5-15-2019

THE ROLE OF TRANSPARENCY IN PRIVACY DECISION-MAKING UNDER UNCERTAINTY

Victoria Fast
University of Passau, victoria.fast@uni-passau.de

THE ROLE OF TRANSPARENCY IN PRIVACY DECISION-MAKING UNDER UNCERTAINTY

Research in Progress

Fast, Victoria, University of Passau, Passau, Germany, victoria.fast@uni-passau.de[1]

Abstract

Recent data breaches at online content and service providers (CSPs) such as Facebook or Uber illustrate the privacy risks associated with the disclosure of personal data. Yet, asymmetric information between users and CSPs makes it difficult for users to assess their privacy risks. Thus, in order to reduce uncertainty and assist users with increasingly complex privacy trade-offs, regulators and consumer protection agencies advise CSPs to be more transparent about their data collection, storage and use. In this context, Information Systems research has largely focused on the effectiveness of transparency measures in specific application scenarios (e.g. recommender systems, targeted advertising) by exogenously assigning subjects to scenarios with or without transparency. However, it is unclear whether users would actively choose a more transparent over a less transparent CSP, as they may prefer ambiguity regarding privacy risks and information avoidance. To advance research in this area, this paper presents an experimental design to study subjects' preferences for transparency in a controlled laboratory environment. Drawing on the field of decision analysis and established theories on uncertainty and ambiguity attitudes, the present study contributes to a better understanding of human privacy decision-making.

Keywords: Transparency, Privacy risk, Ambiguity, Laboratory experiment.

[1] This project was funded by the Bavarian State Ministry of Science and the Arts in the framework of the Centre Digitisation.Bavaria.

1 Introduction

Most online content and service providers (CSPs) such as search engines, social networks or news sites grant users access free of charge. Instead of a monetary price, these CSPs rely on the collection of user data which they monetise, e.g. by placing targeted advertisements (e.g. Goldfarb, 2014). This collection of massive amounts of data and advances in data-processing technologies do not only yield benefits for users, but may also make them vulnerable because of a CSP's opportunistic behaviour or security issues (Martin, Borah, and Palmatier, 2017).

This vulnerability is particularly illustrated by recent high-profile data breaches: in September 2018, security flaws in Facebook's code led to personal data of nearly 30 million users being accessed and potentially controlled by hackers, including search history and location data (Isaac, 2018). Furthermore, in 2016, personal data of about 57 million Uber users was inappropriately accessed, including names and license numbers of 600.000 drivers (Khosrowshahi, 2017). Such data breaches do not only lead to a loss of trust, but may also negatively impact firm reputation and stock prices (Acquisti, Friedman, and Telang, 2006; A. Malhotra and Kubowicz Malhotra, 2011; Martin, Borah, and Palmatier, 2017). The scope and severity of these cases indicate the importance of data protection as a precondition for privacy.

In general, privacy refers to "the extent to which a consumer is aware of and has the ability to control the collection, storage, and use of personal information by a firm" (Beke, Eggers, and Verhoef, 2018, p. 5). Users' assessment of the potential adverse consequences related to data disclosure, however, is often complicated by asymmetric information between users and CSPs regarding data collection, storage and use (Acquisti and Grossklags, 2008, 2012). This leaves users in a state of uncertainty[2] and leads to difficulties in privacy decision-making (Acquisti, Adjerid, et al., 2017). In order to assist users with the assessment of privacy risks and increasingly complex privacy trade-offs, regulators and consumer protection agencies advise CSPs to be more transparent about practices that impact their users' privacy. In particular, they should give users clear information about which data they collect, store and use (Awad and Krishnan, 2006). For example, the European General Data Protection Regulation (GDPR) emphasises that "[p]ersonal data shall be [...] processed lawfully, fairly and in a transparent manner in relation to the data subject" (Article 5(1a) GDPR). Transparency is also discussed in the privacy framework of the Organisation for Economic Co-operation and Development (OECD, 2013) and the Federal Trade Commission's fair information practices in the electronic marketplace (Federal Trade Commission, 2000).

In this context, research has so far focused on the effectiveness of transparency in specific application contexts by comparing user attitudes and behavioural intentions in scenarios with or without transparency. For example, studies show that transparency can increase trust and acceptance of personalised recommendations (e.g. Sinha and Swearingen, 2002) and the effectiveness of targeted advertising (e.g. T. Kim, Barasz, and John, 2019). However, the question whether users actually prefer transparency about privacy risks and whether they would actively choose a more transparent over a less transparent CSP, has received little attention. The traditional, normative perspective on privacy decision-making assumes that users engage in deliberate and effortful information processing and make privacy decisions by rationally weighing associated benefits and risks (Dinev, McConnell, and H. J. Smith, 2015). In this spirit, it is generally assumed that rational users prefer more information to less in order to improve decision making (Schweizer and Szech, 2018). Thus, according to the perspective of the economics of information (Stigler, 1961), users should seek information in situations where transparency potentially yields high benefits, i.e. better privacy decisions. But research also shows that there are situations in which humans tend to avoid information acquisition (e.g. Golman, Hagmann, and Loewenstein, 2017; Grossman and Van Der Weele, 2017). For example, experiments in the field of decision analysis show that subjects tend to avoid *risk* (i.e. the probabilities of the outcomes of an event are known) and seek *ambiguity* (i.e. the probabilities of the outcomes of an event are unknown) when facing situations with probable losses (e.g. Abdellaoui,

[2] In this paper, uncertainty encompasses *risk* (outcomes with known probabilities) and *ambiguity* (outcomes with unknown probabilities).

Vossmann, and Weber, 2005; Ho, Keller, and Keltyka, 2002).
Applied to the case of privacy, even though transparency provides users with information which facilitates privacy decision-making, users may nevertheless ignore the available information. They may focus on the benefits of using an online service and avoid thinking about potential adverse consequences and related negative emotions such as regret (Hertwig and Engel, 2016). This reasoning relates to the growing body of empirical research which focuses on the behavioural perspective of privacy decision-making and investigates aspects such as biases, heuristics or affect in order to explain deviations from economically rational models of decision making and the disparity between stated privacy concerns and actual behaviour (e.g. Adjerid, Acquisti, and Loewenstein, 2018; Brandimarte, Acquisti, and Loewenstein, 2013). Following this line of research, this study proposes a design for a laboratory experiment in order to explore the link between transparency and user behaviour. Specifically, the following research questions are examined: *How do users decide when choosing between online CSPs with different levels of transparency about potential data losses? How does the probability of a data loss influence users' preference for transparency?*
The aim of this research in progress is to highlight existing research gaps and present an experimental design to investigate users' preferences regarding transparency in the context of data loss. Thus, the present study follows calls by Dinev, McConnell, and H. J. Smith (2015), Goes (2013), and Lowry, Dinev, and Willison (2017) and contributes to a better understanding of human privacy behaviour by measuring actual behaviour instead of stated intentions and by exploring the intersection of behavioural economics and privacy decision-making. To answer the research questions, this study draws on the field of decision analysis and established theories on ambiguity attitudes, which have hitherto focused on money as the outcome variable. Therefore, this study additionally examines whether ambiguity attitudes with respect to data loss systematically differ from ambiguity attitudes with respect to money loss.
The remainder of this paper is structured as follows: in Chapter 2, research gaps for three different literature streams are identified and hypotheses are derived. In Chapter 3, a detailed description of the experimental setup and the implementation of the experiment is given. Chapter 4 concludes with an outlook on the calibration of the final experimental setup, including contributions, limitations and possible extensions.

2 Background

This study relates to research on (i) the role of uncertainty in the context of the privacy calculus, (ii) the effectiveness of transparency and (iii) decision making under uncertainty. In the following, an overview of these three literature streams is given and research gaps are highlighted.

2.1 Privacy calculus, risk and ambiguity

Users can benefit from the disclosure of personal data as it provides them with tangible (e.g. free access to (personalised) services, price discounts, recommendations) and intangible advantages (e.g. convenience, social interaction, entertainment) (Acquisti, Taylor, and Wagman, 2016; Marreiros et al., 2017). Disclosing personal data, however, also makes users vulnerable (Martin, Borah, and Palmatier, 2017) as it entails risks, especially when personal data is not stored and protected appropriately (Acquisti, Taylor, and Wagman, 2016). More specifically, data disclosure can result in unwanted consequences such as intrusive targeted advertising (e.g. Tucker, 2012), price discrimination (e.g. Acquisti and Varian, 2005), data sharing with third parties (e.g. Jentzsch, Sapi, and Suleymanova, 2013) or identity theft (e.g. P. A. Wang and Nyshadham, 2011). Users are said to rationally weigh these benefits and risks in a *privacy calculus* when deciding about data disclosure (Culnan and Armstrong, 1999; Culnan and Bies, 2003; Dinev and Hart, 2006; Laufer and Wolfe, 1977).
According to theory, *perceived privacy risk* is defined as "the expectation of losses associated with the disclosure of personal information" (H. Xu et al., 2011, p. 804) and is formed by a user's evaluation of the (i) severity and (ii) probability of adverse consequences related to data disclosure (Peter and Tarpey Sr.,

1975; H. Xu et al., 2011). In practice, users rarely know these two aspects precisely because of incomplete and asymmetric information (Akerlof, 1970), whereas CSPs typically know more about data collection, use and protection (Aleem, Cavusoglu, and Benbasat, 2017; N. K. Malhotra, S. S. Kim, and Agarwal, 2004; H. J. Smith, Milberg, and Burke, 1996). This makes it difficult for users to assess privacy risks (Acquisti and Grossklags, 2008). Thus, users rather find themselves in situations of *ambiguity* (i.e. the probabilities of the outcomes of an event are unknown) than *risk* (i.e. the probabilities of the outcomes of an event are known) without being given any additional information (Acquisti and Grossklags, 2012).
So far, Information Systems researchers have studied the impact of privacy risks on privacy concerns (e.g. H. Xu et al., 2011) and behavioural intentions such as the intention to disclose personal information (e.g. Adjerid, Peer, and Acquisti, 2018; Keith et al., 2013; Krasnova et al., 2010). However, there is surprisingly little research studying the link between privacy and ambiguity. An exception is Acquisti and Grossklags (2012) who discuss risk and ambiguity in the context of privacy decision-making and explore the influence of marketing offers with ambiguous privacy consequences on the valuation of different categories of personal data. In the context of cybersecurity and identity theft, P. A. Wang and Nyshadham (2011) compare users' attitudes and intentions under different knowledge states (i.e. certainty, risk, ambiguity) and show that users may be willing to pay a premium to avoid ambiguity. Moreover, Fuchs et al. (2016) illustrate different types of ambiguity in the context of big data (i.e. data ambiguity, process ambiguity, outcome ambiguity) and show that the type of ambiguity may influence users' intention to accept algorithmic recommendations.
The present study contributes to the scant research regarding privacy decision-making in the context of uncertainty. Specifically, it is explored whether users prefer situations of risk or ambiguity regarding privacy loss. It is assumed that transparency helps users reduce ambiguity and shift to a situation of risk.

2.2 Transparency

In principle, privacy policies are designed to reduce information asymmetries by informing users about the data handling practices of a particular CSP (Milne and Culnan, 2002). In practice, however, these are often difficult to understand and time consuming to read (Jensen and Potts, 2004; McDonald and Cranor, 2008; Tsai et al., 2011). As a result, even though users recognise that they can consult a CSP's privacy policies, they hardly read them and still lack information to make informed decisions regarding data disclosure (Milne and Culnan, 2002; Tsai et al., 2011). Transparency features that give users a simplified overview over which (personal) data a CSP collects, stores and uses may facilitate the evaluation of privacy risks and reduce ambiguity (Awad and Krishnan, 2006; Karwatzki et al., 2017).
Information Systems researchers have investigated the effectiveness of transparency in specific application contexts such as recommender systems, e-commerce, targeted advertising and personalisation. For example, several studies show a positive effect of explaining the reasoning behind personalised recommendations on the confidence in recommendations (e.g. Sinha and Swearingen, 2002), acceptance of recommendations (e.g. Herlocker, Konstan, and Riedl, 2000), or trusting beliefs regarding recommendations (e.g. W. Wang and Benbasat, 2007; W. Wang, J. Xu, and M. Wang, 2018). In the context of e-commerce, transparency may induce users to purchase from retailers which better protect their privacy (Tsai et al., 2011). Regarding online advertising, transparency about the collection of (personal) data may lead to a positive effect of ad targeting and personalisation on ad effectiveness (Aguirre et al., 2015). Further research has identified factors which influence the effectiveness of transparency in the context of advertising, such as the type of information revealed and trust (T. Kim, Barasz, and John, 2019) as well as users' opinion on targeting (Samat, Acquisti, and Babcock, 2017).
All of the aforementioned studies focus on the effect of transparency on users' acceptance of a specific data use by a CSP. Fewer studies explore the effect of transparency on data disclosure behaviour: in the context of personalisation, a positive significant effect of transparency on the intention to disclose data has not been found (Karwatzki et al., 2017). This is explained by the dual effect of transparency: even though transparency features provide users with information necessary for privacy decision-making, they

may also trigger privacy concerns which dampen disclosure intentions (Karwatzki et al., 2017). Moreover, research shows that the effect of transparency is sensitive to framing and simple misdirections (Adjerid, Acquisti, Brandimarte, et al., 2013).
Common to all studies is that users are exogenously assigned to either a scenario with transparency or a scenario without transparency when asked to indicate attitudes and behavioural intentions. In contrast, this study explores whether users actually prefer transparency by implementing a decision situation involving an endogenous choice of transparency. Whereas previous research on transparency has largely relied on scenario-based surveys, this study devises a laboratory experiment based on research on decision making under uncertainty.

2.3 Decision making under uncertainty

In the field of decision analysis, decision making under uncertainty, i.e. risk and ambiguity, has been studied extensively, primarily with urn experiments. Originally, Ellsberg (1961) suggested that subjects tend to avoid ambiguity and prefer situations with risk (*ambiguity aversion*). A large number of studies have replicated this result, but, like Ellsberg, they have largely focused on uncertain gains and moderate likelihood events (Kocher, Lahno, and Trautmann, 2018; Li et al., 2018). More recent studies reveal more nuanced results: similar to risk attitudes (Tversky and Kahneman, 1992), ambiguity attitudes seem to depend on the domain of the outcome as well as the probability range and follow a fourfold pattern (Kocher, Lahno, and Trautmann, 2018; Trautmann and Van De Kuilen, 2015): in the gain domain, ambiguity aversion is prevailing for moderate to high probabilities and ambiguity seeking for low probabilities. In the loss domain, ambiguity aversion is prevailing for unlikely losses and ambiguity seeking for moderate to high probability losses. This reversal of attitudes is often explained by fear and hope effects (Viscusi and Chesson, 1999).
So far, most studies on ambiguity attitudes have used money as the outcome variable in contexts such as financial investments (e.g. Du and Budescu, 2005) or technology adoption (e.g. Barham et al., 2014). Despite the prominence of uncertainty in the context of privacy decision-making (see Chapter 2.1), ambiguity attitudes in the context of data (loss) are yet to be studied. Hence, the present study will use an Ellsberg-type experimental design in order to elicit ambiguity attitudes in the context of data loss. Based upon this, subjects' preferences for transparency are derived. It is assumed that a transparent CSP gives users more information about data collection, use and protection. Thus, it is easier for users to estimate the probability of adverse consequences such as data breaches. That is, in a stylised setting, a transparent CSP corresponds to a situation of risk and a non-transparent CSP to a situation of ambiguity. As there is no empirical evidence or theory that would allow a prediction, it is assumed that ambiguity attitudes regarding data coincide with ambiguity attitudes regarding money. Therefore, the following hypotheses are derived from the findings on ambiguity attitudes with respect to money loss in different probability ranges (as explained above):

Hypothesis 1: *If subjects choose between a transparent and a non-transparent online CSP,*

(a) subjects prefer transparency (i.e. risk) if the probability of data loss is low (ambiguity aversion).

(b) subjects avoid transparency (i.e. risk) if the probability of data loss is high (ambiguity seeking).

Additionally, the present study will conduct a money-loss treatment. Replicating previous studies, this baseline allows to explicitly test whether ambiguity attitudes with respect to data loss systematically differ from ambiguity attitudes with respect to money loss. In line with the reasoning above and Hypothesis 1, the following hypothesis is proposed:

Hypothesis 2: *There is no systematic difference between ambiguity attitudes with respect to money loss and ambiguity attitudes with respect to data loss.*

3 Methodology

In the following, the study's experimental design to elicit ambiguity attitudes in the context of data loss and money loss is presented (based on Kocher, Lahno, and Trautmann, 2018). As explained above, ambiguity aversion is expected in the low probability treatments and ambiguity seeking in the moderate probability treatments.

3.1 Experimental design

The experiment implements a full-factorial 2 (data vs. money) x 2 (low vs. moderate probability to lose) between-subject design in order to obtain independent observations for each treatment cell (see Table 1). Participants will be recruited from the subject pool of the University of Passau using *ORSEE* (Greiner, 2015) and the experiment is programmed using the experimental software *oTree* (Chen, Schonger, and Wickens, 2016).

Treatment	Data (D)	Money (M)
(L) Low probability ($p_n = 0.1$)	DL	ML
(M) Moderate probability ($p_n = 0.5$)	DM	MM

Table 1. Experimental treatments.

To ensure experimental control and internal validity, subjects have to be incentivised appropriately (V. L. Smith, 1976). Thus, each participant receives a show-up fee of 5 EUR and an endowment of K EUR after successfully completing a real effort task (see Charness, Gneezy, and Henderson, 2018, for an overview). The endowment is identical for all participants in all treatments. In the data treatment, it serves as an incentive for participants to stay in the experiment and to enter their personal data. In the money treatment, the endowment protects participants from negative earnings in the experiment. In all treatments, participants may exit the experiment at any time and forego their endowment.

3.2 Data loss under uncertainty (data treatment)

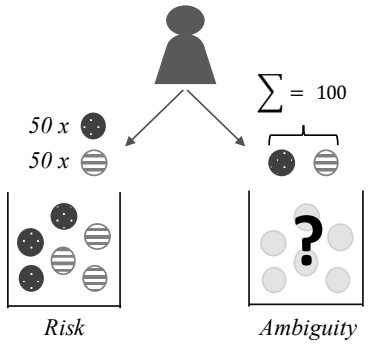
After informing participants about potential data disclosure and signing consent forms, personal data about the participants is collected, which is later put under threat of disclosure in the laboratory. Next, participants face nine decision tasks in which they choose between an ambiguous and a risky bag for different known probabilities p_i in the risk scenario. Ambiguity attitudes are then determined by comparing probability equivalents p_{eq} to the ambiguity-neutral probability p_n. After the decision tasks, participants have to fill out a questionnaire and the experimental outcome is implemented (as explained below).

Collection of personal data: In principle, different types of data could be collected in the laboratory. Demographic data such as age, education, martial status and annual income represent one possibility (e.g. Marreiros et al., 2017). However, participants may not consider this information as overly sensitive for disclosure. Moreover, some studies use quizzes or intelligence tests (e.g. Feri, Giannetti, and Jentzsch, 2016; Grossklags and Acquisti, 2007) but this could divide participants into good and bad types and influence user behaviour heterogeneously (Frik and Gaudeul, 2018). Another possibility are questions on the engagement in ethically questionable behaviour such as drug use, lying, pornography or rape (e.g. Acquisti, John, and Loewenstein, 2012; John, Acquisti, and Loewenstein, 2011). However, participants may not tell the truth due to conformity bias and the disclosure of this data could be misused to damage participants (Frik and Gaudeul, 2018). Finally, opinions on statements regarding controversial and socially relevant topics such as vaccination, abortion and euthanasia could be elicited (Frik and Gaudeul, 2018). This would overcome the aforementioned disadvantages as a majority opinion regarding these topics often

does not exist in society. To test this assumption, the sensitivity and monetary valuation of different data types are measured in a pre-study in order to decide which type of data will be collected and to determine the amount K EUR of the initial endowment in both the data and money treatment.

Decision tasks: Participants choose from which of the two bags a coloured chip is randomly drawn (see Figure 1(a)). Both bags are opaque and contain 100 chips of j different colours. At the beginning of the experiment, participants choose their personal decision colour which ultimately defines the losing event. This is to avoid that the participants suspect the experimenters to trick them (Pulford, 2009). If a chip of the personal decision colour is later drawn from the selected bag, the participant has to disclose her personal data in front of the other participants. Each participant makes nine binary choices for different probabilities p_i in the risky bag and chooses her preferred bag in the middle column for each row i (see Figure 1(b) for a mock-up of the screen shown to participants).
The composition of colours is known in the risky bag: the bag contains $p_i \times 100$ chips of the personal decision colour and $(1 - p_i) \times 100$ chips of the other colour(s) (either one or nine other colours, depending on the respective treatment). In contrast, the composition of colours is unknown in the ambiguous bag which has been prepared in advance by an outside party such as a student assistant. Moreover, it is announced that participants can inspect the bags after the experiment. In the low probability treatment, the ambiguous bag contains at most ten colours ($j = 10$) and in the moderate probability treatment, the ambiguous bag contains at most two colours ($j = 2$). In each treatment, there is one losing colour, i.e. the personal decision colour chosen at the beginning of the experiment. This is equivalent to an ambiguity-neutral probability $p_n = 1/j = 0.1$ in the low probability treatment L and $p_n = 1/j = 0.5$ in the moderate probability treatment M.

(a)



(b)

Row i	100 chips in bag R		R	A	100 chips in bag A	
	Probability of personal decision colour & data loss (p_i)	Probability of other colour & no data loss ($1 - p_i$)			Probability of personal decision colour & data loss	Probability of other colour & no data loss
1	.25	.75	☐	☐	unknown	1 - unknown
2	.30	.70	☐	☐		
3	.35	.65	☐	☐		
4	.40	.60	☐	☐		
5	.45	.55	☐	☐		
6	.50	.50	☐	☐		
7	.55	.45	☐	☐		
8	.60	.40	☐	☐		
9	.65	.35	☐	☐		

Figure 1. Participants' decision situation in the moderate probability scenario DM ($p_n = 0.5$).

Determination of ambiguity attitudes: Following Kocher, Lahno, and Trautmann (2018), the known probability p_i increases across the rows i. Thus, the risky bag becomes less attractive when going down the choice list. Consequently, there should be a probability at which the participant is indifferent between the two bags and eventually switches from the risky to the ambiguous bag. This probability determines the probability equivalent p_{eq} which is compared to the ambiguity-neutral probability p_n in order to elicit participants' ambiguity attitudes (see e.g. Dimmock, Kouwenberg, and Wakker, 2016).
Subjects are assumed to assign a subjective probability to the event that their personal decision colour is drawn from the ambiguous bag. As shown by Chew and Sagi (2008), an ambiguity-neutral decision maker would assign probability $p_n = 1/j$ to the event that her personal decision colour is drawn from

the ambiguous bag and consequently, would switch from risk to ambiguity at this probability, such that $p_{eq} = p_n$. However, if the probability equivalent p_{eq} is larger than the ambiguity-neutral probability p_n, a participant is classified as ambiguity averse. In contrast, if p_{eq} is smaller than p_n, a participant is classified as ambiguity seeking. For example, in the moderate probability scenario ($j = 2$), the ambiguity-neutral probability would be $p_n = 0.5$ (one losing colour and two colours in total). If a participant switches from risk to ambiguity at a probability $p_i < 0.5$, she is classified as ambiguity seeking. In contrast, if she switches at a probability $p_i > 0.5$, she is classified as ambiguity averse. The choice lists are designed so that p_n is in the middle of the table in order to reduce design-driven biases in the measurement of p_{eq} (see Kocher, Lahno, and Trautmann, 2018).

Questionnaire: After the decision task, the participants have to fill out a questionnaire with questions on demographics, the experimental procedure and privacy attitudes. By measuring constructs such as Internet privacy concerns (Dinev and Hart, 2006), disposition to value privacy (Karwatzki et al., 2017), privacy awareness, previous privacy experience and perceived privacy risk (H. Xu et al., 2011), it is possible to compare stated attitudes and intentions with actual behaviour.

Outcome: At the end of each session, one participant and one of the nine decision tasks are randomly selected for implementation. If the chip drawn from the chosen bag is of the selected participant's personal decision colour, the outcome is a data loss and the participant has to stand in front of the other participants. Her name, photo and the collected personal data are then displayed on the screens (see Frik and Gaudeul, 2018).

3.3 Money loss under uncertainty (money treatment)

In the money treatment, the same personal data is collected in order to make sure that stated opinions do not vary systematically between both treatments. Next, participants face the same nine decision tasks as in the data-loss treatment. The only difference is that the outcome triggered by the personal decision colour is not a disclosure of data but a loss of the endowment of K EUR. Ambiguity attitudes are then determined in the same way as in the data treatment and participants have to fill out the same questionnaires.

4 Contributions, limitations and outlook

In conclusion, this study is the first to elicit ambiguity attitudes regarding personal data and to compare them to ambiguity attitudes regarding money. Thereby, it contributes to the scant research studying the link between privacy decision-making, risk and ambiguity. Simultaneously, this study explores endogenous transparency choices in order to inform CSPs and policy makers about the desirability of transparency in different uncertainty settings.

To achieve internal validity by the means of a controlled environment, laboratory experiments must rely on a stylised representation of reality. Of course, this limits external validity and thus, generalisability. In order to test the robustness of the findings, it is planned to extend this study to the field with data from an online service. Moreover, treatments with differing disclosure contexts (Samat and Acquisti, 2017) and interdependent privacy decisions (Pu and Grossklags, 2017) will be added. The next steps include conducting the pre-study on data valuation and running pilot sessions to validate the treatment design.

References

Abdellaoui, M., F. Vossmann, and M. Weber (2005). "Choice-based elicitation and decomposition of decision weights for gains and losses under uncertainty." *Management Science* 51 (9), 1384–1399.

Acquisti, A., I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang, and S. Wilson (2017). "Nudges for privacy and security: understanding and assisting users' choices online." *ACM Computing Surveys (CSUR)* 50 (3), 44:1–44:41.

Acquisti, A., A. Friedman, and R. Telang (2006). "Is there a cost to privacy breaches? An event study." In: *Proceedings of the 27th International Conference on Information Systems (ICIS 2006)*. Milwaukee, WI, USA: Association for Information Systems, p. 94.

Acquisti, A. and J. Grossklags (2008). "What can behavioral economics teach us about privacy?" In: *Digital Privacy: Theory, Technologies and Practices*. Ed. by A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. De Capitani di Vimercati. Boca Raton, FL, USA: Auerbach Publications. Chap. 18, pp. 363–377.

— (2012). "An online survey experiment on ambiguity and privacy." *Communications & Strategies* 88 (4), 19–39.

Acquisti, A., L. K. John, and G. Loewenstein (2012). "The impact of relative standards on the propensity to disclose." *Journal of Marketing Research* 49 (2), 160–174.

Acquisti, A., C. Taylor, and L. Wagman (2016). "The economics of privacy." *Journal of Economic Literature* 54 (2), 442–492.

Acquisti, A. and H. R. Varian (2005). "Conditioning prices on purchase history." *Marketing Science* 24 (3), 367–381.

Adjerid, I., A. Acquisti, L. Brandimarte, and G. Loewenstein (2013). "Sleights of privacy: Framing, disclosures, and the limits of transparency." In: *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS)*. New York, NY, USA: ACM, p. 9.

Adjerid, I., A. Acquisti, and G. Loewenstein (2018). "Choice architecture, framing, and cascaded privacy choices." *Management Science*. Article in Advance. https://doi.org/10.1287/mnsc.2018.3028.

Adjerid, I., E. Peer, and A. Acquisti (2018). "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making." *MIS Quarterly* 42 (2), 465–488.

Aguirre, E., D. Mahr, D. Grewal, K. de Ruyter, and M. Wetzels (2015). "Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness." *Journal of Retailing* 91 (1), 34–49.

Akerlof, G. A. (1970). "The market for "lemons": Quality uncertainty and the market mechanism." *The Quarterly Journal of Economics* 84 (3), 488–500.

Aleem, U., H. Cavusoglu, and I. Benbasat (2017). "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps." In: *Proceedings of the 16th Annual Workshop on the Economics of Information Security (WEIS)*. La Jolla, CA, USA, p. 1.

Awad, N. F. and M. S. Krishnan (2006). "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization." *MIS Quarterly* 30 (1), 13–28.

Barham, B. L., J.-P. Chavas, D. Fitz, V. R. Salas, and L. Schechter (2014). "The roles of risk and ambiguity in technology adoption." *Journal of Economic Behavior & Organization* 97, 204–218.

Beke, F. T., F. Eggers, and P. C. Verhoef (2018). "Consumer Informational Privacy: Current Knowledge and Research Directions." *Foundations and Trends® in Marketing* 11 (1), 1–71.

Brandimarte, L., A. Acquisti, and G. Loewenstein (2013). "Misplaced confidences: Privacy and the control paradox." *Social Psychological and Personality Science* 4 (3), 340–347.

Charness, G., U. Gneezy, and A. Henderson (2018). "Experimental methods: Measuring effort in economics experiments." *Journal of Economic Behavior & Organization* 149, 74–87.

Chen, D. L., M. Schonger, and C. Wickens (2016). "oTree—An open-source platform for laboratory, online, and field experiments." *Journal of Behavioral and Experimental Finance* 9, 88–97.

Chew, S. H. and J. S. Sagi (2008). "Small worlds: Modeling attitudes toward sources of uncertainty." *Journal of Economic Theory* 139 (1), 1–24.

Culnan, M. J. and P. K. Armstrong (1999). "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation." *Organization Science* 10 (1), 104–115.

Culnan, M. J. and R. J. Bies (2003). "Consumer privacy: Balancing economic and justice considerations." *Journal of Social Issues* 59 (2), 323–342.

Dimmock, S. G., R. Kouwenberg, and P. P. Wakker (2016). "Ambiguity attitudes in a large representative sample." *Management Science* 62 (5), 1363–1380.

Dinev, T. and P. Hart (2006). "An extended privacy calculus model for e-commerce transactions." *Information Systems Research* 17 (1), 61–80.

Dinev, T., A. R. McConnell, and H. J. Smith (2015). "Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box." *Information Systems Research* 26 (4), 639–655.

Du, N. and D. V. Budescu (2005). "The effects of imprecise probabilities and outcomes in evaluating investment options." *Management Science* 51 (12), 1791–1803.

Ellsberg, D. (1961). "Risk, ambiguity, and the Savage axioms." *The Quarterly Journal of Economics* 75 (4), 643–669.

Federal Trade Commission (2000). *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*. URL: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (visited on 03/26/2019).

Feri, F., C. Giannetti, and N. Jentzsch (2016). "Disclosure of personal information under risk of privacy shocks." *Journal of Economic Behavior & Organization* 123, 138–148.

Frik, A. and A. Gaudeul (2018). "An experimental method for the elicitation of implicit attitudes to privacy risk." Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211184.

Fuchs, C., C. Matt, T. Hess, and C. Hoerndlein (2016). "Human vs. Algorithmic Recommendations in Big Data and the Role of Ambiguity." In: *Twenty-second Americas Conference on Information Systems (AMCIS)*. San Diego, CA, USA: AIS, p. 1.

Goes, P. B. (2013). "Editor's comments: information systems research and behavioral economics." *MIS Quarterly* 37 (3), iii–viii.

Goldfarb, A. (2014). "What is different about online advertising?" *Review of Industrial Organization* 44 (2), 115–129.

Golman, R., D. Hagmann, and G. Loewenstein (2017). "Information avoidance." *Journal of Economic Literature* 55 (1), 96–135.

Greiner, B. (2015). "Subject pool recruitment procedures: organizing experiments with ORSEE." *Journal of the Economic Science Association* 1 (1), 114–125.

Grossklags, J. and A. Acquisti (2007). "When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information." In: *Proceedings of the 6th Annual Workshop on the Economics of Information Security (WEIS)*. Pittsburgh, PA, USA, p. 1.

Grossman, Z. and J. J. Van Der Weele (2017). "Self-image and willful ignorance in social decisions." *Journal of the European Economic Association* 15 (1), 173–217.

Herlocker, J. L., J. A. Konstan, and J. Riedl (2000). "Explaining collaborative filtering recommendations." In: *Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work (CSCW)*. New York, NY, USA: ACM, p. 241.

Hertwig, R. and C. Engel (2016). "Homo ignorans: Deliberately choosing not to know." *Perspectives on Psychological Science* 11 (3), 359–372.

Ho, J. L. Y., L. R. Keller, and P. Keltyka (2002). "Effects of outcome and probabilistic ambiguity on managerial choices." *Journal of Risk and Uncertainty* 24 (1), 47–74.

Isaac, M. (2018). *Facebook Hack Included Search History and Location Data of Millions*. URL: https://www.nytimes.com/2018/10/12/technology/facebook-hack-investigation.html (visited on 11/27/2018).

Jensen, C. and C. Potts (2004). "Privacy policies as decision-making tools: an evaluation of online privacy notices." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Vienna, Austria: ACM, p. 471.

Jentzsch, N., G. Sapi, and I. Suleymanova (2013). "Targeted pricing and customer data sharing among rivals." *International Journal of Industrial Organization* 31 (2), 131–144.

John, L. K., A. Acquisti, and G. Loewenstein (2011). "Strangers on a plane: Context-dependent willingness to divulge sensitive information." *Journal of Consumer Research* 37 (5), 858–873.

Karwatzki, S., O. Dytynko, M. Trenz, and D. Veit (2017). "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization." *Journal of Management Information Systems* 34 (2), 369–400.

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

Khosrowshahi, D. (2017). *2016 Data Security Incident*. URL: `https://www.uber.com/newsroom/2016-data-incident` (visited on 03/26/2019).

Kim, T., K. Barasz, and L. K. John (2019). "Why am I seeing this ad? The effect of ad transparency on ad effectiveness." *Journal of Consumer Research* 45 (5), 906–932.

Kocher, M. G., A. M. Lahno, and S. T. Trautmann (2018). "Ambiguity aversion is not universal." *European Economic Review* 101, 268–283.

Krasnova, H., S. Spiekermann, K. Koroleva, and T. Hildebrand (2010). "Online social networks: Why we disclose." *Journal of Information Technology* 25 (2), 109–125.

Laufer, R. S. and M. Wolfe (1977). "Privacy as a concept and a social issue: A multidimensional developmental theory." *Journal of Social Issues* 33 (3), 22–42.

Li, Z., J. Müller, P. P. Wakker, and T. V. Wang (2018). "The Rich Domain of Ambiguity Explored." *Management Science* 64 (7), 3227–3240.

Lowry, P. B., T. Dinev, and R. Willison (2017). "Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda." *European Journal of Information Systems* 26 (6), 546–563.

Malhotra, A. and C. Kubowicz Malhotra (2011). "Evaluating customer information breaches as service failures: An event study approach." *Journal of Service Research* 14 (1), 44–59.

Malhotra, N. K., S. S. Kim, and J. Agarwal (2004). "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." *Information Systems Research* 15 (4), 336–355.

Marreiros, H., M. Tonin, M. Vlassopoulos, and M. Schraefel (2017). ""Now that you mention it": A survey experiment on information, inattention and online privacy." *Journal of Economic Behavior & Organization* 140, 1–17.

Martin, K. D., A. Borah, and R. W. Palmatier (2017). "Data privacy: Effects on customer and firm performance." *Journal of Marketing* 81 (1), 36–58.

McDonald, A. M. and L. F. Cranor (2008). "The cost of reading privacy policies." *I/S: A Journal of Law and Policy for the Information Society (ISJLP)* 4 (3), 543–568.

Milne, G. R. and M. J. Culnan (2002). "Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 US Web surveys." *The Information Society* 18 (5), 345–359.

OECD (2013). *The OECD Privacy Framework*. URL: `http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf` (visited on 03/26/2019).

Peter, J. P. and L. X. Tarpey Sr. (1975). "A comparative analysis of three consumer decision strategies." *Journal of Consumer Research* 2 (1), 29–37.

Pu, Y. and J. Grossklags (2017). "Valuating Friends' Privacy: Does Anonymity of Sharing Personal Data Matter?" In: *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS)*. Santa Clara, CA, USA: USENIX Association, p. 339.

Pulford, B. D. (2009). "Is luck on my side? Optimism, pessimism, and ambiguity aversion." *The Quarterly Journal of Experimental Psychology* 62 (6), 1079–1087.

Samat, S. and A. Acquisti (2017). "Format vs. Content: The Impact of Risk and Presentation on Disclosure Decisions." In: *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS)*. Santa Clara, CA, USA: USENIX Association, p. 377.

Samat, S., A. Acquisti, and L. Babcock (2017). "Raise the Curtains: The Effect of Awareness About Targeting on Consumer Attitudes and Purchase Intentions." In: *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS)*. Santa Clara, CA, USA: USENIX Association, p. 299.

Schweizer, N. and N. Szech (2018). "Optimal revelation of life-changing information." *Management Science* 64 (11), 4697–5460.

Sinha, R. and K. Swearingen (2002). "The role of transparency in recommender systems." In: *CHI'02 Extended Abstracts on Human Factors in Computing Systems*. Minneapolis, MN, USA: ACM, p. 830.

Smith, H. J., S. J. Milberg, and S. J. Burke (1996). "Information privacy: measuring individuals' concerns about organizational practices." *MIS Quarterly* 20 (2), 167–196.

Smith, V. L. (1976). "Experimental economics: Induced value theory." *The American Economic Review* 66 (2), 274–279.

Stigler, G. J. (1961). "The economics of information." *The Journal of Political Economy* 69 (3), 213–225.

Trautmann, S. T. and G. Van De Kuilen (2015). "Ambiguity attitudes." In: *The Wiley Blackwell Handbook of Judgment and Decision Making*. Ed. by G. Keren and G. Wu. Vol. 1. Chichester, UK: John Wiley & Sons. Chap. 3, pp. 89–116.

Tsai, J. Y., S. Egelman, L. Cranor, and A. Acquisti (2011). "The effect of online privacy information on purchasing behavior: An experimental study." *Information Systems Research* 22 (2), 254–268.

Tucker, C. E. (2012). "The economics of advertising and privacy." *International Journal of Industrial Organization* 30 (3), 326–329.

Tversky, A. and D. Kahneman (1992). "Advances in prospect theory: Cumulative representation of uncertainty." *Journal of Risk and Uncertainty* 5 (4), 297–323.

Viscusi, W. K. and H. Chesson (1999). "Hopes and fears: the conflicting effects of risk ambiguity." *Theory and Decision* 47 (2), 157–184.

Wang, P. A. and E. Nyshadham (2011). "Knowledge of online security risks and consumer decision making: An experimental study." In: *Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS)*. Koloa, Hawaii: IEEE, p. 1.

Wang, W. and I. Benbasat (2007). "Recommendation agents for electronic commerce: Effects of explanation facilities on trusting beliefs." *Journal of Management Information Systems* 23 (4), 217–246.

Wang, W., J. Xu, and M. Wang (2018). "Effects of Recommendation Neutrality and Sponsorship Disclosure on Trust vs. Distrust in Online Recommendation Agents: Moderating Role of Explanations for Organic Recommendations." *Management Science* 64 (11), 4967–5460.

Xu, H., T. Dinev, J. Smith, and P. Hart (2011). "Information privacy concerns: Linking individual perceptions with institutional privacy assurances." *Journal of the Association for Information Systems* 12 (12), 798–824.