ICIS 2022 Proceedings

Cybersecurity, Privacy and Ethics in AI

Dec 12th, 12:00 AM

Privacy Risks in Digital Markets: The Impact of Ambiguity Attitudes on Transparency Choices

Nikolai Sachs
University of Passau, nikolai.sachs@uni-passau.de

Daniel Schnurr
University of Passau, daniel.schnurr@ur.de

Recommended Citation

Sachs, Nikolai and Schnurr, Daniel, "Privacy Risks in Digital Markets: The Impact of Ambiguity Attitudes on Transparency Choices" (2022). *ICIS 2022 Proceedings*. 12.
https://aisel.aisnet.org/icis2022/security/security/12

Privacy Risks in Digital Markets: The Impact of Ambiguity Attitudes on Transparency Choices

Completed Research Paper

Nikolai Sachs
University of Passau
Dr.-Hans-Kapfinger-Str. 12
94032 Passau, Germany
nikolai.sachs@uni-passau.de

Daniel Schnurr
University of Regensburg
93040 Regensburg, Germany
daniel.schnurr@ur.de

Abstract

Transparency is viewed as an essential prerequisite for consumers to make informed privacy decisions in digital markets. However, it remains an open research question whether and when individuals actually prefer transparency about privacy risks when given a chance to avoid it. We investigate this question with a randomized controlled online experiment based on an Ellsberg-type design, where subjects repeatedly choose between risk and ambiguity while facing the threat of an actual disclosure of their personal data. We find empirical support for ambiguity attitudes as a novel behavioral mechanism underlying people's transparency choices in privacy contexts. In particular, we find that most individuals avoid ambiguity and prefer transparency for low likelihood privacy losses. However, this pattern reverses for high likelihood losses and when subjects perceive data disclosure as a gain. Most notably, a significant share of people seek ambiguity and thus prefer to avoid transparency when facing high likelihood privacy risks.

Keywords: Privacy, transparency, privacy uncertainty, privacy risks, ambiguity attitudes

Introduction

Digital devices and services frequently collect large amounts of user data, for example, to personalize services or to display targeted advertisements (Tucker 2012). As the Internet of Things (IoT) increasingly connects everyday devices such as music speakers, door locks or security cameras, this collection of personal data is becoming omnipresent. However, most consumers do not know about the extent to which devices and services collect data about them, how the data is used or how it is protected (Al-Natour et al. 2020). At the same time, a majority of users feel that disclosing their personal data involves risks of data being misused by companies or information being compromised in data breaches (The Harris Poll 2020). Frequent data breaches (Identity Theft Resource Center 2021) and the large number of consumers affected by recent privacy incidents on popular digital platforms such as Facebook (Peters 2021) or Yahoo (Perlroth 2017) underscore that sharing data with firms can entail significant privacy risks. Therefore, data protection regulations such as the European General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) stipulate that data processing practices should be transparent such that consumers can make informed privacy decisions. Although most firms comply with the legal requirements by posting privacy policies, these are often difficult to understand and are thus rarely read by consumers (Obar and Oeldorf-Hirsch 2020).

Thus, efforts to increase the transparency of privacy practices in digital markets are ongoing. This is, in particular, the case for the IoT, where privacy and security attributes of smart devices are often highly opaque and non-transparent to users (Blythe et al. 2019). In consequence, regulators and consumer protection advocates have called on IoT device manufacturers to be more transparent about how their IoT devices process personal data so that consumers are made aware of the privacy implications when buying and using these products (BEUC 2017). In both the EU and the US, this has propelled initiatives to introduce IoT product labels that shall offer users greater transparency about privacy risks (European Commission 2016; Executive Order 14028 2021). Yet, these initiatives rely on IoT manufacturers to voluntarily adopt such product labels. In particular, policymakers envision that when consumers can integrate privacy attributes into their purchase and use decisions, privacy becomes a salient dimension along which manufacturers will compete. In turn, this may create a virtuous circle where manufacturers have incentives to offer more privacy-friendly products. Evidently, this reasoning hinges crucially on the assumption that consumers actively choose more transparent products. However, so far, there is little research on consumers' decision-making in situations where they can choose between products or services that are more or less transparent about the involved privacy risks. In fact, despite the beneficial effects of transparency, previous studies have found that consumers sometimes avoid information or react negatively to transparency (Brough et al. 2022; Kim et al. 2019).

In this study, we, therefore, draw on the theory on decision making under uncertainty to investigate people's choices between more and less transparency in privacy contexts. From a behavioral economics perspective, transparency choices in privacy contexts can be generalized to a decision between different degrees of uncertainty about privacy risk. In particular, we argue that transparency corresponds to a situation where individual decision makers are informed about privacy risks (i.e., the probabilities for an uncertain disclosure of personal data can be estimated). In contrast, without transparency, decision makers face a situation of ambiguity (i.e., the probabilities for an uncertain disclosure of personal data are unknown). Building on the well-established theory of ambiguity attitudes, we, therefore, empirically investigate the research question of how individuals choose between different degrees of uncertainty when the consequence of this choice is the disclosure of individuals' personal data to others.

In a randomized controlled online experiment based on an Ellsberg-type design that puts subjects' personal data under threat of actual disclosure, we find that ambiguity aversion among subjects prevails for low likelihood losses, but ambiguity seeking is more prevalent for high likelihood losses. From these findings, we conclude that people prefer transparency when privacy risks are perceived to be low. However, when facing high privacy risks, a significant share of people seeks ambiguity and actively avoids transparency. These results indicate that, when consumers perceive general privacy risks to be low, voluntary transparency initiatives, such as IoT product labels, could promote choices for products that better protect consumers' privacy. In contrast, when consumers perceive privacy risks to be high, a significant share of consumers might prefer to choose non-transparent products, which would undermine the effectiveness of voluntary transparency efforts. Thus, in industries and markets with high privacy risks, mandatory transparency policies may be warranted. In line with previous research on ambiguity attitudes for monetary outcomes, we further find that these transparency preferences reverse if people perceive the disclosure of their personal data as a gain. In this case, transparency is preferred when the likelihood of disclosure is high but ambiguity is preferred if the likelihood is low. Overall, these empirical findings can be rationalized by hope and fear effects (Viscusi and Chesson 1999) that may motivate individuals to prefer ambiguous outcomes and to avoid information about the likelihood of a data disclosure. From a theoretical perspective, our findings suggest that ambiguity preferences represent an important behavioral mechanism that significantly shapes individuals' transparency choices in privacy contexts.

The remainder of this paper is structured as follows. First, we review the related literature, highlight the research gap and develop our hypotheses. We then introduce the experimental design, provide details about the experimental procedures and describe our sample before the experimental results are presented. Before we conclude, we discuss the theoretical contributions and implications for practice of our findings.

Related Literature and Hypotheses

The Effects of Transparency in Privacy Contexts

In the privacy context, transparency is commonly defined as the provision of information about data processing practices (Betzing et al. 2020; Sleziona and Widjaja 2022). These processing practices can entail the collection, storage, use, protection and sharing of personal data (Awad and Krishnan 2006; Brough et al. 2022; Karwatzki et al. 2017; Martin et al. 2017). In general, transparency reduces asymmetric information between users and data-processing firms, which in turn reduces consumers' perceptions of privacy uncertainty, i.e., "consumers' difficulty in assessing the privacy of the information they entrust" to others (Al-Natour et al. 2020, p.2). Therefore, transparency can be conceptualized as the provision of information that reduces consumers' perceived privacy uncertainty.

The effects of transparency in the privacy domain have been studied in diverse contexts such as targeted advertising, e-commerce, apps or social networks. In general, transparency does seem to facilitate informed decision-making of consumers as it significantly increases individuals' comprehension of privacy practices (Betzing et al. 2020). However, the effects of transparency diverge across studies and investigated contexts. Overall, the findings suggest two main countervailing effects of transparency on consumers' behavior. On the one hand, transparency may increase perceptions of fairness (Kim et al. 2019), reciprocity (Zimmer et al. 2010) and trust (Bansal et al. 2015; Liu et al. 2005). Moreover, it may mitigate feelings of vulnerability (Martin et al. 2017). Altogether, this can lead to the disclosure of more sensitive personal information (Zimmer et al. 2010), higher click-through intentions on targeted ads (Aguirre et al. 2015), or higher intention to use an app (Al-Natour et al. 2020). On the other hand, transparency can make privacy issues more salient and thus raise privacy concerns that were previously dormant (Karwatzki et al. 2017; Marreiros et al. 2017). In consequence, despite the potential benefits, providing more transparency may prove ineffective or even have negative effects for firms. In particular, previous studies have found transparency to be ineffective in changing consumers' willingness to disclose personal information (Karwatzki et al. 2017), to have negative or no effects on targeted advertising effectiveness (Kim et al. 2019) or to negatively affect purchase intentions of consumers (Brough et al. 2022). Whether positive or negative effects of transparency prevail has been found to depend on contextual factors such as the content of a transparency message (Kim et al. 2019), the framing of the decision scenario (Brough et al. 2022) or the timing and reference point of decision (Adjerid et al. 2013). Moreover, positive effects of transparency might only emerge in combination with control (Martin et al. 2017) or preexisting trust in the institution that offers transparency (Kim et al. 2019). Finally, people who value transparency are less inclined to consent to data collection, which can render the provision of transparency an ineffective strategy for firms (Awad and Krishnan 2006).

Notably, all these studies employ experimental designs that exogenously assign subjects to conditions with or without transparency. Whereas such designs are well-suited to isolate the effects of a given transparency level, they do not leave subjects with a choice that would reveal their actual preferences between varying levels of transparency. However, given that transparency can only be effective if consumers indeed consider provided information, the question of whether consumers actually prefer and choose transparency in privacy contexts when given the chance to avoid it is fundamental. Therefore, we design our experiment to explicitly elicit individuals' choices between a transparent and a non-transparent option with privacy implications. Up to now, empirical research on this question is scant. A notable exception is Tsai et al. (2011) who find that individuals prefer to buy from sellers for which a search engine provides privacy information. In the IoT context, Johnson et al. (2020) find that consumers generally prefer devices with an IoT label that makes privacy and security information transparent over devices without such a label. We contribute to these findings by scrutinizing a specific behavioral mechanism that may explain transparency choices in privacy contexts and by identifying conditions under which consumers indeed prefer transparency.

Furthermore, the existing literature focuses primarily on measuring the effects of transparency on behavioral intentions such as intention to disclose information (Karwatzki et al. 2017) or intention to click on a targeted advertisement (Aguirre et al. 2015). The predictive power of these studies for actual behavior might, therefore, suffer from the intentions-behavior gap (Morwitz and Munz 2021; Sheeran and Webb 2016). In privacy contexts, this gives rise to the well-known privacy paradox, as individuals frequently state to be concerned about their privacy but are readily willing to disclose their personal data in return for small benefits (Kokolakis 2017; Norberg et al. 2007). Notably, transparency itself has been shown to affect how stated intentions translate into actual behavior (Zimmer et al. 2010). Thus, studies on stated intention may not fully capture the causal effects of transparency on actual behavior. To complement these existing studies, our experiment investigates actual behavior with realized outcomes rather than stated intentions in hypothetical scenarios. Thus, we follow recent calls for more experimental research on actual behavior and revealed preferences (see, e.g., Dinev et al. 2015; Hulland and Houston 2021; Lowry et al. 2017).

With respect to the established body of knowledge on transparency in privacy contexts, it is striking that the findings differ significantly across application contexts and modes of presentation of transparency (Sleziona and Widjaja 2022). Yet, generalizable behavioral mechanisms that can explain these decisions are still poorly understood. Thus, our experiment aims to test such a mechanism and its general effects on individuals' transparency choices in privacy contexts by deliberately abstracting from context-specific factors of various privacy-related decisions in practice. To this end, the employed randomized controlled online experiment (cf. Gupta et al. 2018) allows us to isolate causal mechanisms by controlling for confounding variables such as transaction costs or peripheral cues. In this vein, we can offer a novel theoretical explanation for people's transparency choices in privacy contexts, whose external validity then should be tested further in more context-specific applications by future empirical studies.

Decision Making under Risk and Ambiguity

In this study, we draw on the theory on decision making under uncertainty and conceptualize the decision between more and less transparent options as a choice between different degrees of uncertainty about privacy risk, i.e., the probabilistic disclosure of personal data. For example, consider IoT product labels that convey information about privacy risks associated with the use of connected devices. These labels allow consumers to form more precise estimates about the possibility of a data disclosure for devices with a label than for devices without such a label (Emami-Naeini et al. 2021). Hence, the behavioral economics literature on ambiguity attitudes is closely related to our research question and conceptualization of privacy risks. This stream of literature distinguishes between two major types of uncertainty: risk and ambiguity. In a situation of risk, the decision maker knows the probabilities for the outcomes of an uncertain event, whereas in a situation of ambiguity, the decision maker cannot assign any probabilities to the possible outcomes. Thus, ”[a]mbiguity is introduced by the absence of salient information that could in principle be available to the decision maker” (Trautmann and van de Kuilen 2015, p. 90).

Ambiguity attitudes, therefore, capture individuals' preferences for taking a bet under risk over a bet under ambiguity (Ellsberg 1961). In economic laboratory experiments, this is often presented to subjects as the choice between winning or losing money with a known probability or winning or losing the same amount of money with an unknown probability. Although ambiguity attitudes are closely related to risk attitudes, the two concepts are, by definition, distinct. Whereas ambiguity attitudes capture preferences for known risks over unknown ambiguity, risk attitudes commonly capture preferences for known risks over certain outcomes (Abdellaoui et al. 2011; Dimmock et al. 2016b). In digital markets, privacy risks are inherently uncertain to consumers, as consumers lack perfect information about how the data they disclose is used and protected by organizations. Depending on the level of transparency provided, consumers will thus perceive a situation of risk or a situation of ambiguity. Therefore, our study focuses exclusively on measuring ambiguity attitudes and does not consider risk attitudes.

A well-known finding, going back to the seminal work by Ellsberg (1961), is that people often display ambiguity aversion for uncertain gains of money, i.e., they prefer risk over ambiguity. Later research then identified a more nuanced pattern of ambiguity attitudes (for an overview, see Trautmann and van de Kuilen 2015): When the likelihood of winning money is relatively high, most people avoid ambiguity. However, when the likelihood of winning is low, ambiguity neutrality and ambiguity seeking become more prevalent attitudes. When the outcome is an uncertain loss of money, the pattern reverses. In the loss domain, individuals tend to avoid ambiguity for low likelihoods of losing money but are instead predominantly ambiguity neutral or ambiguity seeking for high likelihoods of losing. More recently, Kocher et al. (2018) investigate monetary gains and losses in a uniform experimental setting and find confirmatory evidence for this fourfold pattern of ambiguity attitudes, i.e., ambiguity aversion in the domain of high likelihood gains, ambiguity seeking for low likelihood gains and a complete reversal of preferences in the loss domain.

A rich body of literature corroborates the general relevance of ambiguity attitudes for a wide variety of decisions and choices. Whereas most studies that elicit ambiguity attitudes focus on monetary outcomes (Trautmann and van de Kuilen 2015), these ambiguity attitudes have been found to generalize to behavior in financial markets (Bianchi and Tallon 2019; Dimmock et al. 2016a), predict the choice of established brands

(Muthukrishnan et al. 2009), explain technology choices (Barham et al. 2014) and predict health-related behavior in school children (Sutter et al. 2013). In this spirit, Li et al. (2018) call for more research on ambiguity attitudes with respect to different outcomes and sources of uncertainty.

Thus, in this study, we explore the role of ambiguity attitudes for outcomes that involve individuals' uncertain disclosure of personal data as opposed to monetary outcomes. This is especially relevant as the privacy domain is characterized by numerous risks to an intangible good of significant value to most people (Lin 2021; Al-Natour et al. 2020) and as privacy decision-making is known to be subject to various behavioral biases (Acquisti et al. 2015; Dinev et al. 2015). In addition, personal data is fundamentally different from money due to its non-rivalry. People can experience a "privacy loss" and still be in possession of their personal data that has been disclosed to others. Moreover, people have been shown to attribute very heterogeneous valuations to their personal data (see, among others, Benndorf and Normann 2018; Schudy and Utikal 2017), which is in stark contrast to the objective value of money.

Despite these idiosyncrasies of data and calls for more research on behavioral economics phenomena in privacy contexts (see e.g., Arnott and Gao 2022; Dinev et al. 2015; Goes 2013), the effects of ambiguity attitudes on individuals' privacy decisions have so far received scant attention. A notable exception is Wang and Nyshadham (2011), who elicit people's willingness to pay to avoid a particular situation of uncertainty when facing a probabilistic threat of identity theft. Wang and Nyshadham show that subjects are willing to pay a significantly higher amount of money to avoid a situation of ambiguity than to avoid a situation of risk. Thus, subjects could be indirectly classified as ambiguity averse for the given privacy decision context. However, Wang and Nyshadham do not directly elicit ambiguity attitudes by giving subjects an explicit choice between risk and ambiguity. Moreover, they do not vary the likelihood of the potential data disclosure, which may be an important determinant of individuals' ambiguity attitudes, as suggested by the aforementioned experimental studies on money losses. Therefore, we conduct a more systematic analysis of ambiguity attitudes to shed light on people's attitudes towards different degrees of uncertainty in privacy contexts.

Hypotheses

To derive hypotheses on ambiguity attitudes for decisions with privacy outcomes, we build primarily on the behavioral economics literature that has investigated ambiguity attitudes for decisions with monetary outcomes. In particular, this literature has found that ambiguity attitudes depend on the general likelihood of a probabilistic money gain or money loss (Kocher et al. 2018). Therefore, in our study, we test whether the likelihood of a probabilistic data disclosure affects ambiguity attitudes in the context of privacy outcomes. In particular, we compare situations with low and high likelihood disclosures of personal data, respectively. Moreover, previous experimental studies on monetary outcomes have found that ambiguity attitudes depend on the outcome domain, i.e., on whether people face a probabilistic gain or loss of money (Kocher et al. 2018). This suggests that ambiguity attitudes toward privacy outcomes may also depend on whether subjects perceive the disclosure of their personal data as a gain or a loss. However, whereas for money, there is an objective benchmark on what constitutes a monetary gain or loss, people's privacy valuations are highly heterogeneous across individuals. Therefore, some people may place a very high value on the protection of the same type of personal data that others may readily disclose (Benndorf and Normann 2018; Fast and Schnurr 2020). For example, consider a social media post that suddenly becomes viral and is subject to attention by a larger than expected mass of people. While some people might consider this an undesired disclosure of personal data, others might actively seek such publicity. In consequence, the classification of a data disclosure as a loss or a gain arises endogenously based on individuals' perceptions as opposed to the exogenous and objective nature of monetary gains and losses.

With respect to these contingencies, we first derive our hypothesis on the conditions under which we expect a preference for transparency about risks, i.e., ambiguity aversion, to prevail. As discussed above, ambiguity aversion is found to constitute the prevailing ambiguity attitude for monetary outcomes when there is either a low likelihood money loss or a high likelihood money gain (Kocher et al. 2018). A common interpretation of these findings is that people *fear* ambiguity when known risks are perceived to be low, and thus these risks are assumed to offer a relatively safe option over unknown probabilities (Viscusi and Chesson 1999). Hence, in the case of low likelihood losses, people may perceive known probabilities to promise relatively safe protection, while in the case of high likelihood gains, known probabilities are perceived to promise relatively safe gains. An alternative theoretical explanation suggests that people may generally prefer a risky choice over an ambiguous choice because the risky choice offers more information to the decision maker. Thus, in the case of a choice for the risky option with known probabilities, a loss may be attributed to bad luck, whereas in the case of a choice for the ambiguous option, a loss may be attributed to the incompetence of the decision maker who neglected information that was available for the risky choice (Trautmann et al. 2008).

Based on the empirical findings and theoretical rationalizations offered by the extant literature on ambiguity attitudes for monetary outcomes, we derive the following hypothesis on when to expect people to have a preference for transparency:

Hypothesis 1 (Preference for transparency) *Ambiguity aversion exceeds ambiguity seeking when*
(a) data disclosure is perceived as a loss and the likelihood of disclosure is low,
(b) data disclosure is perceived as a gain and the likelihood of disclosure is high.

Second, we derive our hypothesis on the conditions under which we expect people to prefer ambiguity and avoid transparency about privacy risks. Previous studies on monetary outcomes have found ambiguity attitudes change as the likelihood of a money loss increases or the likelihood of a money gain decreases (Trautmann and van de Kuilen 2015). In particular, it has been found that ambiguity aversion diminishes and more people become ambiguity seeking or ambiguity neutral as the likelihood of a money loss increases (Kocher et al. 2018). Conversely, for money gains, Dimmock et al. (2016b) find that, as the likelihood of a money gain becomes smaller, ambiguity seeking becomes the predominant ambiguity attitude over ambiguity aversion. A consistent interpretation for prevalent ambiguity seeking is given by *hope effects* as the counterpart of fear effects discussed for ambiguity aversion and Hypothesis 1: When the likelihood of losing is relatively high, or the likelihood of winning is relatively low, subjects hope for better chances in the ambiguous option than in the known risk option (Viscusi and Chesson 1999). In line with these empirical results and the theoretical explanation offered by hope and fear effects, we posit the following hypothesis on when to expect people to prefer ambiguity instead of transparency:

Hypothesis 2 (Preference for ambiguity) *Ambiguity seeking exceeds ambiguity aversion when*
(a) data disclosure is perceived as a loss and the likelihood of disclosure is high,
(b) data disclosure is perceived as a gain and the likelihood of disclosure is low.

In summary, we expect a reversal of transparency preferences (i) for low and high likelihoods of data disclosure as well as (ii) for perceived privacy losses and perceived privacy gains. By testing these behavioral predictions empirically, we can evaluate the relevance of the proposed theory on ambiguity attitudes for transparency choices in privacy contexts. Thus, we aim to provide empirical evidence on people's ex-ante transparency preferences and their actual choices between varying degrees of uncertainty about privacy risks, which complements well-established findings on the ex-post effects of transparency. In this vein, we also integrate the co-existing, but so-far isolated, streams of literature on transparency in privacy contexts in IS and on ambiguity attitudes in behavioral economics. Hence, our study contributes to recent calls for IS and privacy research to incorporate theories and phenomena from behavioral economics (see e.g., Arnott and Gao 2022; Dinev et al. 2015; Goes 2013) and to a growing body of research that experimentally studies privacy-decision making (e.g., Adjerid et al. 2013; Adjerid et al. 2019).

Methodology

Experimental Design

We investigate individuals' preferences between risk and ambiguity in the privacy domain based on a randomized controlled online experiment. To elicit revealed preferences with high internal validity, we implemented the well-known choice task by Ellsberg (1961), where subjects must repeatedly choose whether they prefer a random draw from a bag with colored chips of known composition or from a bag with chips of unknown composition. A novel feature in our experimental design is that the uncertain outcome of the draw is the potential disclosure of a subject's actual personal data to all other subjects in the same experimental session. Sensitive and verifiable personal data in the controlled experimental environment was generated by having subjects answer 16 questions of a logic test under time pressure and collecting relative test scores among subjects (The International Cognitive Ability Resource Team 2014). Subjects' test scores were then put under threat of disclosure to other participants (cf. Fast and Schnurr 2020; Feri et al. 2016) according to the experimental procedures described below.

To test our hypotheses on the effects of the likelihood of data disclosure, we exogenously varied the likelihood between a high and a low likelihood treatment. This was operationalized by changing the maximum number of colors of the chips in the bags of the Ellsberg choice tasks. Whereas in the high likelihood treatment, bags would contain chips of at maximum two colors, bags in the low likelihood treatment would contain chips of up to ten colors. As perceptions of privacy gains or losses due to a data disclosure emerge only endogenously, we test our second set of hypotheses on the effects of the outcome domain by eliciting subjects' perceptions about data disclosure in the experiment and split the sample in our analysis accordingly (see the Results).

The experiment employs a between-subjects design, i.e., each subject participates in exactly one treatment. This prevents possible carry-over effects and confounding effects of within-subjects designs. Subjects are aware of the treatment conditions that they are receiving, but they do not know that it is a treatment, nor do they know about the other treatments. Treatments are randomized at the session level. The experiment was run online using the software LimeSurvey, and subjects participated in a Zoom meeting with their cameras turned off and anonymized names during the session.

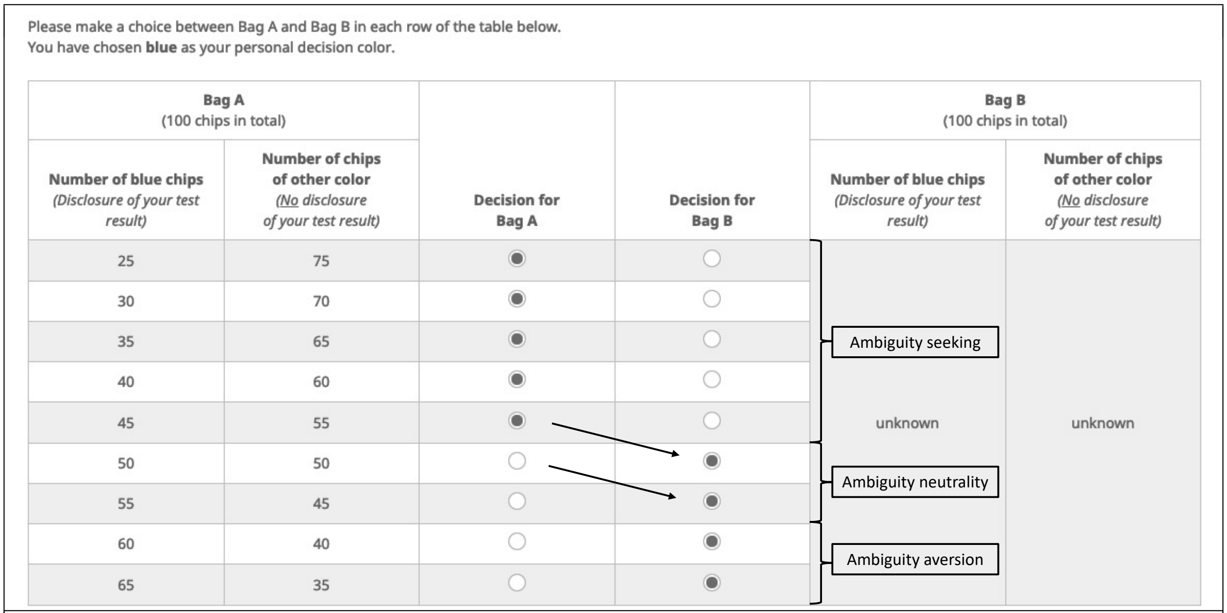
Measurement of Ambiguity Attitudes

We measured ambiguity attitudes using an adaptation of the well-known Ellsberg (1961) choice task by Kocher et al. (2018). In the task, subjects repeatedly chose whether they preferred a random draw from a bag with 100 colored chips of known composition or from a bag with 100 chips of unknown composition. Across treatments, we exogenously varied the maximum number of colors in both bags between ten and two colors, which we refer to as the low likelihood and the high likelihood treatment, respectively. Following Kocher et al. (2018), the choices between the risky and the ambiguous bag were presented to subjects as a choice list, as depicted in Figure 1. In the choice list, every row corresponds to a decision between the two bags, so subjects face a total of nine decisions. In the first decision, the risky bag contains relatively few chips of the personal decision color. Therefore, a disclosure is relatively unlikely in the first choice. Going down the choice list, the number of chips of the personal decision color increases in the risky bag. The composition of the ambiguous bag is unknown throughout all choices and consequently does not change. Thus, subjects that want to avoid the disclosure of their test result should switch from the risky bag to the ambiguous bag at some point in the list as the probability of disclosure increases in the risky bag. At that switching point, subjects reveal the probability at which they are indifferent between the risky and the ambiguous option. This *probability equivalent* p_{eq} is given by the following equation (Kocher et al. 2018):

$$p_{eq} = \begin{cases} p_1 - \frac{1}{2}(p_2 - p_1) & \text{if } i = 0, \\ \frac{1}{2}(p_{i+1} + p_i) & \text{if } i \in \{1, 2, ..., 8\}, \\ p_9 + \frac{1}{2}(p_9 - p_8) & \text{if } i = 9, \end{cases}$$

where i is the row right before a subject switches, and $i + 1$ is the row where the other bag is chosen. If a subject chooses the ambiguous bag already in the first row, then $i = 0$, and if a subject never chooses the ambiguous urn, then $i = 9$. Thus, except for the corner cases, p_{eq} is calculated as the midpoint of the respective probabilities.

Based on the row where subjects switch between the bags in the choice list, subjects are categorized as being ambiguity neutral, ambiguity seeking or ambiguity averse. To this end, the ambiguity neutral probability p_n, i.e., the theoretical probability where an ambiguity-neutral decision maker would switch from the risky to the ambiguous choice, serves as the theoretical benchmark. This probability is given by $p_n = {}^1\!/_n$, where n is the maximum number of colors in both bags (Abdellaoui et al. 2011). Thus, in the high likelihood treatment with two colors $p_n = 50\%$ and in the low likelihood treatment with ten colors $p_n = 10\%$. In both treatments, the respective choice list displays the ambiguity-neutral choice roughly in the middle to avoid confounding due to cognitive biases (Kocher et al. 2018). For the high likelihood treatment, this is illustrated by the



Please make a choice between Bag A and Bag B in each row of the table below.
You have chosen **blue** as your personal decision color.

Bag A (100 chips in total)				**Bag B** (100 chips in total)	
Number of blue chips *(Disclosure of your test result)*	**Number of chips of other color** *(No disclosure of your test result)*	**Decision for Bag A**	**Decision for Bag B**	**Number of blue chips** *(Disclosure of your test result)*	**Number of chips of other color** *(No disclosure of your test result)*
25	75	●	○	unknown	unknown
30	70	●	○		
35	65	●	○		
40	60	●	○		
45	55	●	○		
50	50	○	●		
55	45	○	●		
60	40	○	●		
65	35	○	●		

Figure 1. Ellsberg choice task in the high likelihood treatment

two black arrows in Figure 1, which indicate the switching points that correspond to ambiguity neutrality of the respective decision maker. Subjects that already switch from the risky bag to the ambiguous bag for lower known probabilities, i.e., $p_{eq} < p_n$, are categorized as ambiguity seeking. In contrast, subjects that continue to choose the risky bag for higher known probabilities and switch only later to the ambiguous bag, i.e., $p_{eq} > p_n$, are categorized as ambiguity averse. This assumes that subjects perceive data disclosure as a loss. On the contrary, if subjects perceive data disclosure as a gain, the direction of switching between the ambiguous bag and the risky bag as well as the categorization scheme are simply reversed.

Experimental Procedures

Each experimental session proceeded according to the protocol illustrated in Figure 2 and described in the following. At the start of the experiment, subjects joined a Zoom meeting with anonymized names and had to give their consent to the privacy policy. Apart from the potential data disclosure, subjects entered their decisions in private and could not observe the actions of others. Before any information about the experiment was revealed, every participant independently chose their personal decision color from a fixed list of two or ten colors, depending on the treatment. This procedure is commonly used to prevent subjects from believing the experimenter might have manipulated the composition of the ambiguous bag to the detriment of subjects (Kocher et al. 2018). Next, participants were fully informed about the procedures of the experiment by the displayed experimental instructions that were also read aloud. Participants then had to complete ten comprehension questions on the experimental instructions and could only proceed if they answered each question correctly. Subjects then had to state whether they wanted to participate in the Ellsberg choice task, which would subject their test result to the possibility of disclosure in the experimental session. Subjects who agreed to participate in the choice task received a 20 EURO flat payment in return. Participants had to make this opt-in decision before they learned of their performance in the logic test in order to avoid self-selection. The payment was unconditional on whether a subject's test result was actually disclosed. In line with European data protection law, we, therefore, made sure that subjects could avoid the disclosure of their test result without having to leave the experiment altogether while still providing a strong incentive to participate in all tasks of the experiment. In addition, this consent-based procedure avoids confounding effects due to erratic behavior.

In the next stage, personal data was collected from participants. The collection of personal data in experiments faces the challenge that the data should be verifiable to avoid lying and should not bear the potential

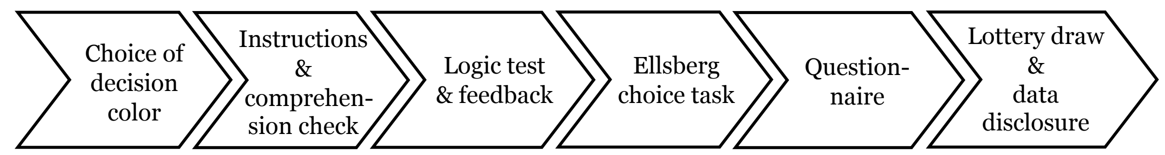


Figure 2. Experimental protocol

to harm participants in case of data disclosure (Feri et al. 2016). Following previous experiments (Fast and Schnurr 2020; Feri et al. 2016), subjects, therefore, performed a logic test, and we used the test result as personal data that was put under threat of disclosure to other participants. The test consisted of 16 questions from the ICAR-project (The International Cognitive Ability Resource Team 2014). Subjects had to answer each question in under one minute and received 30 CENT per correct answer. Immediately after taking the test, subjects received detailed private feedback on their performance, including the number of correctly answered questions and their rank relative to the other participants in the same session. Next, subjects completed the Ellsberg choice task, where they had to state their decisions for the list of choices between the risky and ambiguous options, as described above. This allows us to measure subjects' ambiguity attitudes.

After completing the Ellsberg choice task, subjects answered a questionnaire with a set of questions on their privacy attitudes and demographic characteristics. In particular, we asked subjects whether they perceived their logic test result as sensitive information by adapting the *information sensitivity*[1] scale (Dinev et al. 2013) to our context. Additionally, we asked subjects to which extent they found the disclosure of their test result desirable. To verify that our treatment manipulation was successful, we asked subjects to rate how likely they perceived the disclosure of their test result in the experiment on a seven-point Likert scale. Finally, participants reported basic demographic information such as gender and age.

In the last stage of the experiment, one of the participants was randomly selected by drawing a numbered ball from a lottery with the ids of all participants. For this participant, one of the nine decision rows from the Ellsberg choice task was determined by another draw from a second lottery. Both lottery draws were conducted by the experimenter during the experiment and were streamed by video to subjects via Zoom. For the selected participant, the determined decision was implemented, i.e., a chip was drawn from the bag that the subject had chosen in the respective decision row. If the subject had chosen the risky bag, the experimenter filled a bag with 100 chips according to the composition given by the determined decision row. The ambiguous bag was already prepared before the experimental session and was visible to subjects in the Zoom meeting during the whole session. If the chip drawn from the bag was of the participant's personal decision color, the participant had to disclose their test score together with their name and photo to all participants in the session. This was implemented by showing the respective test result screen in the Zoom meeting by the experimenter. To assure that participants could not use a fake name or photo, the selected subject had to verify their identity by presenting their student card to the experimenter.

Sample

The experiment was pre-registered (https://doi.org/10.1257/rct.8066-1.0) and approved by the Ethics Committee of the University of Passau as well as the German Association for Experimental Research. The privacy policy is fully compliant with the European GDPR and was approved by the data protection officer of the University of Passau. In all sessions, subjects were fully informed about the timeline of the experiment and the consequences of their actions. Moreover, a participant could exit the experiment at any time. Participants received a fixed participation fee of 5 EURO in addition to their variable payoff from the logic test and their participation in the Ellsberg choice task.

In total, 172 student subjects participated in the experiment. Twelve experimental sessions were conducted

[1] Items were measured on seven-point Likert scales (1 = "strongly disagree" and 7 = "strongly agree")

between August and September 2021 with 15 participants per session.[2] Subjects were recruited from the university's student pool PAULA via the ORSEE platform (Greiner 2015). Of the 172 subjects, 15 participants opted out of the Ellsberg choice task during the experiment to avoid the disclosure of their test result and are, therefore, omitted from the final sample. However, these 15 participants fully completed all other steps of the experiment and were present in case of a data disclosure. All participants passed the two attention checks. Twenty-two subjects switched between bags multiple times, which is a common phenomenon in experiments that use choice lists (Barham et al. 2014; Kocher et al. 2018). We can accommodate 13 of these 22 subjects by calculating the mid-point between the first and the last switching point, which has been suggested by previous studies (Kocher et al. 2018).[3]. The remaining nine subjects who switched multiple times, but started and ended their choices with the same bag, were excluded from the analysis because for their behavior, no midpoint and thus no probability equivalent can be determined.

This yields a final sample of 148 subjects, with 70 subjects in the low likelihood treatment and 78 subjects in the high likelihood treatment. The manipulation check confirms that our treatment manipulation was successful: Subjects in the high likelihood treatment perceived the disclosure of their test result as significantly more likely (mean = 3.5, s.d. = 1.35) than subjects in the low likelihood treatment (mean = 2.93, s.d. = 1.22) based on a two-sample t-test ($p < 0.01$).

Results

Across both treatments, we find that the majority of subjects ($n = 95$) choose the risky bag for low known probabilities and then switch to the ambiguous bag as known probabilities increase. This behavior is in line with expected rational behavior if subjects want to protect their test result from disclosure and is the common finding in experiments that investigate money losses (Trautmann and van de Kuilen 2015). The remaining share of subjects ($n = 53$) switches in the opposite direction: they first choose the ambiguous bag when known probabilities in the risky bag are low and then switch to the risky bag as known probabilities increase. This behavior is in line with expected rational behavior if subjects seek the disclosure of their test result and is the common finding in ambiguity experiments that investigate money gains. Therefore, we find two types of switching behavior in our sample. Consistent with the literature on ambiguity attitudes, we classify the respective behavior to either fall into the loss or gain domain and split the sample accordingly. This classification is supported by the following empirical observations and comparisons of group means based on two-sample t-tests: Subjects in the loss domain state a significantly lower desire for the disclosure of their test result ($p < 0.01$) and report a significantly higher perceived information sensitivity of the data ($p < 0.01$). Moreover, subjects in the loss domain performed significantly worse in the logic test ($p < 0.1$), which suggests that they attributed a higher value to the protection of their test score (see also Fast and Schnurr 2020) and were, thus, more likely to switch as if to prevent the disclosure of their test score.

Table 1 reports descriptive statistics of probability equivalents, p_{eq}, for the loss and gain domain as well as for the low and high likelihood treatment, respectively. For subjects who perceive data disclosure as a loss, the mean probability equivalent in the low likelihood treatment, $p_{eq} = 0.138$, exceeds the ambiguity neutral probability of $p_n = 0.1$. This indicates ambiguity aversion, as, on average, these subjects chose the risky bag over the ambiguous bag even after the ambiguity neutral choice. For high likelihood losses, the mean probability equivalent, $p_{eq} = 0.484$ is lower than the ambiguity neutral probability of $p_n = 0.5$. Thus, these subjects tend to be ambiguity seeking, as they switch from the risky to the ambiguous bag already before the ambiguity neutral choice.

For subjects who perceive data disclosure as a gain, the mean probability equivalent in the low likelihood treatment, $p_{eq} = 0.106$, is slightly higher than $p_n = 0.1$, which is indicative of ambiguity neutrality or ambiguity seeking, on average. Note that in the gain domain $p_{eq} > p_n$ indicates ambiguity seeking since subjects switch from the ambiguous bag to the risky bag, i.e., in the opposite direction than in the loss domain. For high likelihood gains, the mean probability equivalent, $p_{eq} = 0.428$, is lower than the ambiguity neutral probability of $p_n = 0.5$ which suggests ambiguity aversion.

[2] Seven subjects dropped out during sessions, and one session had to be run with only 14 participants due to a high number of no-shows.

[3] To corroborate the robustness of our results we replicated the analysis below with a reduced sample that excluded all subjects who switched multiple times. All of our main results continue to hold qualitatively, while quantitative effects remain similar in size.

	Treatment	n	Mean(p_{eq})	SD(p_{eq})	Ambiguity Averse	Ambiguity Neutral	Ambiguity Seeking
Loss Domain	Low ($p_n = 0.1$)	42	0.138	0.032	55%	45%	0%
	High ($p_n = 0.5$)	53	0.484	0.054	10%	60%	30%
Gain Domain	Low ($p_n = 0.1$)	28	0.106	0.040	7%	61%	32%
	High ($p_n = 0.5$)	25	0.428	0.072	56%	44%	0%

Table 1. Probability equivalents and ambiguity attitudes across gain and loss domains as well as treatments

Ambiguity Attitudes and Transparency Preferences

Whereas descriptive mean probability equivalents provide some indication of the average ambiguity attitudes under different conditions, they do not fully capture the heterogeneity of ambiguity attitudes across subjects. Therefore, the following analysis is based on the classification of ambiguity attitudes on the individual level, i.e., each subject is assigned one of the three ambiguity attitudes (ambiguity aversion, ambiguity neutrality, ambiguity seeking) depending on the probability equivalent derived from their individual switching point (see Kocher et al. (2018) for a similar approach). Based on these individual classifications, Table 1 reports the shares for each of the three ambiguity attitudes across treatments and the loss or gain domain as perceived by subjects (see also Figure 3).

Across treatments, the share of ambiguity neutral subjects is relatively stable and ranges from 44% to 61%. In contrast, the share of ambiguity seeking and ambiguity averse subjects differs substantially between low and high likelihood treatments, as illustrated in Figure 3. For perceived losses, a large share of subjects is ambiguity averse in the low likelihood treatment, while no subject is found to be ambiguity seeking under these conditions. The difference in shares between ambiguity averse and ambiguity seeking subjects for low likelihood losses is confirmed to be statistically significant by a binomial test ($p < 0.01$). These findings are consistent with Hypothesis 1(a). For perceived gains, similar results are obtained for the high likelihood treatment. As indicated in Figure 3, we do not find any ambiguity seeking subjects under these conditions, while there is a substantial share of subjects who exhibit ambiguity aversion. Again, this difference is found to be statistically significant by a binomial test ($p < 0.01$), which supports Hypothesis 1(b).

Result 1 (Preference for transparency) *Ambiguity aversion significantly exceeds ambiguity seeking a) when data disclosure is perceived as a loss and the likelihood of disclosure is low and b) when data disclosure is perceived as a gain and the likelihood of disclosure is high. Therefore, under these conditions, a significant share of subjects has a preference for transparency that provides them with information about privacy risks.*

Next, we consider treatment differences, i.e., whether and how ambiguity attitudes change for different likelihoods of a data disclosure, and investigate under which conditions ambiguity seeking may exceed ambiguity aversion. Overall, chi-squared tests confirm significant treatment changes in the distributions of ambiguity attitudes for both the loss domain ($\chi^2(2, N = 95) = 30.0, p < 0.01$) and the gain domain ($\chi^2(2, N = 53) = 19.2, p < 0.01$).

For perceived losses, the share of ambiguity averse subjects decreases significantly when moving from low likelihood losses to high likelihood losses ($\chi^2(1, N = 95) = 21.0, p < 0.01$), as indicated by the left panel of Figure 3. On the contrary, there is a significant increase in the share of ambiguity seeking subjects for high likelihood losses compared to low likelihood losses ($\chi^2(1, N = 95) = 13.2, p < 0.01$). At the same time, there are no significant treatment differences in the shares of ambiguity neutral subjects for perceived losses ($\chi^2(1, N = 95) = 1.6, p = 0.21$). As a result, for high likelihood losses, we find that more than 30% of subjects are ambiguity seeking, and only 9% are ambiguity averse. This difference is statistically significant based on a binomial test ($p < 0.05$). Therefore, in line with Hypothesis 2(a), we find that ambiguity seeking significantly exceeds ambiguity aversion for high likelihood losses.

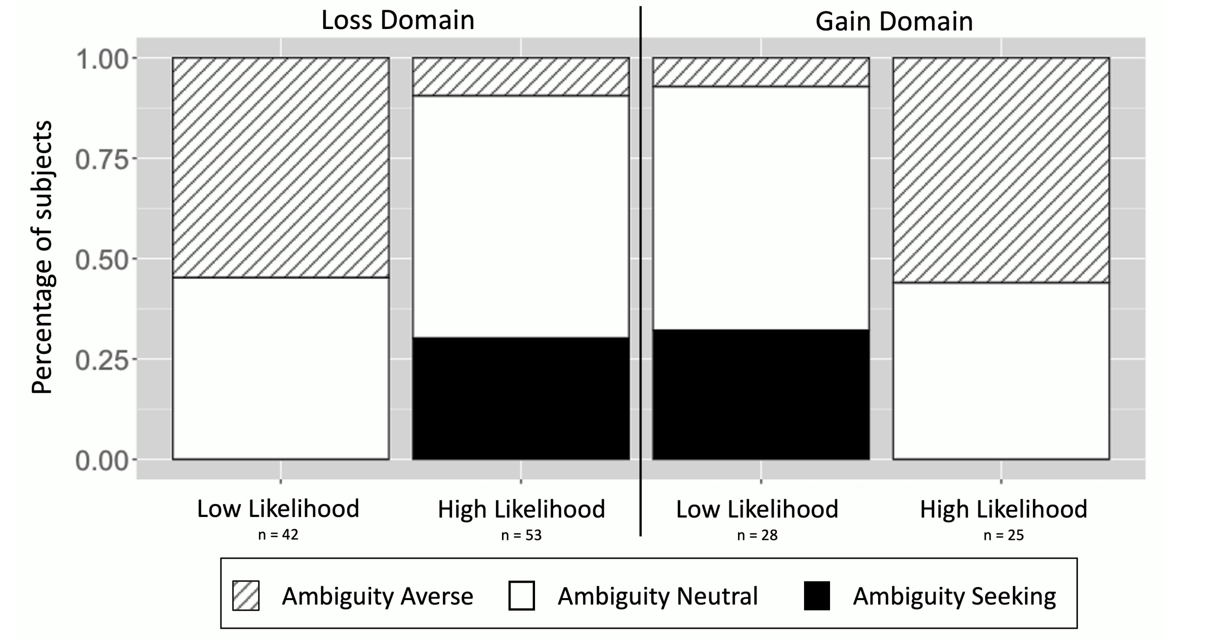


Figure 3. Relative frequencies of ambiguity attitudes across gain and loss domains as well as treatments

For perceived gains, we find the opposite effects and reverse outcomes, which are visualized by the mirror image in Figure 3. In particular, there is a significant increase in the share of ambiguity seeking subjects when moving from the high likelihood treatment to the low likelihood treatment ($\chi^2(1, N = 53) = 7.5, p < 0.01$), as illustrated by the right panel of Figure 3. Conversely, the share of ambiguity averse subjects falls significantly as the likelihood of data disclosure decreases ($\chi^2(1, N = 53) = 12.7, p < 0.01$). The share of ambiguity neutral subjects is again not statistically significant for the different disclosure likelihoods ($\chi^2(1, N = 53) = 0.9, p = 0.35$). As a result, for low likelihood gains, we find that 32% of subjects are ambiguity seeking, whereas only 7% are ambiguity averse. This difference in shares is statistically significant, as confirmed by a binomial test ($p < 0.1$). Thus, we find that for low likelihood gains, subjects exhibit a preference for ambiguity over increased transparency of privacy risks, which supports Hypothesis 2(b).

Result 2 (Preference for ambiguity) *Ambiguity seeking significantly exceeds ambiguity aversion a) when data disclosure is perceived as a loss and the likelihood of disclosure is high and b) when data disclosure is perceived as a gain and the likelihood of disclosure is low. Therefore, under these conditions, a significant share of subjects has a preference for ambiguity where privacy risks are not transparent.*

Robustness checks: Note that for some cases, the chi-squared distribution may be an inadequate approximation of the sampling distribution due to low frequencies. Therefore, we also replicate the above analysis of treatment differences by conducting Fisher's exact tests, which corroborate the robustness of our findings for the loss domain ($p < 0.01$) and for the gain domain ($p < 0.01$). Moreover, we perform Fisher's exact tests for each of the individual treatment comparisons of each ambiguity attitude. These tests again confirm the findings from the partitioned chi-squared tests and specifically the significant differences between ambiguity seeking and ambiguity aversion ($p < 0.01$).

Discussion

Our empirical findings demonstrate that a significant share of people exhibits ambiguity attitudes that diverge from the theoretical prediction and the general assumption of ambiguity neutrality when making decisions about uncertain privacy outcomes. Moreover, whereas the share of ambiguity neutral decision makers remains relatively stable over our different experimental conditions at about 50% of the total population, we observe significant effects of these conditions on the share of ambiguity seeking and ambiguity averse subjects. In particular, for low likelihood privacy losses and for high likelihood privacy gains, most individuals are ambiguity averse, i.e., they prefer information about probabilities of privacy risks over ambiguity. This changes significantly as the likelihood of privacy losses increases or as the likelihood of privacy gains decreases: In these cases, ambiguity seeking among subjects exceeds ambiguity aversion, i.e., more people prefer to avoid transparency about privacy risks and choose ambiguity. In particular, for a high likelihood loss, more than 30% of subjects choose ambiguity, thus foregoing the option that would provide them with explicit information about the probability of present privacy risks.

Thus, in line with previous empirical findings on monetary outcomes (Kocher et al. 2018; Trautmann and van de Kuilen 2015), we observe a reversal of ambiguity attitudes for high and low likelihood data disclosures as well as for perceived privacy losses and privacy gains. Moreover, our findings are consistent with hope and fear effects as a common interpretation of this fourfold pattern of ambiguity attitudes (Viscusi and Chesson 1999). Thus, people rather fear ambiguity when known risks entail a loss with a relatively small probability or ensure a gain with a relatively high probability. However, when known risks predict a loss with high probability or a gain with small probability, people rather embrace ambiguity in the hope of better chances for the desired outcome. Notwithstanding, about half of the subjects follow the theoretical prediction of an ambiguity neutral decision maker. Hence, these people switch to ambiguity when it is reasonable to believe that the risk of a privacy loss is lower for unknown probabilities or vice versa when the likelihood of a privacy gain is higher (Abdellaoui et al. 2011).

Theoretical Implications

From a theoretical point of view, our research highlights that ambiguity attitudes, which have been predominantly investigated for monetary outcomes so far, play an important role in the context of uncertain privacy outcomes. Moreover, we observe the same fourfold pattern for an uncertain disclosure of personal data as previously found for monetary outcomes (Kocher et al. 2018; Trautmann and van de Kuilen 2015). This is remarkable and was a priori uncertain as personal data is substantially different from money, especially due to its non-rivalrous nature and its highly heterogeneous valuations across people (Fast and Schnurr 2020; Schudy and Utikal 2017). A notable difference with respect to our findings in the privacy context is that the loss and gain domain emerge endogenously. In contrast, money has an objective value and a natural benchmark that determines losses and gains exogenously. The endogeneity of loss and gain domains is a direct consequence of the heterogeneity in privacy preferences which is particularly pronounced for our specific type of personal data but is also widespread for other contexts with privacy implications, as demonstrated by the literature on individuals' data valuations (Benndorf and Normann 2018; Collis et al. 2021).

Our findings contribute novel insights to the literature on transparency in privacy contexts. Whereas the existing literature has mainly focused on the effects of exposing individuals to transparency, we investigate people's revealed preferences when faced with a choice between more and less uncertainty about an actual data disclosure. Our experimental findings indicate that about half of the subjects follow the theoretical prediction given by an ambiguity neutral decision maker when faced with a transparency choice in privacy contexts. However, the remaining subjects diverge significantly from this prediction. In particular, when the likelihood of a privacy loss is low, they tend to prefer more transparent options that reveal the probabilities for a privacy risk, although the ambiguous option may offer a better chance to avoid the privacy loss.

However, when the likelihood of a privacy loss is high, a significant share of about 30% subjects chooses the ambiguous option over the transparent option, although the latter may give precise information about the probability of a privacy risk and offer a better chance to avoid a privacy loss. Therefore, people may avoid transparency about privacy risks precisely in those cases where they would most likely benefit from it due to the high likelihood of a privacy loss. Therefore, we provide further evidence that transparency can sometimes backfire (Brough et al. 2022; Kim et al. 2019). Moreover, our findings suggest that independent of other considerations like differences in prices or features (Johnson et al. 2020), consumers may have an inherent preference for or against transparency about privacy risks depending on how likely they consider a privacy loss. Finally, our findings suggest ambiguity attitudes as a novel behavioral mechanism that may affect individuals' transparency choices in privacy contexts across a large range of application scenarios.

To this end, our experiment was designed to isolate ambiguity attitudes in a highly controlled and abstract decision scenario with actual privacy risks. This provides a starting point for future empirical studies that may test the external validity of these findings and the relevance of ambiguity attitudes in more context-specific applications, which involve additional influencing factors on individuals' transparency decisions.

Managerial and Policy Implications

Our findings also offer important implications for managers, consumers, and regulators. From the perspective of a firm, our results suggest that providing transparency about privacy risks can be an effective strategy to attract consumers when the general likelihood of privacy risks in a market or industry is perceived to be low by consumers. However, when the general likelihood of privacy risks is perceived to be high, a significant share of consumers is willing to avoid transparency and to prefer the ambiguity of less transparent competitors. This also has important ramifications for policymakers that aim for more transparency about privacy risks in digital markets. Most notably, our findings suggest that regulators should be cautious about relying exclusively on voluntary transparency adoption by firms. In particular, firms may lack the incentive to provide information about privacy risks to consumers when consumers actually prefer ambiguity about these risks. In this vein, our findings present a dilemma for regulators as consumers' preference for ambiguity is particularly pronounced in situations where the likelihood of undesired data disclosures is high. Therefore, for such market conditions, more rigorous interventions may be warranted. For example, instead of relying on the voluntary adoption of IoT product labels (cf. European Commission 2016; Executive Order 14028 2021), such labels may become obligatory for devices and industries where privacy losses are highly likely and associated with significant harm to consumers. From a consumer protection perspective, people should be made aware that their ambiguity attitudes might lead them to make suboptimal privacy choices. That is especially the case when ambiguity aversion or ambiguity seeking preferences lead them to choose products that involve greater privacy risks than potential alternatives.

Conclusion

In a randomized controlled online experiment, we find that most individuals avoid ambiguity and prefer transparency for low likelihood privacy losses. However, this pattern reverses for high likelihood losses as well as when subjects perceive data disclosure as a gain. Thus, people facing high privacy risks may seek ambiguity and avoid transparency. This finding suggests that initiatives that aim to improve transparency about privacy risk by means of purely voluntary measures are prone to adverse effects: For products associated with high privacy risks, a significant share of consumers may choose to avoid more transparent products due to ambiguity seeking. This would call for mandatory transparency policies, as, for example, in the case of privacy labels for IoT devices. With respect to theoretical implications, our results demonstrate that ambiguity attitudes of subjects also extend to privacy contexts and influence subjects' decisions with respect to their personal data. In particular, our elicitation of subjects' revealed preferences suggests that ambiguity attitudes are an important mechanism that influences individuals' transparency choices. Finally, this underscores the value of applying behavioral economics approaches and theory to privacy research contexts (Arnott and Gao 2022; Dinev et al. 2015; Goes 2013).

With respect to the limitations of our study, we acknowledge that our findings are based on a student sample that is not representative of the German population. Furthermore, we employed a between-subjects treatment design, i.e., each subject participated only in exactly one of the treatments. This design choice ensures that treatment effects are not confounded by learning effects or reference dependence, thus ruling out alternative explanations for our experimental findings. However, we cannot directly measure treatment effects within-subjects and can thus not investigate how behavior changes for a specific individual across treatments. Moreover, with respect to the experimental design, we intentionally created a generic decision context to eliminate confounding factors such as transaction costs or presentation-specific biases. This design decision inherently limits external validity for specific decision contexts in practice, where many other factors may interact with the isolated transparency preferences that we have identified in this study. Thus also the likelihoods for privacy-related outcomes (i.e., 50% and 10%) considered in this study may not be immediately comparable to decision situations in the field. However, what ultimately matters is the qualitative causal effect that we have identified for different likelihoods of data disclosures. These limitations may be addressed by future research. For example, in a follow-up survey study, we aim to corroborate our findings on transparency preferences due to ambiguity attitudes by eliciting consumer choices for IoT devices that offer more and less transparency about privacy risks. Finally, future research could test how ambiguity attitudes interact with other factors that have been shown to affect individuals' transparency decisions, such as control and trust.

Acknowledgments

This project is funded by the Bavarian State Ministry of Science and the Arts and coordinated by the Bavarian Research Institute for Digital Transformation (bidt). The authors are grateful to Victoria Fast for her contributions at an early stage of this project.

References

Abdellaoui, M., Baillon, A., Placido, L., and Wakker, P. P. 2011. "The Rich Domain of Uncertainty: Source Functions and Their Experimental Implementation," *American Economic Review* (101:2), pp. 695–723.

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), pp. 509–514.

Adjerid, I., Acquisti, A., Brandimarte, L., and Loewenstein, G. 2013. "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency," in *Proceedings of the Ninth Symposium on Usable Privacy and Security,* L. Bauer, K. Beznosov, and L. F. Cranor (eds.). Newcastle, UK, pp. 1–11.

Adjerid, I., Acquisti, A., and Loewenstein, G. 2019. "Choice Architecture, Framing, and Cascaded Privacy Choices," *Management Science* (65:5), pp. 2267–2290.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., and Wetzels, M. 2015. "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness," *Journal of Retailing* (91:1), pp. 34–49.

Arnott, D. and Gao, S. 2022. "Behavioral Economics in Information Systems Research: Critical Analysis and Research Strategies," *Journal of Information Technology* (37:1), pp. 80–117.

Awad, N. F. and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13–28.

Bansal, G., Zahedi, F., and Gefen, D. 2015. "The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern," *European Journal of Information Systems* (24:6), pp. 624–644.

Barham, B. L., Chavas, J.-P., Fitz, D., Salas, V. R., and Schechter, L. 2014. "The Roles of Risk and Ambiguity in Technology Adoption," *Journal of Economic Behavior & Organization* (97), pp. 204–218.

Benndorf, V. and Normann, H.-T. 2018. "The Willingness to Sell Personal Data," *The Scandinavian Journal of Economics* (120:4), pp. 1260–1278.

Betzing, J. H., Tietz, M., vom Brocke, J., and Becker, J. 2020. "The Impact of Transparency on Mobile Privacy Decision Making," *Electronic Markets* (30:3), pp. 607–625.

BEUC 2017. *Securing Consumer Trust in the Internet of Things: Principles and Recommendations*. Retrieved May 02, 2022, from https://bit.ly/3vWj9Ia.

Bianchi, M. and Tallon, J.-M. 2019. "Ambiguity Preferences and Portfolio Choices: Evidence From the Field," *Management Science* (65:4), pp. 1486–1501.

Blythe, J. M., Sombatruang, N., and Johnson, S. D. 2019. "What Security Features and Crime Prevention Advice is Communicated in Consumer IoT Device Manuals and Support Pages?," *Journal of Cybersecurity* (5:1), Article 5.

Brough, A. R., Norton, D. A., Sciarappa, S. L., and John, L. K. 2022. "The Bulletproof Glass Effect: Unintended Consequences of Privacy Notices." *Journal of Marketing Research* (Advance online publication).

Collis, A., Moehring, A., Sen, A., and Acquisti, A. 2021. "Information Frictions and Heterogeneity in Valuations of Personal Data," Working Paper. Retrieved from https://ssrn.com/abstract=3974826.

Dimmock, S. G., Kouwenberg, R., Mitchell, O. S., and Peijnenburg, K. 2016a. "Ambiguity Aversion and Household Portfolio Choice Puzzles," *Journal of Financial Economics* (119:3), pp. 559–577.

Dimmock, S. G., Kouwenberg, R., and Wakker, P. P. 2016b. “Ambiguity Attitudes in a Large Representative Sample,” *Management Science* (62:5), pp. 1363–1380.

Dinev, T., McConnell, A. R., and Smith, H. J. 2015. “Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box,” *Information Systems Research* (26:4), pp. 639–655.

Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. “Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts,” *European Journal of Information Systems* (22:3), pp. 295–316.

Ellsberg, D. 1961. “Risk, Ambiguity, and the Savage Axioms,” *The Quarterly Journal of Economics* (75:4), pp. 643–669.

Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., and Cranor, L. F. 2021. “Which Privacy and Security Attributes Most Impact Consumers’ Risk Perception and Willingness to Purchase IoT Devices?,” in *2021 IEEE Symposium on Security and Privacy (SP),* IEEE, pp. 519–536.

European Commission 2016. *Advancing the Internet of Things in Europe [Staff Working Document]*. Retrieved May 02, 2022, from https://bit.ly/3w1MCAv.

Executive Order 14028 2021. *Measuring and Managing the Cyber Risks to Business Operations*. Retrieved May 02, 2022, from https://bit.ly/3vBnSA6.

Fast, V. and Schnurr, D. 2020. “The Value of Personal Data: An Experimental Analysis of Data Types and Personal Antecedents,” in *Proceedings of the 41st International Conference on Information Systems,* Hyderabad, India.

Feri, F., Giannetti, C., and Jentzsch, N. 2016. “Disclosure of Personal Information under Risk of Privacy Shocks,” *Journal of Economic Behavior & Organization* (123), pp. 138–148.

Goes, P. B. 2013. “Editor’s Comments: Information Systems Research and Behavioral Economics,” *MIS Quarterly* (37:3), pp. iii–viii.

Greiner, B. 2015. “Subject Pool Recruitment Procedures: Organizing Experiments With ORSEE,” *Journal of the Economic Science Association* (1:1), pp. 114–125.

Gupta, A., Kannan, K., and Sanyal, P. 2018. “Economic Experiments in Information Systems,” *MIS Quarterly* (42:2), pp. 595–606.

Hulland, J. and Houston, M. 2021. “The Importance of Behavioral Outcomes,” *Journal of the Academy of Marketing Science* (49) 3 2021, pp. 437–440.

Identity Theft Resource Center 2021. *Data Breach Report: 2020 in Review*. Retrieved May 02, 2022, from https://notified.idtheftcenter.org/s/2020-data-breach-report.

Johnson, S. D., Blythe, J. M., Manning, M., and Wong, G. T. W. 2020. “The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay,” *PlOS ONE* (15:1), e0227800.

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

Kim, T., Barasz, K., and John, L. K. 2019. “Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness,” *Journal of Consumer Research* (45:5), pp. 906–932.

Kocher, M. G., Lahno, A. M., and Trautmann, S. T. 2018. “Ambiguity Aversion is Not Universal,” *European Economic Review* (101), pp. 268–283.

Kokolakis, S. 2017. “Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon,” *Computers & security* (64), pp. 122–134.

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

Lin, T. 2021. “Valuing Intrinsic and Instrumental Preferences for Privacy,” Working Paper. Retrieved from https://ssrn.com/abstract=3406412.

Liu, C., Marchewka, J. T., Lu, J., and Yu, C.-S. 2005. “Beyond Concern: A Privacy-Trust-Behavioral Intention Model of Electronic Commerce,” *Information & Management* (42:2), pp. 289–304.

Lowry, P. B., Dinev, T., and Willison, R. 2017. “Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda,” *European Journal of Information Systems* (26:6), pp. 546–563.

Marreiros, H., Tonin, M., Vlassopoulos, M., and Schraefel, M. 2017. ""Now That You Mention It": A Survey Experiment on Information, Inattention and Online Privacy," *Journal of Economic Behavior & Organization* (140), pp. 1–17.

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

Morwitz, V. G. and Munz, K. P. 2021. "Intentions," *Consumer Psychology Review* (4:1), pp. 26–41.

Muthukrishnan, A. V., Wathieu, L., and Xu, A. J. 2009. "Ambiguity Aversion and the Preference for Established Brands," *Management Science* (55:12), pp. 1933–1941.

Al-Natour, S., Cavusoglu, H., Benbasat, I., and Aleem, U. 2020. "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps," *Information Systems Research* (31:4), pp. 1037–1063.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of consumer affairs* (41:1), pp. 100–126.

Obar, J. A. and Oeldorf-Hirsch, A. 2020. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services," *Information, Communication & Society* (23:1), pp. 128–147.

Perlroth, N. 2017. *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*. *The New York Times*. Retrieved May 02, 2022, from https://nyti.ms/3y7NHJP.

Peters, J. 2021. *Personal Data of 533 Million Facebook Users Leaks Online*. *The Verge*. Retrieved May 02, 2022, from https://bit.ly/3ybWxGv.

Schudy, S. and Utikal, V. 2017. "'You Must Not Know About Me'–On the Willingness to Share Personal Data," *Journal of Economic Behavior & Organization* (141), pp. 1–13.

Sheeran, P. and Webb, T. L. 2016. "The Intention–Behavior Gap," *Social and Personality Psychology Compass* (10:9), pp. 503–518.

Sleziona, P. and Widjaja, T. 2022. "Transparency in the Privacy Context: A Structured Literature Review," in *Proceedings of the European Conference on Information Systems,* Timisoara, Romania.

Sutter, M., Kocher, M. G., Glätzle-Rützler, D., and Trautmann, S. T. 2013. "Impatience and Uncertainty: Experimental Decisions Predict Adolescents' Field Behavior," *American Economic Review* (103:1), pp. 510–531.

The Harris Poll 2020. *2019 Cyber Safety Insights Report Global Results*. Retrieved May 02, 2022, from https://bit.ly/37f22Jm.

The International Cognitive Ability Resource Team 2014. *International Cognitive Ability Resource*. Retrieved May 02, 2022, from https://icar-project.com/.

Trautmann, S. T. and van de Kuilen, G. 2015. "Ambiguity Attitudes," in *The Wiley Blackwell Handbook of Judgment and Decision Making, I,* G. Keren and G. Wu (eds.). Chichester, UK: Wiley Blackwell, pp. 89–116.

Trautmann, S. T., Vieider, F. M., and Wakker, P. P. 2008. "Causes of Ambiguity Aversion: Known Versus Unknown Preferences," *Journal of Risk and Uncertainty* (36:3), pp. 225–243.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254–268.

Tucker, C. E. 2012. "The Economics of Advertising and Privacy," *International Journal of Industrial Organization* (30:3), pp. 326–329.

Viscusi, W. K. and Chesson, H. 1999. "Hopes and Fears: The Conflicting Effects of Risk Ambiguity," *Theory and Decision* (47:2), pp. 157–184.

Wang, P. A. and Nyshadham, E. 2011. "Knowledge of Online Security Risks and Consumer Decision Making: An Experimental Study," in *44th Hawaii International Conference on System Sciences,* Kauai, HI, USA, pp. 1–10.

Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., and Grover, V. 2010. "Knowing Your Customers: Using a Reciprocal Relationship to Enhance Voluntary Information Disclosure," *Decision Support Systems* (48:2), pp. 395–406.