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. According to Kano et al. [29], each possible combination of answers can be interpreted in an individual manner and leads to a certain pre-defined classification [28], as shown in Figure 2. As proposed by Matzler et al. [28], we derive the final classification of a measure from the respective most frequent individual result.

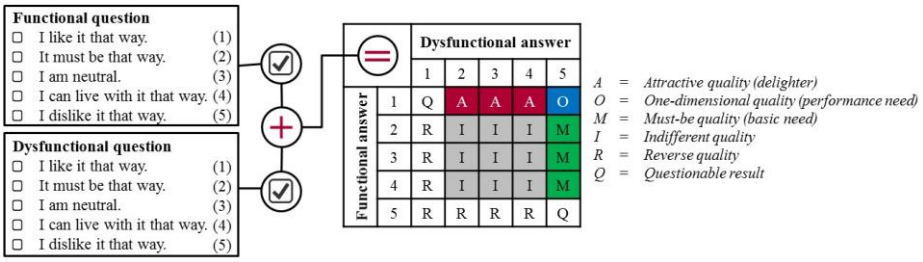

Figure 2. Derivation of Kano model factors based on Matzler et al. [28]

3.3 Survey

Scenario. In order to determine the customers' evaluation of the identified data privacy measures, we conduct an Internet-based survey. To enable the participants to assume a perspective as natural as possible and to illustrate the situation, we need to use a specific, well-known, and simple scenario that relates to an exemplary industry sector, for which data privacy is a considerable issue. That is, the sector 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 industry actors. Furthermore, companies should provide loyalty programs because they are typically based on gathering data on a customer's behavior over a long period.

The aviation sector as a commonly known industry with a considerable amount of customer data collected at different interaction points [31], transmission of data to public authorities, airport operators, or other airlines that are partners in global alliances [32], and loyalty programs, fulfills all of these requirements.

Design. 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 data privacy concerns preceded by short explanations of the respective concerns. The following example of an explanation, a functional, and a dysfunctional

question demonstrates the survey's design. *Explanation:* "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." *Functional question:* "You are informed if your customer data are passed on to external third parties." *Dysfunctional question:* "You are not informed if your customer data are passed on to external third parties." To answer the functional and the dysfunctional question, the participants can choose one of the five previously mentioned possible answers. In this way, we ask the participants about each of the 32 identified measures, resulting in a total of 32 question pairs, each of them addressing one of the data privacy concerns.

Participants. The main survey has 227 German-speaking participants, 219 of whom correctly answered a control question. Invitations were distributed via social media and email, and participation was 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.

4 Results

In the following section, we present the overview of possible data privacy measures for companies in section 4.1 that resulted from the research process previously described. This overview forms the basis of the presentation of the survey results in section 4.2, that is, the perceptions that customers have of the identified privacy measures.

4.1 Data Privacy Concerns and Measures

The overview of possible data privacy measures is compiled from the literature, legislative texts, and expert interviews. Two publications contain various starting points for measures that can be taken to ease customers' concerns: Morey et al. [33], who describe the role of transparency regarding data collection and usage, and Payne et al. [34], 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 [35] were used to complement the statements from a practitioner-oriented perspective. Furthermore, we use legislative texts: the European General Data Protection Regulation, which will become applicable law for countries in the European Union in May 2018, the German Bundesdatenschutzgesetz, and the German Telemediengesetz, both finding predominant application with respect to data privacy. To check the completeness of and to verify the previously found statements, we performed three expert interviews in the way described in section 3.1. 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 potential and existing 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. To complement our research with input from a legal perspective, we interviewed a lawyer.

From all sources, we collected 141 statements merged to 32 groups. From these groups we derived a particular data privacy measure. All 32 measures can be mapped to one of seven privacy concerns following Smith et al. [15], and as listed in Table **2**.

Table 2. Data privacy concerns presented by Smith et al. [15]

Concern	*Description*
Data Collection	Concern that companies store large amounts of personal customer data.
Data Combination	Concern that customer data from different databases may be combined to gain additional information about a customer.
Internal Secondary Usage	Concern that companies use customer data for a secondary unauthorized purpose.
External Secondary Usage	Concern that customer data are disclosed to a third party and used for a secondary unauthorized purpose.
Errors	Concern that customer data may contain deliberate or accidental errors.
Improper Access	Concern that unauthorized persons are able to view and edit customer data.
Reduced Judgment	Concern that decisions are made in an automated manner and that human intervention in decision-making processes is not possible.

The measures are presented in Tables 3 to 9, grouped by the seven concerns. First, Table 3 represents measures that address customers' privacy concern of Data Collection, meaning that companies might store large amounts of personal customer data.

Table 3. Measures addressing customers' privacy concern of Data Collection

#	*Measure description*
A1	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.
A2	Customer data are, as best as is possible, stored anonymously to prevent backtracking of individual customers.
A3	Only the customer data absolutely necessary to provide the agreed service are collected.
A4	Altering or exiting the contractual agreement with regard to personal data is as easy as entering into it. Among others, processing requests occurs quickly and is free of charge.
A5	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 to other companies.

Table 4 comprises measures that address customers' privacy concern of Data Combination. That is, customer data out of different databases might be combined to gain additional information about a customer.

Table 4. Measures addressing customers' privacy concern of Data Combination

#	*Measure description*
B1	The customer is informed if the company combines his data from various internal and external sources.
B2	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.
B3	If customer data are collected for different purposes, the data sets are stored in different databases and are not combined.
B4	The customer decides on whether the company is allowed to combine data from various internal and external sources and can change his decision at any time.

Customers might be concerned that companies use customer data for a secondary unauthorized purpose within the company. Measures addressing the concern of Internal Secondary Usage are listed in Table 5.

Table 5. Measures addressing customers' privacy concern of Internal Secondary Usage

#	*Measure description*
C1	The customer is informed whether and what data are passed on within the company or group of companies and for what purpose.
C2	Customer data are deleted as soon as the original reason for the collection no longer applies or the customer withdraws his permission.
C3	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.
C4	If customer data are collected for different purposes, the data sets are stored in different databases and are not combined.
C5	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.

Measures addressing customers' privacy concern of External Secondary Usage are presented in Table 6. Customer data might be disclosed to a third party and used for a secondary unauthorized purpose.

Table 6. Measures addressing customers' privacy concern of External Secondary Usage

#	*Measure description*
D1	If customer data are passed on to external third parties, the customer is informed. 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.

Table 7 cont'd. Measures addressing customers' privacy concern of External Secondary Usage

#	*Measure description*
D3	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.
D4	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).
D5	If customer data are passed on to external third parties, the data are – as best as possible – forwarded anonymously.
D6	The company does not pass on customer data to external third parties.
D7	The customer has the choice to easily deny sharing his data with external parties even if doing so results in compromising or the complete abortion of the value delivery.

Customer data might contain deliberate or accidental errors. Measures addressing the concern of Errors are listed in Table 8.

Table 8. Measures addressing customers' privacy concern of Errors

#	*Measure description*
E1	Customer data are checked regularly by the company for completeness, accuracy, and being up-to-date.
E2	The company ensures that no customer data are destroyed or lost by technical and organizational means.
E3	Employees with access to customer data are selected carefully, their behavior is checked regularly, and they are held responsible for malpractice.
E4	Entering, viewing, altering, and deleting customer data are recorded to enable retracing at any time who changed the data when, and in what manner. The customer can either view the log file directly or is informed about any alterations to his personal data.
E5	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.

Table 8 contains measures addressing the concern of Improper Access, which means that unauthorized people might be able to view and edit customer data.

Table 9. Measures addressing customers' privacy concern of Improper Access

#	*Measure description*
F1	If the protection of customer data was violated and their security is at risk, the company immediately informs the customer and the authorities.
F2	Storage and transmission of customer data are protected by technical (e.g., password protection, encryption) and organizational means (e.g., access control, companywide standards regarding handling customer data).
F3	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.

Customers might be concerned that decisions are taken in an automated manner and that people cannot intervene in decision-making processes, if necessary. This concern, Reduced Judgment, can be addressed by the measures listed in Table 10.

Table 10. Measures addressing customers' privacy concern of Reduced Judgment

#	*Measure description*
G1	The customer is informed whether a decision was made through an automated systems or through an employee of the company. At the customer's request, the reasons for the decision are communicated and explained.
G2	Automated decision processes are continuously tested and checked for deviations.
G3	Decisions that entail legal consequences (e.g., granting a credit) are never made only on the basis of automated systems.

In summary, Tables 3 to 9 represent a comprehensive list of actions that can be taken by companies to mitigate the risk of displeasing customers and to create the potential for delighting customers regarding data privacy.

4.2 Customers' Evaluation of Data Privacy Measures

Companies need to be aware of customers' evaluation of these data privacy measures, which forms the basis for deriving implications for companies' data privacy policies. To determine whether customers consider the implementation of the different identified data privacy measures as "must-be" (basic need), "one-dimensional" (performance need), "attractive" (delighters), or "indifferent," we analyzed the survey's results using the Kano model as described in the previous section. These results are illustrated in Figure 3. Thereby, the measures are numbered as defined in Tables 3 to 9. The abscissa denotes the majority-share of survey participants that determined the measure's classification as one of the four Kano model factors. The ordinate states the spread between the majority-share and the second highest share to evaluate the result's clarity. In the illustration, a green square represents a measure considered to be a basic need by the majority of the participants. Analogously, red dots symbolize measures that are considered to be delighters and gray triangles mark the respective measures as being of indifferent quality. There are no measures considered to be performance needs. To illustrate this approach, we use measure D5 as an example. According to their choice of answers, the majority of the participants (57%, abscissa) see it as a basic need, whereas the second largest group (23%) consider it as a performance need. Thus, the ordinate is 34% (57%–23%), representing a relatively clear result. Overall, the unity among survey participants regarding the classification of a data privacy measure is the smallest bottom left and increases along the bisector. Thus, the distinctiveness of a categorization is highest toward the top right. Valid implications can be derived from the results starting from a spread of at least 10% on the ordinate in Figure **3**.

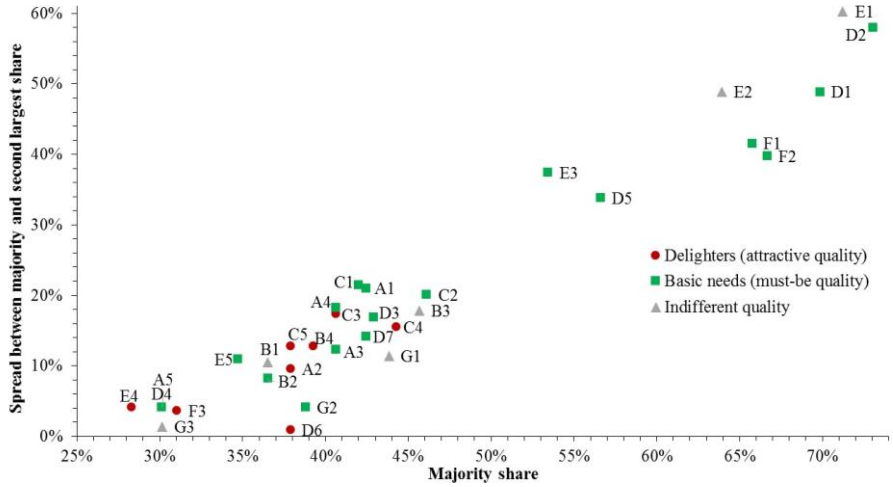

Figure 3. Visualization of the empirical results

Survey participants see 18 out of 32 measures as basic needs. That is, the realization of these measures is neither rewarded nor explicitly demanded by customers. Instead, it is a basic prerequisite when engaging in business with the company. In particular, basic needs can be found among measures addressing the concerns Collection (4 measures out of 5 categorized as a basic need), External Secondary Usage (6/7), and Improper Access (2/3). Hence, these basic needs can be considered a necessary evil because they have downside risk if not implemented but offer no upside opportunities if implemented. The most distinctive example is measure D2, stating that external secondary usage is to be regulated by contracts or other provisions to ensure that data are only used in the manner agreed on with the customer.

Furthermore, no measures are considered to be performance needs. Their constituting properties are, in addition to having a negative impact if not implemented, that they also have the ability to increase customer satisfaction when implemented properly. The total lack of such factors with upside potential is another emphasis of the necessary-evil quality of most data privacy measures.

Entirely, six measures are considered by the survey's participants to be of indifferent quality and, in particular, can be found when addressing the concerns Combining Data (2 measures out of 4 categorized as indifferent) and Reduced Judgment (2/3). These measures do not allow distinctive interpretations toward any direction.

However, there are eight measures categorized as delighters, which are measures that are not required by the customer but may please them, and have no negative impact if not implemented. These measures go beyond the data privacy measures that customers expect. Their implementation positions a company at a level of data privacy commitment higher than anticipated, which has the potential to be rewarded with higher customer satisfaction. Thus, delighters enable companies to differentiate themselves from competitors and to gain a competitive advantage. For instance, Internal Secondary Usage is the concern with the highest share of measures classified as delighters (3/5). In particular, customers can be delighted by providing them with the ability to retrace

who changed the data, how, and when (measure C3), or by storing customer data in different and not combined databases, if the data are collected for different purposes (measure C4).

In summary, most of the identified data privacy measures are classified as basic needs. However, survey participants' answers lead to the classification of some data privacy measures as delighters. Thus, our results show that the implementation of data privacy measures has the potential to delight customers.

5 Summary, Limitations, and Future Research

This paper provides an overview of data privacy measures collected from scientific and practitioner-oriented literature, legislative texts, and expert interviews, and can be useful for researchers and practitioners. On top of this overview, this paper provides first insights into customers' perceptions of the identified data privacy measures. By using the Kano model to design a survey with more than 200 participants, we could show that the majority of data privacy measures must be considered as necessary evils for companies. Nevertheless, some data privacy measures can even delight customers. Thus, this paper's result is that certain data privacy measures have the potential to increase customer satisfaction and enable a competitive advantage for companies. Accordingly, researchers and practitioners may use our approach as inspiration when deriving a data privacy strategy because evaluating customers' perception may assist in prioritizing the implementation of data privacy measures. Measures classified as basic needs should be implemented by every company to avoid data privacy incidents and negative effects on customer satisfaction. Companies that strive for delighting customers through data privacy may also implement measures classified as delighters.

However, researchers and practitioners need to be aware of our research having some limitations. First, the research approach is limited to the consideration of a specific aviation sector scenario. To verify the general validity of the conclusions, the survey has to be rerun for further settings that refer to other industries. Second, in the field of data privacy, statements of customers in empirical surveys do not necessarily match their actions in the real world. According to Norberg et al. [36] and Acquisti and Grossklags [37], the so-called privacy paradox describes the discrepancy between customers' intentions to protect their own privacy and their real-world behavior. To take into account this phenomenon, the results of the survey should be verified in real-world situations. Third, in general, the classification of delighters is less clear than the classification of basic needs. That is, when interpreting this paper's results, implications must be challenged according to the principle of prudence. When in doubt, a measure should rather be considered a basic need than being of indifferent quality or a delighter. Future research could follow Matzler et al. [18], who state that unclear results spread out over several categories can be a starting point for market segmentation. Thus, further research could examine the categorization of data privacy measures as Kano model factors depending on demographic characteristics.

When providing an overview of data privacy measures and outlining the potential to increase customer satisfaction by applying certain data privacy measures, we could also

point out main areas of further research relevant to both researchers and practitioners. Specifically, we plan to extend our research to other industries to evaluate general validity in the near future. Further research can also focus on a break-down of single data privacy measures into its individual components and the influence of these granular aspects on customers' satisfaction with a particular data privacy measure.

References

1. Matthing, J., Sandén, B., Edvardsson, B.: New service development: learning from and with customers. International Journal of Service Industry Management. 15, 479–498 (2004)
2. Saarijärvi, H., Grönroos, C., Kuusela, H.: Reverse use of customer data: implications for service-based business models. Journal of Service Marketing. 28, 529–537 (2014)
3. Berendt, B., Günther, O., Spiekermann, S.: Privacy in e-commerce: stated preferences vs. actual behavior. Communications of the ACM. 48, 101–106 (2005)
4. Preibusch, S., Kübler, D., Beresford, A.R.: Price versus privacy: an experiment into the competitive advantage of collecting less personal information. Electronic Commerce Research. 13, 423–455 (2013)
5. Acquisti, A., Friedman, A., Telang, R.: Is There a Cost to Privacy Breaches? An Event Study. In: ICIS 2006 Proceedings, pp. 1563–1580 (2006)
6. Muntermann, J., Roßnagel, H.: On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market. In: Jøsang, A., Maseng, T., Knapskog, S.J. (eds.) NordSec 2009. LNCS, vol. 5838. pp. 1–14. Springer, Heidelberg (2009)
7. Tanner, A.: 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/#1684385b306a (Accessed: 02.11.2016)
8. Buhl, H.U.: IT as curse and blessing. Business & Information Systems Engineering. 5, 377–381 (2013)
9. Ahmad, A., Mykytyn, P.: Perceived Privacy Breach – the Construct, the Scale, and its Antecedents. In: AMCIS 2012 Proceedings. pp. 1–9. (2012)
10. Pavlou, P.A.: State of the information privacy literature: where are we now and where should we go? MIS Quarterly. 35, 977–988 (2011)
11. Nicholas-Donald, A., Matus, J.F., Ryu, S., Mahmood, A.M.: The Economic Effect of Privacy Breach Announcements on Stocks: A Comprehensive Empirical Investigation. In: AMCIS 2011 Proceedings. pp. 1–15. (2011)
12. Cavusoglu, H., Mishra, B., Raghunathan, S.: 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, 69–104 (2004)
13. Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L.: The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security. 11, 431–448 (2003)
14. Hovay, A., D'Arcy, J.: The impact of denial-of-service attack announcements on the market value of firms. Risk Management and Insurance Review. 6, 97–121 (2003)
15. Smith, H.J., Milberg, S.J., Burke, S.J.: Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly. 20, 167–196 (1996)
16. Klingspor, V.: Why Do We Need Data Privacy? In: Michaelis, S., Piatkowski, N., Stolpe, M. (eds.) Solving Large Scale Learning Tasks. Challenges and Algorithms. LNCS, vol. 9580. pp. 85–95. Springer (2016)

17. Buchmann, E., Böhm, K., Raabe, O.: Privacy 2.0: Towards Collaborative Data-Privacy Protection. In: IFIP International Conference on Trust Management, pp. 247–262. Springer US (2008)
18. Sarathy, R., Robertson, C.J.: Strategic and ethical considerations in managing digital privacy. Journal of Business Ethics. 46, 111–126 (2003)
19. Nufer, G., Prell, K.: Operationalisierung von Kundenzufriedenheit. Reutlinger Diskussionsbeiträge zu Marketing & Management. 4, 1–18 (2011)
20. Parasuraman, A., Zeithaml, V.A., Berry L.L.: A Conceptual Model of Service Quality and Its Implications for Future Research. Journal of Marketing. 49, 41–50 (1985)
21. Ladhari, R.: A review of twenty years of SERVQUAL research. International Journal of Quality and Service Sciences. 1, 172–198 (2009)
22. Hackl, P., Westlund, A.H.: On structural equation modelling for customer satisfaction measurement. Total Quality Management. 11, 820–825 (2000)
23. Bartikowski, B., Llosa, S.: Customer satisfaction measurement: comparing four methods of attribute categorisations. The Service Industries Journal. 24, 67–82 (2004)
24. Füller, J., Matzler, K.: Customer delight and market segmentation: An application of the three-factor theory of customer satisfaction on life style groups. Tourism Management. 29, 116–126 (2008)
25. Löfgren, M., Witell, L.: Two Decades of Using Kano's Theory of Attractive Quality: A Literature Review. The Quality Management Journal. 15, 59–76 (2008)
26. Lai, H.J., Wu, H.H.: A Case Study of Applying Kano's Model and ANOVA Technique in Evaluating Service Quality. Information Technology Journal. 10, 89–97 (2011)
27. Arbore, A., Busacca, B.: Customer satisfaction and dissatisfaction in retail banking: Exploring the asymmetric impact of attribute performances. Journal of Retailing and Consumer Services. 16, 271–280 (2009)
28. Matzler, K., Hinterhuber, H.H., Bailom, F., Sauerwein, E.: How to delight your customers. Journal of Product & Brand Management. 5, 6–18 (1996)
29. Kano, N., Seraku, N., Takahashi, F.: Attractive quality and must-be quality. The Journal of the Japanese Society for Quality Control. 14, 147–156 (1984)
30. Mikulić, J., Prebežac, D.: A critical review of techniques for classifying quality attributes in the Kano model. Managing Service Quality: An International Journal. 21, 46–66 (2011)
31. Strategy&, http://www.strategyand.pwc.com/perspectives/2015-aviation-trends (Accessed: 18.08.2016)
32. Harris, E.C.: 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 answers. American University International Law Review. 22, 745–799 (2007)
33. Morey, T., Forbath, T., Schoop, A.: Customer data: designing for transparency and trust. Harvard Business Review. 93, 96–105 (2015)
34. Payne, D., Landry, B.J.L., Dean, M.D.: Data Mining and Privacy: An initial attempt at a comprehensive code of conduct for online business. Communications of the Association for Information Systems. 37, 717–732 (2015)
35. Audatis Consulting, https://www.audatis.de/wp-content/uploads/Checkliste_Datenschutz_TOM_nach_9_BDSG.pdf (Accessed: 18.08.2016)
36. Norberg, P.A., Horne, D.R., Horne, D.A.: The privacy paradox: personal information disclosure intentions versus behaviors. Journal of Consumer Affairs. 41, 100–126 (2007)
37. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Security & Privacy. 2, 24–30 (2005)