to specify and monitor access requirements to data. Also, Culnan and Armstrong (1999) argue that companies need to implement a comprehensive governance structure in order to manage data privacy appropriately.

Many authors describe a trade-off between the use of personal data to improve the customer experience, e.g., by personalizing customer services, and the implementation of data privacy measures which are often considered as obstacles to profitability (Schneider, Jagpal, Gupta, Li, & Yu, 2017). Only a limited set of articles considers data privacy measures as an opportunity to create a competitive advantage. For instance, Preibusch et al. (2013) show that appropriate management of data privacy issues may have positive implications on customer satisfaction. By conducting an experiment, the article examined the effects of different levels of data privacy in online retail. With regard to online retail, the authors state that privacy becomes a competitive factor. Sarathy and Robertson (2003) provide a framework which assists companies in implementing a data privacy strategy which considers ethical aspects. The authors propose strategies which exceed the level of data privacy required by laws and regulations. Within a research-in-progress paper, Lyons, van der Werff, and Lynn (2016) propose to examine the effects of different privacy protection approaches on customer trust. In this regard, the authors distinguish organizational privacy protection approaches which are driven by control values and such which are driven by justice values.

However, neither article provides recommendations for specific data privacy measures which can be implemented to address customers' data privacy concerns and increase customer satisfaction. Although the importance of customer satisfaction for long-term customer relationships is commonly accepted, using data privacy to delight customers to gain a competitive advantage or to implement different pricing strategies has yet to be comprehensively examined. To the best of our knowledge, related work does not provide insights into addressing customers' different privacy concerns using concrete measures and the extent to which such measures affect customer satisfaction.

As customer satisfaction has a positive impact on customer loyalty (Gronholdt, Martensen, & Kristensen, 2000) and the value of a company (Matzler & Stahl, 2000), many companies strive to achieve a high level of customer satisfaction. Due to this well-supported relation, the literature provides numerous methods of measuring customer

satisfaction and its antecedents. In this context, a commonly used method to measure the quality of service attributes is SERVQUAL (Ladhari, 2009; Parasuraman, Zeithaml, & Berry, 1985). As part of a causal structure, the concept of customer satisfaction can be analyzed with the help of structural equation modeling and neural networks (Hackl & Westlund, 2000). Bartikowski and Llosa (2004) analyze further methods, namely Penalty Reward Contrast Analysis, Correspondence Analysis, Dual Importance Mapping, and the Kano model which was originally proposed by Kano, Seraku, Takahashi, and Tsuji (1984). The Kano model has been discussed and applied in many theoretical and empirical research projects (Füller & Matzler, 2008; Löfgren & Witell, 2008) as it provides a comprehensive presentation of attributes of products or services which influence the degree of customer satisfaction. For instance, the model has been used by Lai and Wu (2011) in order to gain insights in the customers' needs of a public transport company and by Arbore and Busacca (2009) who studied determinants of customer satisfaction for a retail bank.

Research Method

To answer the research questions, we first identify and structure the field of possible data privacy measures and then use the Kano model and data from two online surveys to evaluate customers' perceptions regarding different data privacy measures.

Identification of Data Privacy Measures

As a basis for identifying data privacy measures, we conducted a comprehensive search for relevant statements, that is, any piece of information on any type of action which addresses customers' data privacy concerns. Therefore, our sources are legislative texts in particular (European General Data Protection Regulation (EU-GDPR), German Bundesdatenschutzgesetz (BDSG), and Telemediengesetz (TMG)) but also scientific literature. Beyond using the pertinent literature known to us from prior research on data privacy, we conducted a structured literature search in the databases AISeL, EBSCOhost, and JSTOR. In these databases, we used the following search term: ("data privacy") AND ("concern" OR "issue") AND ("measure" OR "protection" OR "policy"). As interactions between companies and customers and also the amount of generated customer data changed tremendously with the emergence of smartphones and other digital channels, we decided to consider articles which were published within the last ten years (2008-2017). The search was limited to peer-reviewed articles. In total, we found 128 articles. By conducting an abstract screening, we identified four potentially relevant articles (Bélanger & Crossler, 2011; Clement & Obar, 2016; Keith, Babb, Furner, Abdullat, & Lowry, 2016; Payne,

Landry, & Dean, 2015). The in-depth analysis resulted in two papers that contain concrete statements for deriving feasible data privacy measures: Clement and Obar (2016), who examine the data privacy transparency of Canadian internet carriers and Payne et al. (2015), who focus on a list of different laws, regulations, and frameworks and attempt to reconcile the conflicting agendas of companies and customers. Practical recommendations from Audatis Consulting (2016) were used to complement the statements from a practitioner-oriented perspective. Furthermore, we analyzed nine corporate privacy statements across industries: Amazon (2017), Apple (2017), Deutsche Bank (2017), Dropbox (2017), easyJet (2017), Facebook (2017), Telekom DE-Mail (2017), Tesla Motors (2017), and Zalando (2017). We aimed to sample these privacy statements from corporations in different industries, partially known for a strong reliance on gathering and analyzing customer data or a strong obligation to protect customer data. Additionally, we conducted three expert interviews, each lasting approximately 30 to 60 minutes. In the first interview, we talked to an in-house data privacy officer of a German automotive company in order to gain an overview of existing and potential data privacy measures as well as the challenges and difficulties entailed. To verify existing statements and to check whether we had covered all relevant aspects, we conducted a second interview with a researcher who was working on a project with the goal of developing a long-term data privacy strategy for a German bank. For instance, this interviewee mentioned that customers may want to know which personal data a company stores about them. This statement was later considered to develop a data privacy measure that allows customers to easily get a copy of all their personal data stored and processed by a company. To complement our research with input from a legal perspective, we interviewed a lawyer who works for a renowned German business law office and consults on data privacy. Therefore, he possesses expertise in European privacy laws and regulations.

The examination of the different sources resulted in 202 statements. All statements were then grouped by semantic similarity. In doing so, the authors jointly decided on the grouping of the statements. Without having pre-defined groups, each statement was either used to create a new group with a particular data privacy measure or mapped to an existing group. In the rare case of disagreement between the authors, every author firstly explained the reasons for his preferred grouping then the team of authors discussed the different aspects and repeated the grouping process for the respective measure. The procedure resulted in 32 groups, each consisting of one or several statements regarding a particular data privacy measure. From each of the groups of statements, we derived a single measure which addresses all statements within the group. After the formulation of the measures, we assigned each of the measures to one or more specific customer data privacy concerns. To validate the mapping of all measures to the seven concerns, eleven aviation and retail customers were asked for their assessment in an ex-post quality

check. The majority of customers mapped 27 out of all 32 measures to the same concern as the team of authors. For almost all of the remaining five measures, customers' second most frequent classification was congruent with the authors' mapping and the measure had content-related similarity with both the authors' and the customers' mapping. As only slight differences in customers' and experts' assessment can be observed, this ex-post quality check suggests adequate data quality.

Evaluation of Customers' Perceptions

After the derivation of data privacy measures and their assignment to specific data privacy concerns, we now focus on determining their effect on customer satisfaction. As the context at hand requires the possibility of individual investigation of each measure and applicability to hypothetical cases, we decided to use the Kano model. To evaluate customers' perceptions regarding the identified data privacy measures, we conducted two online surveys.

Kano Model

The Kano model describes customer satisfaction on the basis of the degree of implementation or availability of certain attributes of products or services (Kano et al., 1984; Matzler, Hinterhuber, Bailom, & Sauerwein, 1996). Thereby, the perceived degree of implementation or availability depends on the customers' expectations. The model differentiates between four major types of factors. We list these factors in Table 1 and illustrate their nature in Figure 1.

Table 1. List of the Kano model factors as described by Matzler et al. (1996) and applied to the data privacy context

Factor	*Customers' expectations*	*Effect on satisfaction*	
		if implemented	*if not implemented*
Attractive quality (delighter)	Customers do not expect implementation of measure	positive	none
One-dimensional quality (performance need)	Customers explicitly demand implementation of measure	positive	negative
Must-be quality (basic need)	Customers implicitly demand implementation of measure	none	negative
Indifferent quality	Customers are indifferent to implementation of measure	none	none

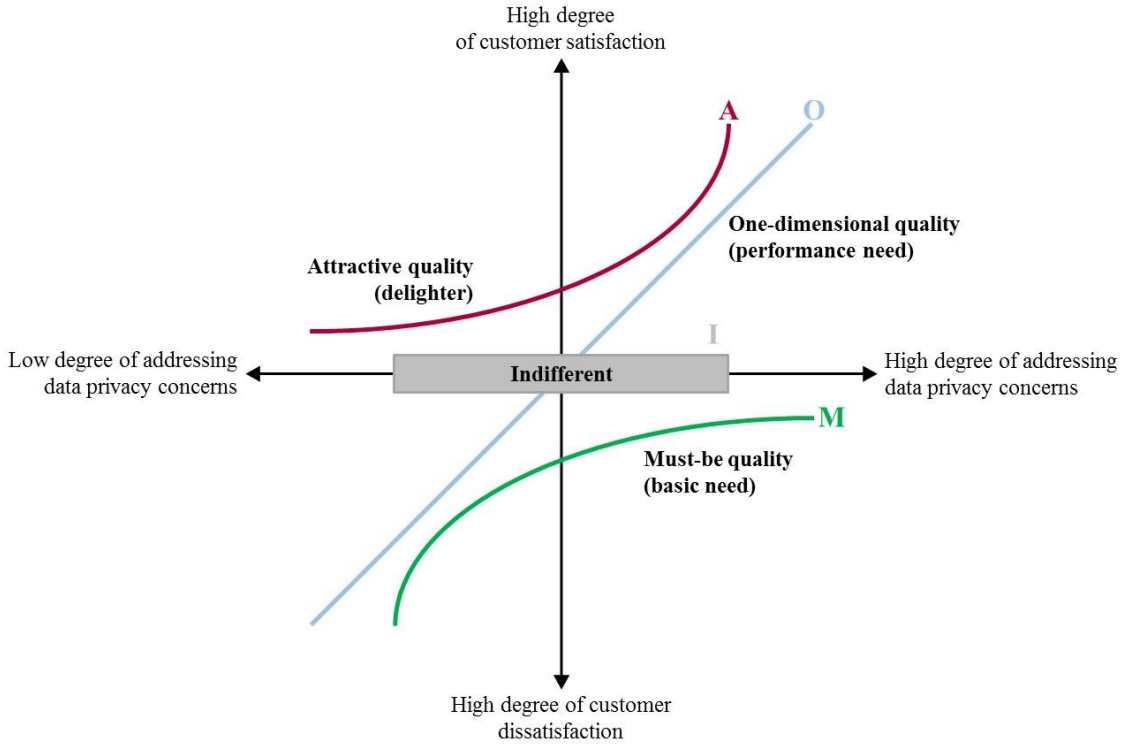

Figure 1. Illustration of the Kano model factors as described by Matzler et al. (1996) and applied to the data privacy context

The classification of a measure as a certain factor depends on customers' answers to both a functional and a dysfunctional question (Kano et al., 1984; Matzler et al., 1996). That is, customers are asked about their evaluation of the hypothetical case in which a measure is implemented and a case in which it is not. Each time, they can choose one of five possible answers: "I like it that way," "It must be that way," "I am neutral," "I can live with it that way," and "I dislike it that way." The different answers do not stand for a level of acceptance and there is no ordinal scale. Each possible combination of answers can be interpreted in an individual manner and leads to a certain pre-defined classification (Kano et al., 1984; Matzler et al., 1996), as shown in Figure 2.

Functional answer \ **Dysfunctional answer**	I like it that way.	It must be that way.	I am neutral.	I can live with it that way.	I dislike it that way.
I like it that way.	Q	A	A	A	O
It must be that way.	R	I	I	I	M
I am neutral.	R	I	I	I	M
I can live with it that way.	R	I	I	I	M
I dislike it that way.	R	R	R	R	Q

Legend

A = *Attractive quality (delighter)*
O = *One-dimensional quality (performance need)*
M = *Must-be quality (basic need)*
I = *Indifferent quality*
R = *Reverse quality*
Q = *Questionable result*

Figure 2. Derivation of Kano model factors based on Matzler et al. (1996)

The easiest and most intuitive way to determine the final classification of a measure as one of the Kano model factors for the overall sample is to choose the classification which appeared the most often, that is, the mode (Berger et al., 1993). However, determining and presenting the results solely based on the mode leads to a lack of further information about other frequently chosen categorizations. This is especially disadvantageous if the shares of participants who evaluated the measures as one of the other frequently chosen categorizations are of similar size (Schaule, 2014). There are numerous ways to determine whether a categorization based on the mode is significant as compared to other frequently chosen ones. Lee and Newcomb (1996) use the variable category strength, which is calculated as the difference between the shares of the most and second most frequently chosen categorizations. If the category strength is higher than six percent, they conclude that assigning the attribute to only one category is justified. If it is below six percent, they assign the attribute to a mixed category. A more sophisticated approach to decide whether the frequencies of the most and second most frequently chosen categorizations are significantly different is the test proposed by Fong (1996). It assumes significance if the category strength is higher than a reference value calculated based on the observed frequencies and the sample size. If determining a result based on the mode is not reasonable, Berger et al. (1993) propose to apply the (A, O, M) < > (I, R, Q) rule. Thereby, categorizations as attractive, one-dimensional, or must-be ((A, O, M) group) mean that an attribute has an influence on customer satisfaction. Categorizations as indifferent, reverse, or questionable ((I, R, Q) group) mean that an attribute has no influence on satisfaction. If one of the most and second most frequently chosen categorizations belong to one group and the remaining one to the other group, the (A, O, M) < > (I, R, Q) rule is applicable. It is executed by determining the group with the highest share of categorizations of the overall sample and then selecting the most frequently chosen categorization within this group. In the current work, we will use the following approach for the determination of the final classification of our measures as one of the Kano model factors: we assign a category based on the mode if the category strength is significant at a five-percent level according to the Fong test. If the category strength is not significant and the (A, O, M) < > (I, R, Q) rule is applicable, we execute this rule. If it is not applicable, we assign the measure to a mixed category following Lee and Newcomb (1996). Additionally, we list all categorizations which do not exhibit a significant difference according to the Fong test as compared to the most frequently chosen one.

An alternative, continuous approach which avoids assigning categories to attributes altogether is the calculation of satisfaction (“better”) and dissatisfaction (“worse”) coefficients (Berger et al., 1993; Schaule, 2014). The satisfaction coefficient is calculated as the sum of all participants who categorized an attribute as a factor which has the power to increase their satisfaction (attributes of attractive and one-dimensional quality) over the sum of

all participants who categorized the attribute as attractive, one-dimensional, must-be, or indifferent. The satisfaction coefficient's possible values range from 0 to 1. Reversely, the dissatisfaction coefficient is calculated as the sum of all participants who categorized the attribute as a factor which has the power to decrease their satisfaction (measures of must-be and one-dimensional quality) over the same denominator. Its value range is -1 to 0. The coefficients thus state the mean importance of attributes over all survey participants with regard to their power to both improve customer satisfaction and avoid customer dissatisfaction. In particular, it can be used to prioritize the implementation of measures (Berger et al., 1993). We will additionally use satisfaction and dissatisfaction coefficients to graphically represent and verify the results of our surveys.

Surveys

To determine the customers' evaluation of the identified data privacy measures, we conducted two Internet-based surveys. To enable the participants to assume a perspective as natural as possible and to illustrate the situation, we decided to use specific, well-known, and simple scenarios which relate to an exemplary industry sector for which data privacy is a considerable issue. That is, the sectors should feature a business-to-consumer market with a significant occurrence of processed customer data. To be able to consider the possible exchange of customer data between companies, cooperation agreements should exist between major actors in the industry. Furthermore, companies should provide loyalty programs because they are typically based on gathering data on a customer's behavior over a long period.

All of these requirements are fulfilled by the aviation sector. A considerable amount of customer data is collected at different interaction points (Clayton & Hilz, 2015). Data are transmitted to public authorities, airport operators, or other airlines which are partners in global alliances (Harris, 2007). Furthermore, airlines often provide loyalty programs (e.g., Miles & More, Emirates Skywards). Finally, the aviation sector is a commonly known industry. Therefore, we decided to face the participants with a typical customer process from the aviation sector.

To ensure high quality results, we first ran a pretest followed by the main survey. In the pretest, we asked 85 German-speaking participants to imagine booking a flight through an airline's website. Each participant was asked a functional and a dysfunctional question for each of the measures. Using the insights of the pretest, we made several modifications to the main survey: for improving the response rate, we mixed the questions with invitations to guess the correct answers to fun-fact questions about the aviation sector. For improving understandability, we grouped the questions with regard to the data privacy concerns they address and preceded them by short explanations of these concerns. The following example of an explanation, a functional, and a dysfunctional

question demonstrates the survey's design. The example refers to a measure which addresses the concern External Secondary Usage (see measure D1 in Table 2 for detail). In the survey, the questions regarding this measure were preceded by the following explanation to acquaint the participants with the concern: "Your customer data may be used by a third party outside of the company for a purpose not previously agreed upon. The company implements the following measures:" The functional question directly related to the measure then read: "Information. If your customer data are passed on to external third parties, you are informed." The dysfunctional question was: "If your customer data are passed on to external third parties, you are not informed." Afterwards, the participants were asked a functional and a dysfunctional question each for every remaining measure which addresses the concern External Secondary Usage. To answer the functional and the dysfunctional question, the participants can choose one of the five previously mentioned possible answer options. In this way, we asked the participants about each of the 32 identified measures, resulting in 32 pairs of questions, each of them addressing one of the data privacy concerns.

227 German-speaking participants completed the main survey, 219 of whom correctly answered a control question. The participants were recruited via social media and email and incentivized through a lottery of vouchers for an online retailer. The sample mostly consists of students (78%) and employees (16%). The age of the participants is between 18 and 57 years (average age 25.4 years). The survey was completed by both women (55%) and men (45%). The majority of the participants is well-educated. The share of participants holding a university degree is 51%. Another 42% of the participants achieved degrees with the matriculation standard.

In order to verify the initial results, we subsequently conducted a second survey. To ensure the comparability of both surveys, we used the same questionnaire as in the first survey. However, to take a step towards a generalizability of the results, the participants of the second survey were faced with a modified scenario. Due to its growing importance and the vast amount of customer data which is collected and processed within a purchase process, we decided to consider the online retail sector. Most of the customers create personal accounts. Furthermore, leading online retailers provide own loyalty programs (Mohammed, 2014). Usually, customer data are transferred to external logistics service providers in order to ship the products to the customers. Therefore, the online retail sector fulfills the previously defined requirements. In this context, the participants of the second survey were asked to imagine ordering a smartphone on the website of an internationally renowned online retailer.

299 German-speaking participants completed the second survey, 270 of whom correctly answered a control question. As in the first survey, participants were recruited via social media and email and incentivized through a lottery of vouchers for an online retailer. Most of the participants are students (77%) or employees (17%). The age

of the participants ranges between 18 and 59 years (average age 24.6 years). The majority of the participants is well-educated. The share of participants holding a university degree is 50%. Another 45% of the participants achieved degrees with the matriculation standard. The majority of the participants (86%) stated that they have not completed a similar survey before, indicating that the set of participants differs significantly from the first survey.

Results

In the first part of this section, we present the overview of possible data privacy measures for companies which resulted from the research process previously described. This overview forms the basis of the presentation of the survey results in the second part of this section, that is, the perceptions which customers have of the identified privacy measures.

Data Privacy Concerns and Measures

As described above, the overview of possible data privacy measures is compiled from academic literature, legislative texts, practical recommendations, corporate privacy statements, and expert interviews. From all sources, we collected 202 statements merged to 32 groups. From these groups, we derived particular data privacy measures and mapped them to the seven privacy concerns described by Smith et al. (1996). The measures are presented in Table 2, numbered and grouped according to the seven concerns. Each measure's detailed explanation is preceded by a short description printed in bold. Some of these short descriptions show recurring themes across concerns, e.g., "empowerment" taking on different facets with respect to most concerns. In the last column, we present the references from which we derived the measures and their detailed descriptions. In summary, Table 2 represents a comprehensive list of actions which can be taken by companies to mitigate the risk of displeasing customers and to create the potential for delighting customers regarding data privacy.

Table 2. Measures addressing the seven privacy concerns

#	*Detailed description*	*Reference(s)*
A	**Data Collection**	
A1	**Information.** The purpose, scope, and storage time of the data collection and the involved advantages, risks, resulting rights, and obligations are clearly explained to the customer.	§33 (1) BDSG; §13 (1) TMG; 5 (1.a), 12 (1), 14 (1), 15 EU-GDPR, Facebook (2017), Telekom DE-Mail (2017), Tesla Motors (2017), Zalando (2017)
A2	**Anonymization.** Customer data are, as good as is possible, stored anonymously to prevent backtracking of individual customers.	§3a BDSG; §13 (6) TMG; 23, 30 (1), 30 (1.a), 30 (2.b) EU-GDPR, Apple (2017), Deutsche Bank (2017)
A3	**Restraint.** Only the customer data absolutely necessary to provide the agreed service are collected. The data are deleted as soon as the purpose of their collection no longer applies.	§3a BDSG; §14 (1), §15 (1) TMG; 5 (1.b), 5 (1.c), 23 EU-GDPR, Deutsche Bank (2017), Dropbox (2017), Facebook (2017)
A4	**Empowerment.** The customer can extend, limit or revoke the permission to store and use his data easily, quickly, free of charge and at any time.	6 (1.a), 6 (1.b), 7 (3), 12 (1.a), 17, 17a, 19 (1) EU-GDPR, Amazon (2017), Apple (2017), Deutsche Bank (2017), Tesla Motors (2017), Zalando (2017)
A5	**Data release.** At the request of the customer and without a long delay, the company provides a set of his personal data free of charge in an easily readable form. Furthermore, the customer has the right to pass these data on to other companies.	12 (1.a), 12 (2), 12 (4), 18 (2) EU-GDPR, Deutsche Bank (2017), easyJet (2017), Facebook (2017), Telekom DE-Mail (2017), Zalando (2017)
B	**Data Combination**	
B1	**Information.** The customer is informed if the company combines his data from various internal and external sources.	5 (1.a), 12 (1), 14a, 15 EU-GDPR, Facebook (2017), Tesla Motors (2017)
B2	**Anonymization.** If the company combines customer data from various internal and external sources, combination and storage are carried out using anonymous data to prevent backtracking of individual customers.	§13 (4), §15 (3) TMG; 23, 30 (1), 30 (1.a), 30 (2.b) EU-GDPR
B3	**Restraint.** If customer data are collected for different purposes, the data sets are stored in different databases and are not combined.	Attachment to §9 (1) BDSG; 13 (4) TMG; 23 EU-GDPR, Deutsche Bank (2017)
B4	**Empowerment.** The customer decides whether the company is allowed to combine data from various internal and external sources and can change his decision at any time.	17a EU-GDPR
C	**Internal Secondary Usage**	
C1	**Information.** The customer is informed whether and what data are passed on within the company or group of companies and for what purposes.	§13 (5) TMG; 5 (1.a), 12 (1), 14 (1), 15 EU-GDPR, Facebook (2017), Tesla Motors (2017)
C2	**Deletion.** Customer data are deleted as soon as the original reason for the collection no longer applies or the customer withdraws his permission to use his data.	§35 (2) BDSG; §13 (4), §15 (7) TMG; 5 (1.e), 17 EU-GDPR, Deutsche Bank (2017), Dropbox (2017), Facebook (2017)
C3	**Tracking.** Entering, viewing, altering, and deleting customer data are recorded to make it possible to retrace who changed the data when, and in what manner at any time. The customer can either directly view the log file or is informed about any alterations of his personal data.	Attachment to §9 (1) BDSG; 17b, 23 EU-GDPR
C4	**Restraint.** If customer data are collected for different purposes, the data sets are stored in different databases and are not combined.	Attachment to §9 (1) BDSG; 13 (4) TMG; 23 EU-GDPR, Deutsche Bank (2017)
C5	**Empowerment.** Customers have the opportunity to easily decide which of their personal data are shared with other departments of the company and/or used for other purposes.	6 (1.a), 6 (1.b), 12 (1.a), 17a EU-GDPR, Facebook (2017)
D	**External Secondary Usage**	
D1	**Information.** If customer data are passed on to external third parties, the customer is informed.	§13 (5) TMG; 5 (1.a), 12 (1), 14 (1), 15 EU-GDPR, Amazon (2017), Clement and Obar (2016), Facebook (2017), Telekom DE-Mail (2017), Tesla Motors (2017)
D2	**Guidelines.** If customer data are passed on to external third parties, the company ensures that the data are only used in the manner agreed on with the customer through contracts or binding commitments to data protection regulations.	§11 (1) (2) BDSG; 5 (1.a), 26 (1), 26 (1.a), 26 (2), 26 (2.a), 27, 40, 42 (1), 43 EU-GDPR, Amazon (2017), Dropbox (2017), Clement and Obar (2016), easyJet (2017), Facebook (2017), Telekom DE-Mail (2017), Tesla Motors (2017)
D3	**Compliance check.** If customer data are passed on to external third parties, the company or an independent certification organization regularly checks the external third party's compliance with data privacy regulations.	26 (1), 26 (1.a) EU-GDPR, Deutsche Bank (2017), Telekom DE-Mail (2017)

#	*Detailed description*	*Reference(s)*
D4	**Codification.** If customer data are passed on to external third parties, data are only forwarded in aggregated or codified form (e.g. income class instead of exact yearly income).	Tesla Motors (2017)
D5	**Anonymization.** If customer data are passed on to external third parties, the data are forwarded anonymously.	§30 (1) BDSG; §15 (5) TMG, Amazon (2017)
D6	**Restraint.** The company does not pass on customer data to external third parties.	Tesla Motors (2017)
D7	**Empowerment.** The customer has the choice to easily permit or deny sharing his data with external parties.	7 (3), 12 (1.a), 17, 17a EU-GDPR, Amazon (2017), Apple (2017), Morey et al. (2015), Payne et al. (2015), Zalando (2017)
E	**Errors**	
E1	**Reviews.** Customer data are checked regularly by the company for completeness, accuracy, and being up-to-date.	5 (1.d) EU-GDPR, Payne et al. (2015), Tesla Motors (2017)
E2	**Protective measures.** The company ensures that no customer data are destroyed or lost by technical and organizational means (e. g., double data storage).	Attachment to §9 (1) BDSG; §13 (7) TMG; 22 (1), 23, 30 (1), 30 (1.a), 30 (2.b) EU-GDPR, Telekom DE-Mail (2017), Tesla Motors (2017), Zalando (2017)
E3	**Employee supervision.** Employees with access to customer data are selected carefully, their behavior is checked regularly, and they are held responsible for malpractice.	30 (1.a), 30 (2.b) EU-GDPR, Tesla Motors (2017)
E4	**Tracking.** Entering, viewing, altering, and deleting customer data are recorded to make it possible to retrace who changed the data when, and in what manner at any time. The customer can either directly view the log file or is informed about any alterations to his personal data.	Attachment to §9 (1) BDSG; 17b, 23 EU-GDPR
E5	**Empowerment.** The customer has access to his data to correct errors, make alterations, or delete data. If he is not provided with direct access to edit his data, they are changed by the company on request.	16 EU-GDPR, Amazon (2017), Apple (2017), Deutsche Bank (2017), Payne et al. (2015), Tesla Motors (2017)
F	**Improper Access**	
F1	**Information.** If the protection of customer data was violated and their security is at risk, the company immediately informs the customer and the authorities.	31 (1), 31 (2), 32 (1) EU-GDPR
F2	**Protective measures.** Storage and transmission of customer data are protected by technical (e.g., password protection, encryption) and organizational means (e.g., access control, dual control principle).	§9 BDSG; Attachment to §9 (1) BDSG; §13 (4), §13 (7) TMG; 5 (1.b), 22 (1), 23, 30 (1.a), 30 (2.b) EU-GDPR, Amazon (2017), Apple (2017), Deutsche Bank (2017), Dropbox (2017), easyJet (2017), Payne et al. (2015), Telekom DE-Mail (2017), Tesla Motors (2017), Zalando (2017)
F3	**Secure server location.** The company ensures that customer data are stored and processed only on its own servers within the European Union or countries trusted by the European Commission.	41 (1) EU-GDPR, Clement and Obar (2016), Telekom DE-Mail (2017)
G	**Reduced Judgment**	
G1	**Information.** The customer is informed whether a decision was made by an automated system or by an employee of the company. At the customer's request, the reasons for the decision are communicated and explained.	§6a BDSG; 5 (1.a), 12 (1), 15 EU-GDPR
G2	**Reviews.** Automated decision processes are continuously tested and checked for deviations.	20 (1), 20 (1.b) EU-GDPR
G3	**Restraint.** Decisions which entail legal consequences (e.g., granting a credit) are never made only on the basis of automated systems.	§6a BDSG; 20 (1), 20 (1.b) EU-GDPR

Customers' Evaluation of Data Privacy Measures

Companies need to be aware of the customers' evaluation of these data privacy measures which forms the basis for deriving implications for companies' data privacy policies. To determine the customers' view regarding the different identified data privacy measures, we applied the Kano model in two empirical studies as described in the previous research method section. Table 3 shows the results. Thereby, the measures are numbered and grouped

according to the addressed concerns and named with the short descriptions presented in Table 2. For both the aviation and the retail survey, we present the category strength and the final categorization of each measure as one of the Kano model factors. The final categorizations were determined following the approach which we described in the previous Kano model section. To illustrate this approach, we use measure A3 as an example. For the aviation survey, the difference between the share of the most and second most frequently chosen factor is 12%, a category strength which is significant at a five-percent level according to the Fong test. The final categorization thus is the most frequently chosen factor which is of a must-be quality. For the retail survey, the differences between the share of the most (one-dimensional quality) and second most (attractive quality) frequently as well as the most and third most (must-be quality) frequently chosen factor are not significant according to the Fong test. The (O + A + M) < > (I + R + Q) rule is not applicable as both the most and second most frequently chosen factor belong to the (O + A + M) group. Consequently, the measure is assigned to the mixed category and all three categorizations are listed.

Table 3. Empirical results of the data privacy measures' evaluation via the Kano model in two surveys

		Aviation survey (n = 219)		**Retail survey (n = 270)**		
#	*Short description*	*Category strength*	*Categorization*	*Category strength*	*Categorization*	*Accordance*
A	**Data Collection**					
A1	Information	21% *	M	30% *	M	yes
A2	Anonymization	10% *	A	11% *	A	yes
A3	Restraint	12% *	M	3% [2]	Mixed (O, A, M)	partially
A4	Empowerment	18% *	M	3% [2]	Mixed (M, A, O)	partially
A5	Data release[b]	4% [2]	Mixed (M, A, O)	3% [1]	A	partially
B	**Data Combination**					
B1	Information	11% *	I	4% [1]	M	no
B2	Anonymization	8% *	M	11% *	M	yes
B3	Restraint	18% *	I	30% *	I	yes
B4	Empowerment	13% *	A	14% *	A	yes
C	**Internal Secondary Usage**					
C1	Information	21% *	M	20% *	M	yes
C2	Deletion	20% *	M	21% *	M	yes
C3	Tracking	17% *	A	4% [2]	Mixed (A, O, I, M)	partially
C4	Restraint	16% *	A	23% *	I	no
C5	Empowerment	13% *	A	13% *	A	yes
D	**External Secondary Usage**					
D1	Information	49% *	M	46% *	M	yes
D2	Guidelines	58% *	M	45% *	M	yes
D3	Compliance check	17% *	M	22% *	M	yes
D4	Codification	4% [2]	Mixed (M, A, I)	3% [1]	M	partially
D5	Anonymization	34% *	M	24% *	M	yes
D6	Restraint	1% [2]	Mixed (A, O)	6% [2]	Mixed (A, O)	yes

[b] Due to technical complications in the process of revising and providing the retail survey online, the questions regarding measure A5 were answered by 143 instead of 270 participants.

D7	Empowerment	14% *	M	8% *	M	yes
E	**Errors**					
E1	Reviews	60% *	I	64% *	I	yes
E2	Protective measures	49% *	I	32% *	I	yes
E3	Employee supervision	37% *	M	40% *	M	yes
E4	Tracking	4% [1]	A	1% [2]	Mixed (M, A, O, I)	partially
E5	Empowerment	11% *	M	13% *	M	yes
F	**Improper Access**					
F1	Information	42% *	M	43% *	M	yes
F2	Protective measures	40% *	M	44% *	M	yes
F3	Secure server location	4% [1]	A	4% [1]	A	yes
G	**Reduced Judgment**					
G1	Information	11% *	I	17% *	I	yes
G2	Reviews	4% [1]	M	4% [1]	M	yes
G3	Restraint	1% [1]	M	10% *	M	yes

Legend:
** = Categorization significant at a five-percent level according to Fong test*
[1] = (O + A + M) < > (I + R + Q) rule applicable
[2] = (O + A + M) < > (I + R + Q) rule not applicable
A = Attractive quality (delighter)
O = One-dimensional quality (performance need)
M = Must-be quality (basic need)
I = Indifferent quality

The results of both the aviation and the retail survey show that in both scenarios, five measures are considered by the participants to be of indifferent quality. These measures do not allow distinctive interpretations toward any direction. In each scenario, 17 out of 32 measures are categorized as basic needs (must-be quality). Furthermore, the categorization as basic need is the most frequent one for two measures belonging to the mixed category in each survey. The realization of these measures is not rewarded. Instead, it is a basic prerequisite when engaging in business with the company. An example for a measure of must-be quality is D2 which addresses the concern External Secondary Usage: if customer data are passed on to external third parties, the company ensures that the data are only used in the manner agreed on with the customer through contracts or binding commitments to data protection regulations. Basic needs can be predominantly found among measures addressing the concerns External Secondary Usage (5-6 measures out of 7 categorized as a basic need in both scenarios), Improper Access (2/3), and Reduced Judgment (2/3). They are also frequently found among measures addressing the concern Data Collection (3/5) in the aviation scenario. These basic needs can be considered a necessary evil because they have downside risks if not implemented but offer no upside opportunities if implemented. In both surveys, no measure is considered to be a performance need. However, this factor occurs among the most frequent categorizations in the mixed category for two measures in the aviation and four measures in the retail scenario. The constituting properties of a performance need are, in addition to having a negative impact if not implemented, that it also might increase customer satisfaction when implemented properly.

Seven measures are categorized as delighters in the aviation scenario and five in the retail scenario. Furthermore, three delighters occur among the most frequent categorizations in the mixed category in the aviation scenario and five in the retail scenario. The implementation of these measures is not required by the customers but may please them. Not implementing these measures has no negative impact. These measures go beyond the data privacy measures which customers expect. In the aviation scenario, delighters can be predominantly found among measures addressing the concern Internal Secondary Usage (3 measures out of 5 categorized as a delighter). In the retail scenario, the delighters are distributed over measures addressing four different concerns and there is no concentration observable. In both scenarios, customers can be delighted by storing their data in an anonymized form (A2), empowering them with regard to the combination of their data (B4) and data sharing within the company (C5), and storing their data on servers with a secure location (F3).

Overall, there are eight (25%) measures which exhibit different categorizations in the aviation scenario as compared to the retail scenario. They address five different concerns and include all Kano model factors with the previously mentioned exception of performance needs. For three of these measures, the categorization in one of the scenarios corresponds to the most frequent result of the mixed category categorization in the other scenario. That is, these categorizations are not equal but the tendencies are similar. The remaining 24 measures are categorized in the same way by participants of the aviation and the retail survey. These measures address all seven concerns and include all Kano model factors. All measures addressing the concerns Improper Access and Reduced Judgment exhibit the same results. To assess the reliability of the measure categorizations across the two different scenarios, we conducted a test of inter rater reliability with two raters. Thereby, the categorizations of measures in the aviation scenario as shown in Table 3 were interpreted as the choice of the first rater and those of the retail scenario as the choice of the second rater. The percent agreement is 0.75 and the Cohen's Kappa is 0.61, indicating a substantial strength of agreement according to Landis and Koch (1977).

The similarity of the measures' categorizations is also reflected in Figure 3. It represents a satisfaction-dissatisfaction diagram of the results of both surveys. The x-coordinate indicates the satisfaction coefficient, the y-coordinate states the dissatisfaction coefficient. We present the data points for both scenarios and connect them with a line. Few measures exhibit relatively large differences between the aviation and the retail surveys' results (e.g., A4, C3 and C4) while the data points for the majority of measures are in rather close proximity to their counterparts. The indication of high reliability of the 32 measures' satisfaction and dissatisfaction coefficients across the two scenarios is confirmed by their high and highly significant Pearson's correlations: 0.91 (p-value $<< 0.001$) for the satisfaction coefficients and 0.96 (p-value $<< 0.001$) for the dissatisfaction coefficients.

We limited the range of the axes to the actually occurring values for better readability. The fact that the dissatisfaction coefficient's axis exhibits a broader range than the satisfaction coefficient's axis as well as the relatively high concentration of measures in the bottom left quadrant emphasize the dominance of measures of must-be quality. They will decrease the overall customer satisfaction if not implemented but will only moderately increase it if implemented. However, the opposite case can be observed as well. Implementing measure B4, for example, has the potential to increase the overall satisfaction of a notable share of survey participants while not implementing it will have a relatively small negative effect.

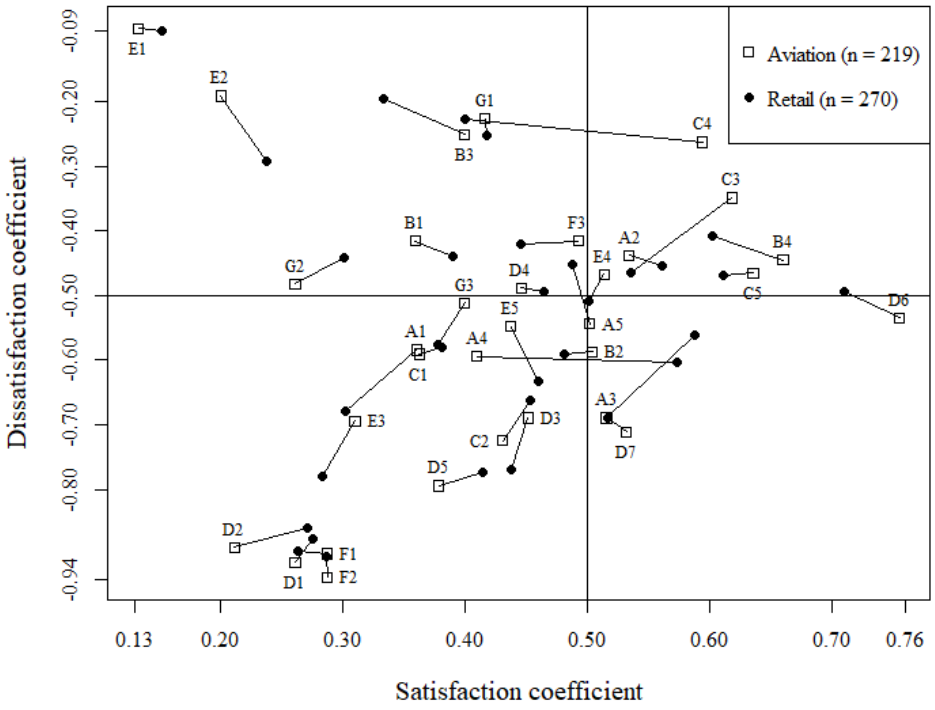

Figure 3. Joint satisfaction-dissatisfaction diagram of the results of both surveys

These results are underlined by a more detailed look at the categorization of measures on the participant-level. For both scenarios, Table 4 presents the minimum, median, mean and maximum count of categorizations as a specific Kano model factor per survey participant. It also indicates the share of participants who categorized zero and at least ten measures as the specific Kano model factor. Measures of must-be quality are dominant: more than 60% of the participants of both surveys categorized more than 10 of our 32 measures as such basic needs. However, only 8% of participants of the aviation survey and 9% of participants of the retail survey evaluated none of the measures as attractive. This implies that data privacy has the overall potential to improve the satisfaction of a very large share of customers: 92% (aviation) and 91% (retail) see at least one data privacy measure as delighter, that is, as a measure with upside potential only. 32% (aviation) and 29% (retail) categorized more than 10 measures as

such delighters. All but one (99.5%, aviation) and all but six (97.8%, retail) survey participants categorized at least one measure as performance need or delighter, that is, as a measure with upside potential.

Table 4. Statistics regarding the number of categorizations per Kano model factor and survey participant

	Aviation survey (n = 219)						**Retail survey (n = 270)**					
	min	*med*	*mean*	*max*	*none*	*>= 10*	*min*	*med*	*mean*	*max*	*none*	*>= 10*
Attractive quality	0	7	7,4	21	8%	32%	0	6	6,7	25	9%	29%
One-dimensional quality	0	5	6,2	28	7%	20%	0	5	6,4	30	9%	21%
Must-be quality	0	11	11,1	29	3%	60%	0	11	10,7	30	5%	62%
Indifferent quality	0	6	7,0	28	5%	26%	0	6	7,3	30	3%	28%
Reverse quality	0	0	0,3	4	78%	0%	0	0	0,3	10	84%	0%
Questionable result	0	0	0,1	5	95%	0%	0	0	0,1	7	93%	0%

Discussion

Theoretical Contribution

This paper contributes to the body of knowledge about data privacy. Most scientific and practitioner-oriented literature describes data privacy as necessary evil that organizations have to deal with in order to mitigate risks. We shed light on the upside of data privacy beyond mere risk management. Our paper consists of two main contributions. First, we created a set of 32 specific data privacy measures that address the customers' seven main data privacy concerns. We derived these measures from several legislative texts of the German and European law system as well as from scientific and practitioner-oriented literature and corporate privacy statements. With the consideration of the European General Data Protection Regulation (EU-GDPR) which will become applicable law in May 2018, we took a future-oriented perspective and incorporated the most recent legislation into our research. The consolidated and enriched set of measures from several sources was evaluated in discussions with data privacy experts. It can serve as a basis for the development of further data privacy concepts and strategies. Second, we provided an evaluation of these data privacy measures by customers. Via two online surveys, we empirically captured customers' perceptions of the identified data privacy measures as must-be, one-dimensional, attractive, or as indifferent. A similar classification of most measures across both surveys showed a consistent and reliable picture of customer sentiment. A further analysis of the survey responses with a satisfaction-dissatisfaction diagram strengthened the dominating assertion of data privacy measures as necessary evil. However, among both industry scenarios, we showed that the implementation of certain data privacy measures has the potential to delight customers. The vast majority of participants could be delighted with data privacy measures and almost a third of

all participants could be delighted by 10 or more measures. Our research specifically highlights the upside of data privacy. In summary, the customers' evaluation of data privacy measures as presented in this paper is a starting point for all researchers who try to understand customer sentiment toward specific measures and data privacy in general.

Limitations

Researchers and practitioners should be aware of the limitations of this research. First, the derivation of data privacy measures focused on Germany and Europe. Other regions with different cultures and legislative systems might yield other or further measures. Second, the results of the empirical part of this research should only be interpreted in a company- and customer-specific manner. We selected the booking process for a flight and the online purchase of a product to present realistic scenarios to our survey participants who were predominantly students, that is, potential customers of the present and future. To verify the validity of the conclusions for other industry scenarios and customer groups, the survey and analyses have to be rerun as presented in this paper. Third, in the field of data privacy, statements of customers in empirical surveys do not necessarily match their actions in the real world. The so-called privacy paradox describes the discrepancy between customers' intentions to protect their own privacy and their real-world behavior (Acquisti & Grossklags, 2005; Norberg, Horne, & Horne, 2007). The survey answers may be further biased as all data privacy measures were introduced with a description of the concern they address. This concern may not always be present to customers in real life. To take into account this limitation, the results of the survey should be verified in real-world situations not specifically referring to privacy concerns. Fourth, in general, the classification of delighters is less clear than the classification of basic needs. That is, when interpreting this paper's results, implications should be challenged according to the principle of prudence. Future research could follow Matzler et al. (1996) who state that unclear results spread out over several categories can be a starting point for market segmentation.

Managerial Implications

This paper provides advice to practitioners working in the field of data privacy and thinking about the implementation of certain data privacy measures and an overarching data privacy strategy. Our paper provides practitioners with an overview of possible data privacy measures specifically addressing customers' concerns regarding data privacy. Practitioners also get first insights into the measures' contribution to customer satisfaction and potential for a competitive advantage. Based on the measures' categorization, companies may implement

different pricing strategies which take into account the level of data privacy related to a certain product. For instance, companies may offer a basic product which merely comprises the implementation of basic and performance needs and a more expensive luxury product which additionally entails the implementation of all privacy measures that are categorized as delighters.

Overall, our research indicates that companies can delight the vast majority of customers with appropriate data privacy measures. Though companies might not want to implement every measure that delights customers, they can lever our research in the trade-off between customer excitement, economic value, regulatory requirements, and technical feasibility when deciding between the implementation of individual measures. To establish a generic and systematic "privacy by design" process which goes beyond mere technical solutions (Danezis et al., 2015), companies could follow the procedure of our research. A rational first step could be the derivation of a data privacy strategy that aligns with the overarching company strategy. Companies could gather their existing and potential future customers' concerns with regard to data privacy leveraging the work of Smith et al. (1996). Furthermore, companies could use our set of data privacy measures as a starting point and elaborate measures that specifically address the concerns of their customers. As demonstrated in this paper, companies could get insights into the relationship between individual data privacy measures and customer satisfaction by asking for their customers' evaluation. Considering their data privacy strategy and their customers' evaluation, companies could implement respective measures and measure their performance. Results from the performance measurement could serve as an input for adjustments of the company's data privacy strategy. To decide on the implementation of a data privacy strategy and particular measures, companies should nevertheless employ an interdisciplinary team which works on data privacy related topics and particularly includes a customer perspective besides a legal one.

Conclusion and Further Research

Answering the first research question, this paper provides an overview of data privacy measures collected from scientific and practitioner-oriented literature, legislative texts, and corporate privacy statements and evaluated by expert interviews. In addition, this paper provides first insights into customers' perceptions of the identified data privacy measures. By using the Kano model to design two online surveys, each with more than 200 participants, we could show that the majority of data privacy measures must be considered as necessary evils for companies. Nevertheless, both surveys highlighted the upside of data privacy, as almost all potential customers could be delighted with at least one measure. Thus, this paper positively answers the research question whether some measures are perceived as attractive and can delight customers. Their implementation might even lead to a

competitive advantage for companies. Accordingly, researchers and practitioners may use our approach as an inspiration when deriving a data privacy strategy. The list of measures may be useful. Evaluating customers' perception may assist in prioritizing the implementation of data privacy measures.

As every research endeavor, our paper leaves room for future research. Firstly, future research could focus on the evaluation of the general validity of our research in other industries than aviation and retail and with other customer groups. Secondly, researchers could segment customers by age, career, education, and other criteria in order to isolate groups that can be especially delighted with data privacy and derive strategies for those customers who do not. Thirdly, a decomposition of single data privacy measures in its individual components could shed light on the influence of individual aspects of a data privacy measure on customers' satisfaction. Fourth, researchers could further investigate the reasons why an individual data privacy measure is classified as one of the factors of the Kano model to better understand customers' sentiment towards data privacy in general.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. In *ICIS 2006 Proceedings* (Paper 94).

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy*, *3*(1), 26–33.

Ahmad, A., & Mykytyn, P. (2012). Perceived Privacy Breach - the Construct, the Scale, and its Antecedents. In *AMCIS 2012 Proceedings* (Paper 21).

Amazon. (2017). Amazon.de-Datenschutzerklärung. Retrieved from https://www.amazon.de/gp/help/customer/display.html?nodeId=3312401. Accessed on 2017-10-23.

Apple. (2017). Apple Datenschutzrichtlinie. Retrieved from https://www.apple.com/legal/privacy/de-ww/. Accessed on 2017-10-23.

Arbore, A., & Busacca, B. (2009). Customer satisfaction and dissatisfaction in retail banking: Exploring the asymmetric impact of attribute performances. *Journal of Retailing and Consumer Services*, *16*(4), 271–280.

Audatis Consulting. (2016). Checkliste: Technische und organisatorische Maßnahmen. Retrieved from https://www.audatis.de/wp-content/uploads/Checkliste_Datenschutz_TOM_nach_9_BDSG.pdf. Accessed on 18.08.2016.

Bartikowski, B., & Llosa, S. (2004). Customer Satisfaction Measurement: Comparing Four Methods of Attribute Categorisations. *The Service Industries Journal*, *24*(4), 67–82.

BBC. (2015). Ashley Madison infidelity site's customer data 'leaked'. Retrieved from http://www.bbc.com/news/business-33984017. Accessed on 2017-05-10.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1041.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. *Communications of the ACM*, *48*(4), 101–106.

Berger, C., Blauth, R., Boger, D., Bolster, C., Burchill, G., DuMouchel, W.,. . . Walden, D. (1993). Kano's Methods for Understanding Customer-defined Quality. *Center for Quallity Management Journal*, *2*(4), 3–36.

Buchmann, E., Böhm, K., & Raabe, O. (2008). Privacy 2.0: Towards Collaborative Data-Privacy Protection. In Y. Karabulut, J. Mitchell, P. Herrmann, & C. D. Jensen (Eds.), *Proceedings of IFIPTM 2008* (pp. 247–262).

Buhl, H. U. (2013). IT as Curse and Blessing. *Business & Information Systems Engineering*, *5*(6), 377–381.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, *9*(1), 69–104.

Clayton, E., & Hilz, A. (2015). 2015 Aviation Trends. Retrieved from http://www.strategyand.pwc.com/perspectives/2015-aviation-trends. Accessed on 2016-08-18.

Clement, A., & Obar, J. A. (2016). Keeping Internet Users in the Know or in the Dark: An Analysis of the Data Privacy Transparency of Canadian Internet Carriers. *Journal of Information Policy*, *6*, 294–331.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Métayer, D. Le, Tirtea, R., & Schiffner, S. (2015). *Privacy and Data Protection by Design - from policy to engineering*. Athens. Retrieved from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design. Accessed on 25.04.2017.

Deutsche Bank. (2017). Datenschutz. Retrieved from https://www.deutsche-bank.de/pfb/content/pk-datenschutz.html. Accessed on 2017-10-23.

Dhasarathan, C., Thirumal, V., & Ponnurangam, D. (2015). Data privacy breach prevention framework for the cloud service. *Security and Communication Networks*, *8*(6), 982–1005.

Dropbox. (2017). Dropbox-Datenschutzrichtlinie. Retrieved from https://www.dropbox.com/privacy. Accessed on 2017-10-23.

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*, *58*, 214–220.

easyJet. (2017). Datenschutzerklärung. Retrieved from https://www.easyjet.com/de/politik/datenschutzerklarung. Accessed on 2017-10-23.

Facebook. (2017). Datenrichtlinie. Retrieved from https://de-de.facebook.com/about/privacy. Accessed on 2017-10-23.

Fong, D. (1996). Using the Self-Stated Importance Questionnaire to Interpret Kano Questionnaire Results. *Center for Quallity Management Journal*, *5*(3), 21–23.

Füller, J., & Matzler, K. (2008). Customer delight and market segmentation: An application of the three-factor theory of customer satisfaction on life style groups. *Tourism Management*, *29*(1), 116–126.

Gronholdt, L., Martensen, A., & Kristensen, K. (2000). The relationship between customer satisfaction and loyalty: Cross-industry differences. *Total Quality Management*, *11*(4-6), 509–514.

Hackl, P., & Westlund, A. H. (2000). On structural equation modelling for customer satisfaction measurement. *Total Quality Management*, *11*(4-6), 820–825.

Harris, E. C. (2007). Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answer. *American University International Law Review*, *22*(5), 745–799.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*(1), 275–298.

Hovav, A., & D'Arcy, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, *6*(2), 97–121.

Inman, J. J., & Nikolova, H. (2017). Shopper-Facing Retail Technology: A Retailer Adoption Decision Framework Incorporating Shopper Attitudes and Privacy Concerns. *Journal of Retailing*, *93*(1), 7–28.

Kano, N., Seraku, N., Takahashi, F., & Tsuji, S. i. (1984). Attractive quality and must-be quality. *The Journal of the Japanese Society for Quality Control*, *14*(2), 147–156.

Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. B. (2016). Limited Information and Quick Decisions: Consumer Privacy Calculus for Mobile Applications. *AIS Transactions on Human-Computer Interaction*, *8*(3), 88–130.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173.

Khatri, V., & Brown, C. V. (2010). Designing Data Governance. *Communications of the ACM*, *53*(1), 148.

Klingspor, V. (2016). Why Do We Need Data Privacy? In S. Michaelis, N. Piatkowski, & M. Stolpe (Eds.), *Solving Large Scale Learning Tasks: Challenges and Algorithms* (pp. 85–95). Cham: Springer.

Ladhari, R. (2009). A review of twenty years of SERVQUAL research. *International Journal of Quality and Service Sciences*, *1*(2), 172–198.

Lai, H.-J., & Wu, H.-H. (2011). A Case Study of Applying Kano's Model and ANOVA Technique in Evaluating Service Quality. *Information Technology Journal*, *10*(1), 89–97.

Landis, R. J., & Koch, G. G. (1977). The Measurement of Observer Agreement for Categorical Data. *Biometrics*, *33*, 159–174.

Lee, M. C., & Newcomb, J. (1996). Applying the Kano Methodology in Managing NASA's Science Research Program. *Center for Quallity Management Journal*, *5*(3), 13–20.

Löfgren, M., & Witell, L. (2008). Two Decades of Using Kano's Theory of Attractive Quality: A Literature Review. *The Quality Management Journal*, *15*(1), 59–75.

Lyons, V., van der Werff, L., & Lynn, T. (2016). Ethics as Pacemaker: Regulating the Heart of the Privacy-Trust Relationship. A proposed conceptual model. In *ICIS 2016 Proceedings.*

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355.

Mamonov, S., & Koufaris, M. (2014). The Impact of Perceived Privacy Breach on Smartphone User Attitudes and Intention to Terminate the Relationship with the Mobile Carrier. *Communications of the Association for Information Systems*, *34*(60).

Matthing, J., Sandén, B., & Edvardsson, B. (2004). New service development: learning from and with customers. *International Journal of Service Industry Management*, *15*(5), 479–498.

Matzler, K., Hinterhuber, H. H., Bailom, F., & Sauerwein, E. (1996). How to delight your customers. *Journal of Product & Brand Management*, *5*(2), 6–18.

Matzler, K., & Stahl, H. K. (2000). Kundenzufriedenheit und Unternehmenswertsteigerung. *Die Betriebswirtschaft*, *60*, 626–641.

Mohammed, R. (2014). Why Amazon Should Unbundle Prime. Retrieved from https://hbr.org/2014/02/why-amazon-should-unbundle-prime. Accessed on 2017-10-12.

Morey, T., Forbath, T., & Schoop, A. (2015). Customer Data: Designing for Transparency and Trust. *Harvard Business Review*. (May), 96–105.

Moshki, H., & Barki, H. (2016). Coping with Information Privacy Breaches: An Exploratory Framework. In *ICIS 2016 Proceedings.*

Muntermann, J., & Roßnagel, H. (2009). On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market. In A. Jøsang, T. Maseng, & S. J. Knapskog (Eds.), *Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age* (pp. 1–14).

Nicholas-Donald, A., Matus, J. F., Ryu, S., & Mahmood, A. M. (2011). The Economic Effect of Privacy Breach Announcements on Stocks: A Comprehensive Empirical Investigation. In *AMCIS 2011 Proceedings* (Paper 341).

Nofer, M., Hinz, O., Muntermann, J., & Roßnagel, H. (2014). The Economic Impact of Privacy Violations and Security Breaches. *Business & Information Systems Engineering*, *6*(6), 339–348.

Nofer, M., Hinz, O., Muntermann, J., & Rossnagel, H. (2014). The Economic Impact of Privacy Violations and Security Breaches. *Business & Information Systems Engineering*, *6*(6), 339–348.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126.

Otto, B. (2011). Organizing Data Governance: Findings from the Telecommunications Industry and Consequences for Large Service Providers. *Communications of the Association for Information Systems*, *29*(3), 45–66.

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1985). A Conceptual Model of Service Quality and Its Implications for Future Research. *Journal of Marketing*, *49*(4), 41–50.

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly*, *35*(4), 977–988.

Payne, D., Landry, B. J. L., & Dean, M. D. (2015). Data Mining and Privacy: An Initial Attempt at a Comprehensive Code of Conduct for Online Business. *Communications of the ACM*, *37*, Article 34.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, *71*(12), 1133–1143.

Preibusch, S., Kübler, D., & Beresford, A. R. (2013). Price versus privacy: an experiment into the competitive advantage of collecting less personal information. *Electronic Commerce Research*, *13*(4), 423–455.

Saarijärvi, H., Grönroos, C., & Kuusela, H. (2014). Reverse use of customer data: implications for service-based business models. *Journal of Services Marketing*, *28*(7), 529–537.

Sarathy, R., & Robertson, C. J. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. *Journal of Business Ethics*, *46*(2), 111–126.

Schaule, M. (2014). Anreize für eine nachhaltige Immobilienentwicklung: Nutzerzufriedenheit und Zahlungsbereitschaft als Funktion von Gebäudeeigenschaften bei Büroimmobilien (Doctoral thesis). Fakultät für Bauingenieur- und Vermessungswesen, Munich.

Schneider, M. J., Jagpal, S., Gupta, S., Li, S., & Yu, Y. (2017). Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing*, *34*(3), 593–603.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167–196.

Tanner, A. (2013). Here Are Some of America's Most Privacy Friendly Companies: http://www.forbes.com/sites/adamtanner/2013/09/11/here-are-some-of-americas-most-privacy-friendly-companies/. Accessed on 2016-11-02. Retrieved from http://www.forbes.com/sites/adamtanner/2013/09/11/here-are-some-of-americas-most-privacy-friendly-companies/. Accessed on 2016-11-02.

Telekom DE-Mail. (2017). Datenschutzhinweise für De-Mail der Telekom Deutschland GmbH. Retrieved from http://www.telekom.de/dlp/agb/pdf/42734.pdf. Accessed on 2017-10-23.

Tesla Motors. (2017). Datenschutzerklärung. Retrieved from https://www.tesla.com/sites/default/files/pdfs/de_DE/tmi_privacy_statement_external_6-14-2013_v2.pdf. Accessed on 2017-10-23.

The Guardian. (2011). iPhone keeps record of everywhere you go. Retrieved from https://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears. Accessed on 2017-05-10.

The Telegraph. (2010). Facebook admits 'inadvertent' privacy breach. Retrieved from http://www.telegraph.co.uk/technology/facebook/8070513/Facebook-admits-inadvertent-privacy-breach.html. Accessed on 2017-05-07.

Zalando. (2017). Datenschutzerklärung und Einwilligung zur Datennutzung. Retrieved from https://www.zalando.de/zalando-datenschutz/. Accessed on 2017-10-23.