A measure of the implicit value of privacy under risk

Alisa Frik
International Computer Science Institute, Berkeley, California, USA and Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, California, USA, and
Alexia Gaudeul
Faculty of Economic Sciences, Georg-August-Universitat Gottingen, Gottingen, Germany

Abstract

Purpose – Many online transactions and digital services depend on consumers' willingness to take privacy risks, such as when shopping online, joining social networks, using online banking or interacting with e-health platforms. Their decisions depend on not only how much they would suffer if their data were revealed but also how uncomfortable they feel about taking such a risk. Such an aversion to risk is a neglected factor when evaluating the value of privacy. The aim of this paper is to propose an empirical method to measure both privacy risk aversion and privacy worth and how those affect privacy decisions.

Design/methodology/approach – The authors let individuals play privacy lotteries and derive a measure of the value of privacy under risk (VPR) and empirically test the validity of this measure in a laboratory experiment with 148 participants. Individuals were asked to make a series of incentivized decisions on whether to incur the risk of revealing private information to other participants.

Findings – The results confirm that the willingness to incur a privacy risk is driven by a complex array of factors, including risk aversion, self-reported value for private information and general attitudes to privacy (derived from surveys). The VPR does not depend on whether there is a preexisting threat to privacy. The authors find qualified support for the existence of an order effect, whereby presenting financial choices prior to privacy ones leads to less concern for privacy.

Practical implications – Attitude to risk in the domain of privacy decisions is largely understudied. In this paper, the authors take a first step toward closing this empirical and methodological gap by offering (and validating) a method for the incentivized elicitation of the implicit VPR and proposing a robust and meaningful monetary measure of the level of aversion to privacy risks. This measure is a crucial step in designing and implementing the practical strategies for evaluating privacy as a competitive advantage and designing markets for privacy risk regulations (e.g. through cyber insurances).

Social implications – The present study advances research on the economics of consumer privacy – one of the most controversial topics in the digital age. In light of the proliferation of privacy regulations, the mentioned method for measuring the VPR provides an important instrument for policymakers' informed decisions regarding what tradeoffs consumers consider beneficial and fair and where to draw the line for violations of consumers' expectations, preferences and welfare.

Originality/value – The authors present a novel method to measure the VPR that takes account of both the value of private information to consumers and their tolerance for privacy risks. The authors explain how this method can be used more generally to elicit attitudes to a wide range of privacy risks involving exposure of various types of private information.

Keywords Privacy attitudes, Personal information, Disclosure, Risk, Control, Laboratory experiment

Paper type Research paper

1. Introduction

Online services (including information search, e-commerce, e-banking, online marketing and social media) rely heavily on the collection, use and exchange of consumers' personal information. This opens many new business opportunities but poses substantial risks to privacy, such as private information disclosure, price discrimination, identity theft, stalking and bullying.

When making privacy decisions, individuals weigh such costs with benefits, such as service provision, convenience or discounts. Companies also weigh clients' privacy protection with the loss of opportunities and revenue if they limit their use of consumer data. Balancing those concerns is a major issue for

The current issue and full text archive of this journal is available on Emerald Insight at: **https://www.emerald.com/insight/0736-3761.htm**

Journal of Consumer Marketing
© Emerald Publishing Limited [ISSN 0736-3761]
[DOI 10.1108/JCM-06-2019-3286]

JEL classification – C91,D81,O30
The authors thank Marco Tecilla for technical assistance, as well as Alessandro Acquisti, Caterina Giannetti, Alex Imas, Luigi Mittone, Matteo Ploner, Michele Vescovi and other colleagues and faculty members for valuable comments and feedback that helped the authors to improve the manuscript. The study was carried out while Alisa Frik was doing her PhD at the School of Social Sciences of the Università degli Studi di Trento, in collaboration with SKIL Joint Open Lab (Trento, Italy). No potential conflict of interest was reported by the authors. Funding for the doctoral scholarship of Alisa Frik was supported by a fellowship from TIM – Telecom Italia. Opinions, findings and conclusions are those of the authors and do not necessarily reflect the views of the funders.

Received 20 June 2019
Revised 23 November 2019
24 January 2020
Accepted 21 February 2020

companies and consumer protection agencies (Culnan and Bies, 2003; Bennett and Raab, 2006).

Numerous empirical studies have attempted to measure the value of personal information (Grossklags and Acquisti, 2007; Tsai *et al.*, 2011; Beresford *et al.*, 2012). However, existing measures do not consider situations where personal information is revealed only with some probability, rather than with certainty. Measures of aversion to risk in the privacy domain are, therefore, largely lacking.

This is a problem because individual privacy decisions depend on not only the value of the personal information itself but also individual risk tolerance. Although a person may have low valuation for their data, they may be very uncomfortable about not knowing what will happen to it. Conversely, a person may value privacy but may also be comfortable with uncertainty.

We, therefore, propose a new, incentivized method for the elicitation of the implicit value of privacy under risk (VPR). The VPR takes account of both the worth of privacy and the level of tolerance for privacy risks. It indicates how much people are ready to pay to protect themselves from privacy threats. Our measure has several advantages over existing measures. First, it is incentivized, thus relevant in economic environments. Second, it is implicit, as we infer the intuitive VPR from behavior, instead of self-reported explicit values. Third, it considers the value of not only keeping personal data private but also risk aversion; both are crucial when making privacy decisions, as privacy exposure follows a stochastic (random) process.

We validate our method in a laboratory experiment with 148 participants and correlate our measure with established measures of attitudes to privacy and risk. We find that participants' behavior is consistent with their level of risk aversion, expressed privacy concerns, willingness to pay to protect their information from disclosure and willingness to accept payments to disclose their information. Our measure is robust to the realistic scenario of a preexisting and unavoidable risk of personal information disclosure. We discuss the implications of our measure for policymakers and outline how to apply it for decision scenarios involving various types of privacy risks.

2. Related work

In this section, we review privacy considerations in marketing and existing measures of privacy attitudes and explain how and why our measurement methodology differs from those.

2.1 The role of privacy concerns in marketing

Research in marketing shows that privacy concerns induce consumers to limit their activity on the internet (Arnott *et al.*, 2007; Fang *et al.*, 2017), reduce their intentions to purchase online (Dinev and Hart, 2006; George, 2004; Goldfarb and Tucker, 2011), undermine consumers' trust in online vendors (Camp, 2003), lower willingness to buy from them (Bart *et al.*, 2005; Schlosser *et al.*, 2006) and decrease trust and click-through rates (Bleier and Eisenbeiss, 2015; Tucker, 2014).

However, consumers' behavior sometimes contradicts their expressed privacy concerns (Point 1), and consumers also derive advantages in exchange for their loss of privacy (Point 2). Furthermore, firms can alleviate consumer concerns by fostering trust, increasing perceived control and promoting transparency in the use of data (Point 3).

Regarding Point 1, doubts have been raised about the validity of privacy concerns, as consumers are often unwilling to pay for online privacy protection (Shostack, 2003) or to give up on discounts for personal data (Spiekerman *et al.*, 2001). This "privacy paradox" may be related to the endowment effect (Kahneman *et al.*, 1991), whereby willingness to pay (WTP) for a good is lower than willingness to accept (WTA) payments for that same good (Knetsch and Sinden, 1984). That may explain why consumers are not ready to pay for privacy protection while being unwilling to relinquish privacy. Furthermore, Tsai *et al.* (2011) show that consumers are willing to pay a premium for the products from websites with added privacy protection. Other research in marketing demonstrates a positive effect of transparency and control on trust (and, subsequently, economic intentions), as those mitigate privacy concerns (Milne and Culnan, 2004; Martin, 2015).

Regarding Point 2, consumers derive benefits (e.g. through personalized offers, direct compensations, lower prices and free services) that can outweigh and compensate for privacy concerns according to the justice theory (Ashworth and Free, 2006; Culnan and Bies, 2003), the social contract theory (Martin, 2015; Phelps *et al.*, 2000) and the social exchange theory (Lwin *et al.*, 2007). Chellappa and Sin (2005), Hann *et al.* (2007) and Gabisch and Milne (2014) give related empirical evidence. This may however be largely driven by the wish to reciprocate free services rather than by derived benefits (Schumann *et al.*, 2014)[1].

Regarding Point 3, fair information practices, transparency and control can mitigate reactance, according to the justice theory and the reactance theory (Bleier and Eisenbeiss, 2015; Tucker, 2014; White *et al.*, 2008). However, marketers need to respect ethical considerations in relation to personal data practices, regardless of economic outcomes (Ferrell and Gresham, 1985; Lwin *et al.*, 2007). Inducing consumers' trust, but then failing to be accountable for it, or violating it with unfair information practices, is unethical. Increasing perceived control to lull consumers' vigilance may also lead to outcomes contrary to their preferences due to the "control paradox" (Brandimarte *et al.*, 2012).

Given the abovementioned, privacy concerns continue to matter for consumers and require fair compensation and mitigation. Policymakers and companies need methods to measure different aspects of privacy attitudes to make informed decisions about how to fulfill consumers' expectations and preferences, promote welfare and design and implement privacy regulations. Scholars and practitioners also need measures of privacy values to advance the economic analysis of privacy.

2.2 The existing measures of privacy attitudes

Individual privacy attitudes have been measured with surveys and experiments. Some surveys examine attitudes and responses to hypothetical scenarios that involve privacy concerns – e.g. Westin's Privacy Index (Westin, 1968) and Internet Users' Information Privacy Concerns (Malhotra *et al.*, 2004). Other surveys directly ask participants for their WTA or

WTP to avoid revealing private information. Experiments elicit privacy preferences based on individual behaviors. For example, they offer participants a choice of purchasing a product from the websites that request less and more personal information (Tsai *et al.*, 2011; Beresford *et al.*, 2012; Egelman *et al.*, 2013) or of disclosing personal information in exchange for rewards (Grossklags and Acquisti, 2007; Hann *et al.*, 2007; Acquisti *et al.*, 2013).

We chose the indirect experimental approach over surveys and direct elicitation for three reasons. *First*, Acquisti *et al.* (2016) noted that stated preferences often differ from observed behavior: people claim to care about privacy (Turow *et al.*, 2015), but they disclose personal information relatively freely (Norberg *et al.*, 2007). Prior research have provided evidence of this so-called "privacy paradox" (Sutanto *et al.*, 2013; Taddicken, 2014). Preferences derived from observed choices, even in the relatively artificial context of a laboratory experiment, may thus better predict actual behavior than self-reported attitudes to hypothetical scenarios. *Second*, direct measurements of privacy attitudes (e.g. WTA/WTP) force people to consciously choose answers. This is unreliable because people may find it difficult to accurately and explicitly assess risks and losses associated with privacy (Schwarz, 1999). Graeff and Harmon (2002), Lewis *et al.* (2008) and Preibusch (2013) indeed reported superior performance of indirect methods over direct surveys in measuring privacy concerns. *Third*, we incentivized answers, so that people consider privacy outcomes in connection with economic tradeoffs and have to balance monetary gains and privacy loss.

Our method differs from existing methods by presenting a *risk* of a loss of privacy instead of an immediate and certain threat to privacy (Spiekerman *et al.*, 2001; Shostack, 2003; Grossklags and Acquisti, 2007; Hann *et al.*, 2007). In real life, people have to decide how much to invest to protect their information from unspecified stochastic threats with uncertain consequences. Preferences elicited in a context of threat *certainty* may therefore not translate into actual behavior in a risky situation, as it overlooks people's level of tolerance for privacy risks. We believe that the behavior of people confronted with the *risk* of privacy loss is a more nuanced predictor of their behavior in real life than their attitudes to sure privacy outcomes.

The abovementioned reasons lead us to propose an implicit assessment of the VPR.

3. Method

We present our experimental procedures and derive measures of VPR. Supplementary material is available at https://osf.io/pmqes/ and is referenced by sections S1 to S6.

3.1 Synthetic generation of a privacy concern

We synthetically generate a privacy concern by collecting the name, surname and photos of our participants and combining this information with answers to a preliminary questionnaire about opinions on potentially sensitive topics, such as abortion, illegal immigration and appropriate methods of birth contraception (see S1). This private information remained unknown to other participants in the room unless the outcome of the experiment was to reveal it at the end. Our method is not limited to the type of personal information used in this experiment, and researchers are encouraged to apply the method to different types of personal information and related privacy risks and concerns.

The intraclass correlation coefficient among answers on the preliminary questionnaire equals 0.56, proving that a large proportion of participants expressed opinions that differed from others, meaning that there was no universal truth or socially preferable norm in the group. Thus, regardless of someone's expressed belief, about half of the participants in the laboratory would disagree with it if that belief were revealed. We are not concerned about whether one's *expressed* opinion corresponds to one's truthfully *held* opinion, because expressed opinions, even if untruthful, will contradict the opinions of some other people. Thus, the risk of information disclosure generates a fear of being shunned by some other people if one's expressed opinions contradict theirs (Noelle-Neumann, 1974)[2].

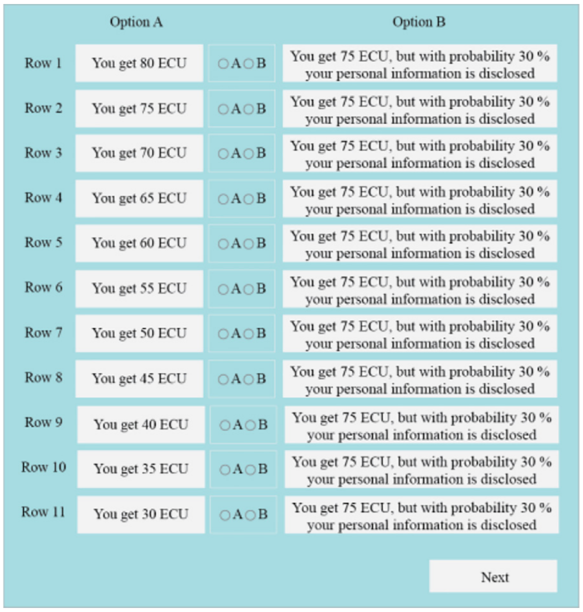
Several experimental studies *synthetically* produced personal information to investigate privacy attitudes, e.g. using public good game (Rivenbark, 2012), quiz (Grossklags and Acquisti, 2007) and logic test (Feri *et al.*, 2016). Such methods suffer from an overconfidence bias (Griffin and Varey, 1996), whereby people tend to believe they belong to a group with a test score above median. Our novel method overcomes this disadvantage of using intelligence test scores. By covering multiple contexts, we increase the probability to capture an issue that is sensitive for an individual. Our method thus induces a privacy concern without falling into issues with truth-telling. Although the elicited information is sensitive in the laboratory context, it cannot be misused to damage the participants materially, which helps overcome legal constraints in the collection, storage and use of personal information.

3.2 The elicitation of risk aversion

After collecting personal data, we generated privacy concern by putting private information under the risk of disclosure to other participants. To elicit risk aversion, we asked participants to make choices between gambles in a variation of the multiple price list (MPL) commonly used to elicit preferences in experimental economics. MPLs are easy to understand for participants and are incentive-compatible (Holt and Laury, 2002; Andersen *et al.*, 2006). Participants were offered eight lists, each requiring 11 decisions between safe options and risky lotteries (see Tables I and II in S2). Payoffs were expressed in experimental currency units (ECU), with 1 ECU = €0.1. There were two types of lotteries: *monetary lotteries* that involved only monetary payoffs, which the participant would receive with a certain probability, and *privacy lotteries*, which in addition to monetary rewards involved a certain known risk of personal information revelation to other experimental participants. Subjects were asked to indicate the option they preferred to play for every row (see example in Figure 1). The order of MPLs, within each task, was randomized.

In each row, the participants had to choose between a safe payoff x and a lottery L. Lottery L offers monetary payoff y, reduced by c with probability $1 - p$ (in monetary lotteries) or combined with disclosure of personal information with probability $1 - p$ (in privacy lotteries)[3]. Values of x, y and p were the same in monetary and privacy tasks.

Figure 1 Example of an MPL in the privacy task



	Option A		Option B
Row 1	You get 80 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 2	You get 75 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 3	You get 70 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 4	You get 65 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 5	You get 60 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 6	You get 55 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 7	You get 50 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 8	You get 45 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 9	You get 40 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 10	You get 35 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed
Row 11	You get 30 ECU	○A○B	You get 75 ECU, but with probability 30 % your personal information is disclosed

We kept the probability of loss fixed at 30 per cent[4] and not lower to avoid the issue of probability weighting, whereby low probabilities are overweighted (Tversky and Kahneman, 1992). We chose to vary the safe payoff across rows rather than probabilities of a loss because comparisons of monetary payoffs are easier for participants than comparisons of probabilities.

3.3 Measure of financial risk aversion

We measure financial risk aversion by calculating the *rate of return* ("*ror*") required by each participant to choose the lottery rather than the safe payoff. If a participant is indifferent between safe payoff x_{kj} and lottery $L_k = (y, p; y - c, 1 - p)$ in row $j \in [1{,}11]$ of table $k \in [1{,}4]$ – where y is a monetary payoff, which is reduced by c with probability $1 - p$ – then $x_{kj} \cdot (1 + ror_{kj} = y_k \cdot p + (y_k - c_k) \cdot (1 - p)$. Therefore, the participant requires a rate of return of:

$$ror_{kj} = \frac{y_k \cdot p + (y_k - c_k) \cdot (1 - p) - x_{kj}}{x_{kj}} \qquad (1)$$

We first compute ror_{kj} for each row of each MPL in a monetary task. Then we identify the indifference point as the row participant i switches from the safe to the risky option and use the midpoint of the relevant interval of ror_{ik} as a measure of the participant's financial risk aversion (see Table III in S2). We also compute $\overline{ror}_i$, the average individual *ror* across all MPLs in the monetary task. With our MPLs in the monetary task, we are able to obtain an estimate of the risk premium even for high or low values of *ror* (between −32 per cent and 100 per cent)[5].

3.4 Measure of value of privacy under risk

We measure the *v*alue of *p*rivacy under *r*isk ("VPR") as an implicit monetary equivalent of the (dis)utility of the risk of personal information disclosure for a risk-neutral participant. Closest to our measure of *VPR* is the notion in the work by Hirschprung *et al.* (2016), which defines privacy value as "the value of the benefits at the equilibrium point, when an individual is indifferent to the information disclosure." Our measure of *VPR* is an indicator of participants' combined aversion to both risk and personal information disclosure, because their choices between lottery and safe options take account of both their individual risk tolerance and their value of privacy.

If a risk-neutral participant is indifferent between safe payoff x_{kj} and privacy lottery $L_k = (y, p; y - VPR, 1 - p)$ in row $j \in [1{,}11]$ of table $k \in [5{,}8]$ – where y is a monetary payoff, accompanied by probability $1-p$ of information disclosure – then $x_{kj} = y_k \cdot p + (y_k - VPR_{kj}) \cdot (1 - p)$. Thus:

$$VPR_{kj} = \frac{y_k - x_{kj}}{1 - p} \qquad (2)$$

Using equation (2), we compute an interval estimate of VPR_{ik} implied by individual switching points in the MPL of the privacy task (see Table IV in S2)[6]. We also compute $\overline{VPR}_i$, the average individual *VPR* across MPLs.

With our MPLs in the privacy task, we can measure *VPR* between 150 ECU (€15) and −100 ECU (−€10). Positive and negative values of *VPR* represent disliking and enjoying the risk of personal information disclosure, respectively. Note that the *VPR* is not a monetary equivalent of privacy loss but of the *risk* of such a loss. In other words, *VPR* combines the individual's perceived value of privacy and his level of aversion to risk – participants who are more risk-averse and participants who value privacy more have higher *VPR*. (Although outside of the scope of this paper, further research should disentangle those two aspects of decision under privacy risk.)

We also measure privacy attitudes from survey responses [WTA, WTP, general privacy concerns, index of online information revelation, Privacy Index (Westin, 1968), online social network used, online privacy settings and self-disclosure index]. We also elicit a risk index reflecting general and domain-specific risk aversion, a trust index and sociodemographic indicators (see S3). An index of *conformity* to the opinion of others in the preliminary questionnaire (average percentage of participants who agree with one's opinion, summed over all questions) accounts for a possible exacerbated privacy concern for those participants whose opinion does not fit with the majority.

3.5 Experimental procedures

We conducted our experiment at the University of Trento, upon approval by the institutional review board[7]. We recruited 148 participants, in groups of 15-21 participants per 1-h session, among undergraduate students. The demographic characteristics were similar across all sessions, with 66 per cent male participants and 94 per cent between the age of 18 and 25 years (see S3). On average, the participants obtained €8.83 per person, including a €3 show-up fee.

When invited to participate, the subjects were not told that the scope of the study was related to privacy. After reading about the potential revelation of personal information, the participants were given a chance to withdraw from the study without losing the show-up fee. All decided to participate and signed a consent form. We then took photos of the participants and let them answer the preliminary questionnaire. We guaranteed them that their photos would be deleted after the session and that their answers were anonymized.

After reading the instructions (see S5) and passing a comprehension test, the participants made a sequence of binary choices between safe and risky options in two types of lotteries: *monetary* lotteries that imply changes in monetary outcome, and *privacy* lotteries that imply the disclosure of personal information. The participants played either monetary or privacy lotteries first.

Eventually, the participants answered a final questionnaire about the experiment, demographics, attitudes towards privacy, risk, self-disclosure, fairness, trust and WTA/WTP for their personal information (see S3).

At the end of each session, the participants separately came to the experimenter and one of the participants' decisions in the experiment was implemented. A dice roll decided the probabilistic outcome. If personal information had to be disclosed to other participants, then the participant stood in front of the audience in the lab and the experimenter verified his name and surname from the ID card and announced it aloud. Other participants saw on the screen the participant's photo and his answers in the preliminary questionnaire, along the fraction of participants who answered differently, to emphasize differences in opinions.

4. Results

There were 70 participants in the *privacy lotteries first* condition group and 78 participants in the *monetary lotteries first* condition group. In 95.86 per cent of the cases, the participants switched from the safe to the risky option in the MPLs once, demonstrating consistent monotonic preferences[8].

4.1 Value of privacy under risk

Average $\overline{VPR}$ for the participants for whom it was observed (90 per cent of the total) was 25 ECU (€2.5), whereas mean WTA was €16.1 and mean WTP was €1.9[9]. Table AI summarizes the estimations of privacy value under risk, and Figure A1 shows their distribution.

Of the 148 participants, 49 participants (33 per cent) had $\overline{VPR} = 5$ ECU (€0.5); those participants systematically decided based only on expected monetary payoffs. They are thus *indifferent* to the risk of personal information disclosure. Another 94 participants (64 per cent) had $\overline{VPR} > 5$ ECU (*privacy protective*), of which 14 never took any privacy risk ($\overline{VPR} > 150$ ECU)[10]. Finally, five participants (3 per cent) had $\overline{VPR} < 5$ ECU (*privacy risk loving*). There were no participants who always chose the risky option ($\overline{VPR} < -100$ ECU).

The majority of our participants were thus averse to privacy disclosure, a large minority was indifferent and a small minority enjoyed privacy disclosure[11].

Most of our participants were not comfortable with personal information disclosure, and they chose safe options in privacy lotteries at least some of the time, demonstrating the presence of privacy concerns. However, some appeared willing to make their personal information and opinions public. This may reflect differences in goals, attitudes, personality traits and other factors (Correa *et al.*, 2010). This minority tendency to disclose is consistent with the use of social media and could be especially prevalent for the active users of such technologies, extensively present in the population of students and, consequently, in our sample.

4.2 The drivers of the value of privacy under risk

We test the drivers of the VPR by specifying two models for regression analysis. The first model relates *VPR* and *ror*:

$$\overline{VPR}_i = \beta_0 + \beta_1 \cdot \overline{ror_i} + \beta_2 \cdot Order_i + \ldots + \varepsilon_{ik} \tag{3}$$

where $\overline{VPR_i}$ is average *VPR* for individual *i* across tables $k \in [5,8]$, except if the individual always choses Option A (right-censoring, $\overline{VPR_i} > 150$ ECU) or always choses Option B (left-censoring, $\overline{VPR_i} < -100$ECU). Further, ror_i is average *ror* for participant *i* from his choices in tables $k \in [1,4]$[12]. $Order_k$ takes value 0 if monetary tasks appeared before privacy tasks, and 1 otherwise.

To test the robustness of our results, we test a second regression model, where we use the number of safe choices in privacy lotteries as the dependent variable and the average number of safe choices made in the monetary lotteries, instead of $\overline{ror_i}$, as an independent variable:

$$safe\,privacy_{ik} = \beta_0 + \beta_1 \cdot safe\,monetary_{ik} + \beta_2 \cdot Order_i + \beta_3 \cdot Table_k + \ldots + \varepsilon_{ik} \tag{4}$$

whereby $safe\,privacy_{ik}$ is the number of safe choices made by individual *i* in privacy MPL $k \in [5,8]$ and $safe\,monetary_{ik}$ is the average number of safe choices made by individual *i* in monetary MPLs. $Order_i$ takes value 0 if the monetary task appeared before the privacy task, and 1 otherwise; $Table_k$ is a control for differences in the number of safe choices across tables. To estimate the second model, we run panel random-effects interval regressions, taking into account right- and left-censoring (when a participant always chooses Option A or Option B in a given MPL).

4.2.1 The relation between financial and privacy risk aversion.
Our regressions show that the *ror* measure of aversion to risk in monetary tasks is a significant positive predictor of *VPR* (Table AII). We find the same positive significant relation between the number of safe choices in monetary and privacy lotteries (Table AIII). Thus, the participants who are more risk-averse in monetary lotteries are also more risk-averse in privacy lotteries; someone who is unwilling to take a risk involving a monetary loss will be also generally unwilling to take a risk involving a privacy loss.

4.2.2 The relation between explicit privacy attitudes and implicit values of privacy under risk
Higher WTA and WTP predict higher *VPR*, whereby *VPR* increases by an average of 0.5 ECU (€0.05) for every euro increase in WTA and by an average of 2 ECU (€0.20) for every euro increase in WTP (Table AII). There is, therefore, a relation between our implicit measure of privacy risk aversion and explicit measures of valuations for privacy, but that relation is rather weak.

Other factors that relate to *VPR* are past experiences of privacy violation, general privacy concerns and whether one is a

Westin's fundamentalist. None of the sociodemographic characteristics influences privacy decisions, except being a foreigner (non-Italian), which increases the number of safe choices made in privacy lotteries. This can be related to cultural differences, the potentially higher uncertainty among foreigners regarding sensitive opinion distribution in Italy or generally lower self-confidence related to being a national minority.

These findings confirm that the participants who express more concern for privacy and/or express higher values for protecting their private information are also less likely to take the risk of having to reveal private information[13].

Regarding contributions of privacy attitudes and financial risk preferences to explaining the VPR, the McFadden's pseudo R^2 of our full model is 10.7 per cent for *VPR* regressions and 8.9 per cent for safe choice regressions. Of this, about 40 per cent is contributed by measures of risk attitude in monetary lotteries, 40 per cent by WTA/WTP and the rest by survey measures of privacy attitudes and sociodemographic variables. Those numbers indicate the relative importance of the risk and privacy loss aspects of privacy risk.

Overall, the participants who are more risk-averse than others when faced with monetary lotteries are also more risk-averse than others when faced with privacy lotteries. The participants who express more concern for privacy and who are ready to pay more to protect it, or who require more money to reveal it, are less likely to take a risk in privacy lotteries.

5. Robustness to order effect and preexisting threat

We test the robustness of the *VPR* to:

- the order of elicitation of monetary and privacy risk attitudes; and
- the inability to avoid incurring any privacy risk.

The first issue is important for experimenters, as they have to choose what attitude to elicit first, and the order of elicitation may impact how participants perceive the tasks. The second issue is important for policymakers, as they are interested in eliciting attitude to privacy risks that the population is already exposed to.

5.1 Order of elicitation

In our experiment, we presented privacy lotteries first for some participants ($N = 70$) and monetary lotteries first for the others ($N = 78$). The order of elicitation can matter because theories of selective information processing state that focus on a primary task reduce attention to a secondary task (Kahneman, 1973). The emphasis on monetary values could drive attention away from the evaluation of the utility of maintaining personal information private. The latter could be even considered as irrelevant for decision-making when the financial context is set up in advance and perceived as more salient (Broadbent, 1957). Moreover, due to immediacy effects (Prelec and Loewenstein, 1991), the participants may make more privacy protective decisions right after answering private questions. The time delay between answering the sensitive questions in the opinion survey and putting these responses under risk of disclosure is longer when the privacy lotteries are played after the monetary lotteries. Adjerid *et al.* (2013) found that the 15 second delay between demonstration of privacy notice and disclosure decisions was sufficient to distract participants and mute the perception of risk.

Statistical tests and cumulative distribution function show a significant order effect in the privacy task: participants made more safe choices in the privacy lotteries and had higher *VPR* when the privacy tasks appeared before the monetary tasks[14]. Similarly, more participants took only safe alternatives in privacy lotteries when the privacy task appeared first (20 per cent) than when the monetary task appeared first (12 per cent) [15]. Fewer people (25 per cent) behaved as if they had value for privacy close to zero when privacy lotteries appeared first (25 per cent) than when monetary lotteries appeared first (36 per cent)[16]. Thus, the willingness to protect personal information from the risk of revelation increases when those decisions are made before decisions involving risk of a monetary loss.

Although cumulative distribution function and statistical tests show that *VPR* is higher when privacy tasks appear first, coefficients on this condition dummy in regressions (Appendix 2) are not consistently significant. However, we find that the relation between *VPR* and *ror* is stronger when the privacy task appeared first (Figure 2). This suggests that when the privacy tasks appeared before the monetary ones, then decisions in the privacy task were more closely driven by risk aversion.

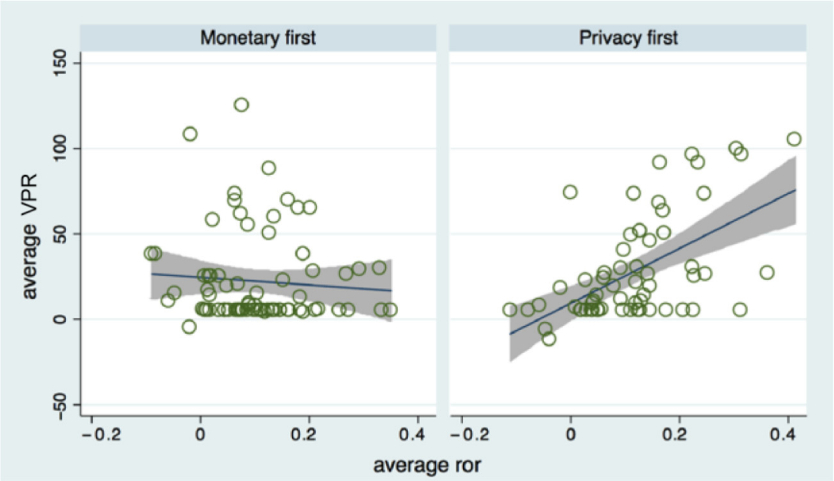
5.2 Preexisting risk to privacy

We also tested the effect of introducing an unavoidable risk of revelation of personal information, independent of the choice to incur privacy risks in the experiment. Prior research has identified control (or the lack thereof) as an important driver of risk aversion and behaviors (Slovic, 2000). Individuals deprived of control are reluctant to exert effort to achieve a desirable outcome (Hopstaken *et al.*, 2015). People who lost control over personal data may feel it is futile to protect it and disengage from privacy decisions (Choi *et al.*, 2018).

In our experiment, we tested the effect of reducing control over the release of personal information by running a treatment with the possibility of a "privacy shock" ($N = 67$) along with a treatment without such a privacy shock ($N = 81$). We crossed this treatment with the order of elicitation in a 2 × 2 treatment design (see Table VI in S6). In the shock treatment, participants were told before the experiment that there was a 21 per cent probability that their information will be revealed to others irrespective of their decisions in the laboratory. Such possibility of a privacy shock reflects a real-world externality of data trading: Data subjects do not have full control over their personal information because the possibility of a data breach depends on not only their behavior and choices alone but also the vulnerabilities of companies' security systems (Feri *et al.*, 2016). Statistical tests and cumulative distribution function show no significant effect of introducing a privacy shock: Participants made the same number of safe choices in the privacy lotteries and had the same *VPR*[17].

Thus, the introduction of a privacy shock does not lead people to change their attitudes toward personal information protection. Even when losing complete control over personal information, people keep on considering the level of risk that remains under their control in a similar way as if they had full control over whether to incur this risk.

Figure 2 Scatter plot of $\overline{ror}$ and $\overline{VPR}$ by order of elicitation, with prediction line of linear regression and 95 per cent confidence interval for forecast



6. Conclusion

We presented a novel method for the implicit elicitation of the VPR. Our method is based on observed behavior instead of surveyed attitudes; it is incentivized and involves a probabilistic risk to privacy. In a laboratory experiment, 148 participants chose between sure monetary payoff and lotteries of two types: monetary lotteries elicited financial risk preferences, whereas privacy lotteries elicited the willingness to protect personal information. We found a positive relationship between financial and privacy risk aversion. Willingness to protect personal information is driven at least in part by risk aversion rather than by differences in values for personal information and privacy attitudes. Further research is needed to test how well intentions correlate with actual decisions to jeopardize or protect private information. Already, however, we showed that our measure correlates with reported attitudes to risk and privacy and WTA/WTP for privacy protection.

We make further methodological and practical contributions:

- First, our method to synthetically elicit privacy concerns overcomes the shortcoming of other synthetic concern generation methods.
- Second, we propose a novel technique for the implicit elicitation of the VPR. This method is incentive-compatible and implies more intuitive decisions for the participants than direct calculation of the value of personal information, which is less readily cognitively available.
- Third, we find qualified support for the existence of an order effect: presenting privacy choices prior to financial ones leads to more privacy-protective behavior. We discussed potential interpretations in Section 5.1.
- Fourth, we find that taking away full control over one's personal information does not change willingness to incur privacy risk. Thus, the VPR can be measured accurately even if participants' personal information is already jeopardized by factors out of their control, for example, if they have provided information to a company or other entity and are therefore already exposed to a privacy risk. This property is especially useful when running natural and field experiments.

We encourage further work to study privacy risk aversion and quantify consumer welfare losses incurred because of risk exposure in various scenarios. Our approach can be applied to different types of private information and risks, including risks with remote rather than immediate consequences (e.g. unauthorized sharing with third parties, use for unsolicited targeted marketing, fraud, price discrimination when calculating insurance premiums). Because exposing individuals to a real risk of losing private health, financial or social network information may not be ethically feasible, researchers may use our incentivized lottery-based method for vignette studies with hypothetical scenarios of privacy loss, associated risks and its likelihood of occurrence. Finally, researchers could vary the means by which privacy protection is achieved (the safe options in privacy lotteries) and its price. This may involve purchasing a cybersecurity insurance, using privacy-enhancing technologies or using software for data protection. Such measures of privacy risk aversion would be useful for policymakers when surveying public opinion, evaluating existing policies (e.g. whether current regulations address consumers' concerns) and making decisions about privacy regulations and consumer protection. Surveying privacy risk aversion and the VPR can also serve a practical role when computing privacy insurance premiums, deciding what privacy insurance should cover and when doing comparative studies of factors affecting privacy risk tolerance.

Notes

[1] See Martin and Murphy (2017) and Milne (2015) for a review of other organizational privacy models, the impact of privacy regulation on economic outcomes and other roles of privacy in marketing.

[2] Due to counter-conformity motivation (Tian *et al.*, 2001), some people may prefer to avoid conformity with popular opinions. However, due to randomization, the proportion of such people between conditions is equal, canceling out the impact of this factor on treatment effects.

[3] Variable *c* took a negative value in one of the tables, to consider how participants respond to the probability of a gain.

4 We chose 30 per cent, because 50 per cent probability of personal information disclosure is unrealistically high for the privacy risk domain. The same level of risk was used in the study by Hirschprung *et al.* (2016).

5 Adopting the idea that back-and-forth switching behavior could be the result of indifference, we use the mean value between the lower bound of the first switch and the upper bound of the last switch in MPL (Andersen *et al.*, 2006). If a participant never switched in an MPL, then we consider the level of *ror* unobserved. If a participant never chose Option B in any MPL, then his $ror > 100$ per cent. If a participant always chose Option B, then his $ror < -32$ per cent.

6 In case of multiple switching, for *VPR*, we use the mean value between the lower bound of the first switch and the upper bound of the last switch in MPL.

7 See a more detailed description of the experimental procedures in S4.

8 This is similar to observations in the study by Holt and Laury (2002). All the results were robust to exclusion of observations from the participants who switched more than once.

9 Mean WTA/WTP exclude outliers more than two standard deviations from the mean.

10 The situations, when participants always chose safe options over privacy lotteries, indicate either right-censored privacy risk values or the view of privacy as a fundamental human right, with no price high enough to compensate for the privacy loss.

11 This contrasts with WTA/WTP, which were all higher than or equal to zero. Future experiments on privacy should make participants aware of possibility to express willingness to disclose personal data rather than assuming that all participants are unwilling to disclose.

12 Because three participants always avoided financial risk ($\overline{ror_i} > 100\%$), meaning that their level of risk aversion is not observed, we also include in our regressions a dummy highly risk averse, which is equal to 1 if $\overline{ror_i} > 100\%$, and equal to 0 otherwise. Formally, our regression is therefore of the form $\overline{VPR}_i = \beta_0 + \beta_1 \cdot \overline{ror_i} \cdot 1(\overline{ror_i} < 100\%) + \beta_1' \cdot 1(\overline{ror_i} > 100\%) + \beta_2 \cdot Order_i + \cdot + \varepsilon_{ik}$.

13 The results are robust when considering the number of safe choices in privacy lotteries (Table AIII).

14 Tests of the difference in the number of safe choices (and VPR in parentheses): Wilcoxon $p = 0.01$ (0.028), *t*-test $p = 0.01$ (0.03); Kolmogorov–Smirnov corrected $p = 0.04$ (0.10); ANOVA $\beta = 0.77$ (5.53), $p = 0.02$ (0.06); Kruskal–Wallis $p = 0.01$ (0.03). $N_{ID} = 148$; $N_{obs} = 592$ (375). Power = 0.66 (0.45).

15 Excluding MPL 4, proportion test $p = 0.01$. Pearson χ^2 (1) = 5.32 ($p = 0.021$). Power = 0.63.

16 Two-sample test of proportions: $p = 0.00$. Power = 0.83.

17 Tests of the difference in the number of safe choices (and in VPR in parentheses): Wilcoxon $p = 0.84$ (0.41); *t*-test $p = 0.9996$ (0.91); Kolmogorov–Smirnov corrected $p = 0.99$ (0.79); ANOVA $\beta = -0.0002$ (-0.30), $p = 1.00$ (0.91); Kruskal–Wallis $p = 0.84$ (0.41). $N = 592$ (375). Power = 0.05.

References

Acquisti, A., John, L.K. and Loewenstein, G. (2013), "What is privacy worth? ", *The Journal of Legal Studies*, Vol. 42 No. 2, pp. 249-274.

Acquisti, A., Taylor, R. and Wagman, L. (2016), "The economics of privacy", *Journal of Economic Literature*, Vol. 54 No. 2, pp. 442-492.

Adjerid, I., Acquisti, A., Brandimarte, L., (2013), and G. and Loewenstein, "Sleights of privacy: framing, disclosures, and the limits of transparency", *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM, pp. 9:1-9:11.

Andersen, S., Harrison, G.W., Lau, M.I. and Rutström, E.E. (2006), "Elicitation using multiple price list formats", *Experimental Economics*, Vol. 9 No. 4, pp. 383-405.

Arnott, D.C., Wilson, D., Mukherjee, A. and Nath, P. (2007), "Role of electronic trust in online retailing: a re-examination of the commitment-trust theory", *European Journal of Marketing*, Vol. 41 Nos 9/10, pp. 1173-1202.

Ashworth, L. and Free, C. (2006), "Marketing dataveillance and digital privacy: using theories of justice to understand consumers' online privacy concerns", *Journal of Business Ethics*, Vol. 67 No. 2, pp. 107-123.

Bart, Y., Shankar, V., Sultan, F. and Urban, G.L. (2005), "Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study", *Journal of Marketing*, Vol. 69 No. 4, pp. 133-152.

Bennett, C.J. and Raab, C.D. (2006), *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, Massachusetts.

Beresford, A.R., Kübler, D. and Preibusch, S. (2012), "Unwillingness to pay for privacy: a field experiment", *Economics Letters*, Vol. 117 No. 1, pp. 25-27.

Bleier, A. and Eisenbeiss, M. (2015), "Personalized online advertising effectiveness: the interplay of what, when, and where", *Marketing Science*, Vol. 34 No. 5, pp. 669-688.

Brandimarte, L., Acquisti, A. and Lowenstein, G. (2012), "Misplaced confidences: privacy and the control paradox", *Social Psychological and Personality Science*, Vol. 4, pp. 341-347.

Broadbent, D.E. (1957), "A mechanical model for human attention and immediate memory", *Psychological Review*, Vol. 64 No. 3, pp. 205-215.

Camp, L.J. (2003), "Design for trust", in Falcone, R. (Ed.), *Trust, Reputation and Security: Theories and Practice*, Springer-Verlag.

Chellappa, R.K. and Sin, R.G. (2005), "Personalization versus privacy: an empirical examination of the online consumer's dilemma", *Information Technology and Management*, Vol. 6 Nos. 2/3, pp. 181-202.

Choi, H., Park, J. and Jung, Y. (2018), "The role of privacy fatigue in online privacy behavior", *Computers in Human Behavior*, Vol. 81, pp. 42-51.

Correa, T., Hinsley, A.W. and De Zuniga, H.G. (2010), "Who interacts on the web? The intersection of users' personality and social media use", *Computers in Human Behavior*, Vol. 26 No. 2, pp. 247-253.

Culnan, M.J. and Bies, R.J. (2003), "Consumer privacy: balancing economic and justice considerations", *Journal of Social Issues*, Vol. 59 No. 2, pp. 323-342.

Dinev, T. and Hart, P. (2006), "An extended privacy calculus model for e-commerce transactions", *Information Systems Research*, Vol. 17 No. 1, pp. 61-80.

Egelman, S., Felt, A.P. and Wagner, D. (2013), "Choice architecture and smartphone privacy: there's a price for that", *The Economics of Information Security and Privacy*, Springer, pp. 211-236.

Fang, J., Zhao, Z., Wen, C. and Wang, R. (2017), "Design and performance attributes driving mobile travel application engagement", *International Journal of Information Management*, Vol. 37 No. 4, pp. 269-283.

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

Ferrell, O.C. and Gresham, L.G. (1985), "A contingency framework for understanding ethical decision making in marketing", *Journal of Marketing*, Vol. 49 No. 3, pp. 87-96.

Gabisch, J.A. and Milne, G.R. (2014), "The impact of compensation on information ownership and privacy control", *Journal of Consumer Marketing*, Vol. 31, pp. 13-26.

George, J.F. (2004), "The theory of planned behavior and internet purchasing", *Internet Research*, Vol. 14 No. 3, pp. 198-212.

Goldfarb, A. and Tucker, C. (2011), "Online display advertising: targeting and obtrusiveness", *Marketing Science*, Vol. 30 No. 3, pp. 389-404.

Graeff, T.R. and Harmon, S. (2002), "Collecting and using personal data: consumers' awareness and concerns", *Journal of Consumer Marketing*, Vol. 19 No. 4, pp. 302-318.

Griffin, D.W. and Varey, C.A. (1996), "Towards a consensus on overconfidence", *Organizational Behavior and Human Decision Processes*, Vol. 65 No. 3, pp. 227-231.

Grossklags, J. and Acquisti, A. (2007), "When 25 cents is too much: an experiment on willingness-to-sell and willingness-to-protect personal information", *Proceedings of the Sixth Workshop on the Economics of Information Security*, pp. 7-18.

Hann, I.-H., Hui, K.-L., Lee, S.-Y.T. and Png, I.P. (2007), "Overcoming online information privacy concerns: an information-processing theory approach", *Journal of Management Information Systems*, Vol. 24 No. 2, pp. 13-42.

Hirschprung, R., Toch, E., Bolton, F. and Maimon, O. (2016), "A methodology for estimating the value of privacy in information disclosure systems", *Computers in Human Behavior*, Vol. 61, pp. 443-453.

Holt, C.A. and Laury, S.K. (2002), "Risk aversion and incentive effects", *American Economic Review*, Vol. 92 No. 5, pp. 1644-1655.

Hopstaken, J.F., Linden, D., Bakker, A.B. and Kompier, M.A. (2015), "A multifaceted investigation of the link between mental fatigue and task disengagement", *Psychophysiology*, Vol. 52 No. 3, pp. 305-315.

Kahneman, D. (1973), *Attention and Effort*, Prentice-Hall, Englewood Cliffs.

Kahneman, D., Knetsch, J.L. and Thaler, R.H. (1991), "Anomalies: the endowment effect, loss aversion, and status quo bias", *Journal of Economic Perspectives*, Vol. 5 No. 1, pp. 193-206.

Knetsch, J.L. and Sinden, J.A. (1984), "Willingness to pay and compensation demanded: experimental evidence of an unexpected disparity in measures of value", *The Quarterly Journal of Economics*, Vol. 99 No. 3, pp. 507-521.

Lewis, K., Kaufman, J. and Christakis, N. (2008), "The taste for privacy: an analysis of college student privacy settings in an online social network", *Journal of Computer-Mediated Communication*, Vol. 14 No. 1, pp. 79-100.

Lwin, M., Wirtz, J. and Williams, J.D. (2007), "Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective", *Journal of the Academy of Marketing Science*, Vol. 35 No. 4, pp. 572-585.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research*, Vol. 15 No. 4, pp. 336-355.

Martin, K. (2015), "Privacy notices as tabula rasa: an empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online", *Journal of Public Policy & Marketing*, Vol. 34, pp. 210-227.

Martin, K.D. and Murphy, P.E. (2017), "The role of data privacy in marketing", *Journal of the Academy of Marketing Science*, Vol. 45 No. 2, pp. 135-155.

Milne, G. (2015), *Digital Privacy in the Marketplace: Perspectives on the Information Exchange*, Business Expert Press, New York, NY.

Milne, G.R. and Culnan, M.J. (2004), "Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices", *Journal of Interactive Marketing*, Vol. 18 No. 3, pp. 15-29.

Noelle-Neumann, E. (1974), "The spiral of silence: a theory of public opinion", *Journal of Communication*, Vol. 24 No. 2, pp. 43-51.

Norberg, P.A., Horne, D.R. and Horne, D.A. (2007), "The privacy paradox: personal information disclosure intentions versus behaviors", *Journal of Consumer Affairs*, Vol. 41 No. 1, pp. 100-126.

Phelps, J., Nowak, G. and Ferrell, E. (2000), "Privacy concerns and consumer willingness to provide personal information", *Journal of Public Policy & Marketing*, Vol. 19 No. 1, pp. 27-41.

Preibusch, S. (2013), "Guide to measuring privacy concern: review of survey and observational instruments", *International Journal of Human-Computer Studies*, Vol. 71 No. 12, pp. 1133-1143.

Prelec, D. and Loewenstein, G. (1991), "Decision making over time and under uncertainty: a common approach", *Management Science*, Vol. 37 No. 7, pp. 770-786.

Rivenbark, D.R. (2012), "Valuing the risk from privacy loss: experimentally elicited beliefs explain privacy behavior", *Working Paper*, University of Central FL, Orlando, FL.

Schlosser, A.E., White, T.B. and Lloyd, S.M. (2006), "Converting web site visitors: investment increases consumer trusting beliefs and online purchase intentions", *Journal of Marketing*, Vol. 70 No. 2, pp. 133-148.

Schumann, J.H., Wangenheim, F.V. and Groene, N. (2014), "Targeted online advertising reciprocity appeals to increase acceptance among users of free web services", *Journal of Marketing*, Vol. 78 No. 1, pp. 59-75.

Schwarz, N. (1999), "Self-reports: how the questions shape the answers", *American Psychologist*, Vol. 54 No. 2, pp. 93-105.

Shostack, A. (2003), "Paying for privacy: consumers and infrastructures", *Proceedings of the 2nd Annual Workshop on Economics and Information Security*, Vol. 3.

Slovic, P.E. (2000), *The Perception of Risk*, Earthscan Publications, London.

Spiekerman, A., Grossklags, J. and Berendt, B. (2001), "E-privacy in 2nd generation e-commerce: privacy preferences versus actual behaviour", *Proceedings of the 3rd ACM Conference on Electronic Commerce*, ACM, New York, NY, 38-47.

Sutanto, J., Palme, E., Tan, C.-H. and Phang, C.W. (2013), "Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users", *MIS Quarterly*, Vol. 37 No. 4, pp. 1141-1164.

Taddicken, M. (2014), "The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure", *Journal of Computer-Mediated Communication*, Vol. 19 No. 2, pp. 248-273.

Tian, K.T., Bearden, W.O. and Hunter, G.L. (2001), "Consumers' need for uniqueness: scale development and validation", *Journal of Consumer Research*, Vol. 28 No. 1, pp. 50-66.

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*, Vol. 22 No. 2, pp. 254-268.

Tucker, C.E. (2014), "Social networks, personalized advertising and privacy controls", *Journal of Marketing Research*, Vol. 51 No. 5, pp. 1547-7193.

Turow, J., Hennessy, M. and Draper, N. (2015), "The tradeoff fallacy: how marketers are misrepresenting American consumers and opening them up to exploitation", Working Paper, The Annenberg School for Communication, University of Pennsylvania.

Tversky, A. and Kahneman, D. (1992), "Advances in prospect theory: cumulative representation of uncertainty", *Journal of Risk and Uncertainty*, Vol. 5 No. 4, pp. 297-323.

Westin, A.F. (1968), *Privacy and Freedom*. Atheneum, New York.

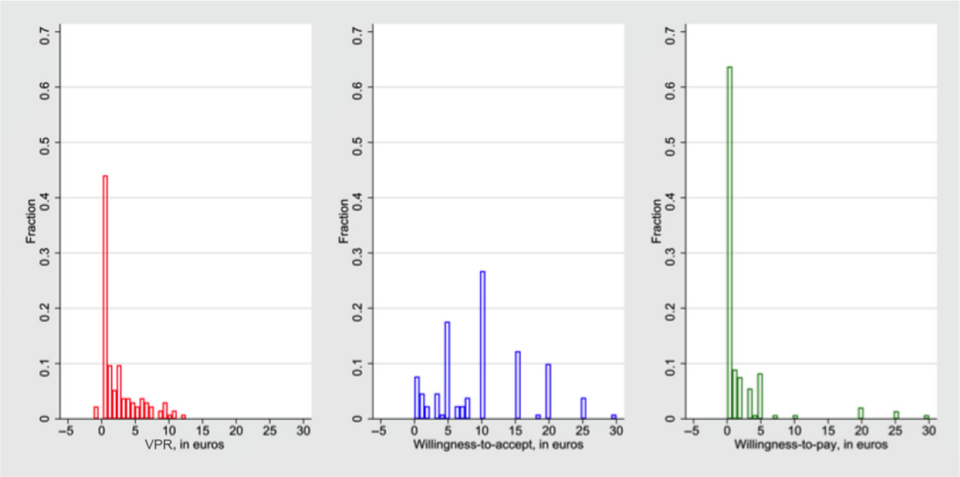
White, T.B., Zahay, D.L., Thorbjørnsen, H. and Shavitt, S. (2008), "Getting too personal: reactance to highly personalized email solicitations", *Marketing Letters*, Vol. 19 No. 1, pp. 40-50.

Appendix 1. Summary statistics

Table AI Measures of risk aversion (in %) and (dis)utility of personal information disclosure (in Euros)

	$\overline{ror}$	*VPR*	WTA	WTA (excluding outliers)	WTP	WTP (excluding outliers)
Min	−11%	−1.17	0	0	0	0
Max	41%	12.50	1,000	200	1,000	30
Mean	11%	2.52	36.20	16.12	10.00	1.92
Std. deviation	10%	2.89	141.84	25.33	83.67	4.85
N	145	134	147	144	148	146

Figure A1 Distribution of VPR, WTA and WTP



Appendix 2. Regressions

Table AII Interval regression of $\overline{VPR_i}$ over $\overline{ror_i}$

Model	(1)	(2)	(3)	(4)
$\overline{\mathrm{ror_i}}$	116.62**[42.63,190.62]	113.62**[39.21,188.02]	119.75***[48.75,190.76]	127.33***[54.70,199.96]
Highly risk averse (=1 if $\overline{\mathrm{ror_i}} > 100\%$ (a))	109.76***[49.29,170.23]	106.08***[44.92,167.25]	77.38**[20.13,134.62]	67.47*[10.01,124.93]
Treatment with privacy shock		−4.47 [−19.81,10.86]	−7.79 [−22.15,6.57]	−11.65 [−25.87,2.56]
Condition with privacy lotteries first		8.11[−7.36,23.58]	7.04 [−7.55,21.63]	3.19 [−11.51,17.89]
Q6: WTA			0.53** [0.19,0.86]	0.53**[0.21,0.86]
Q7: WTP			1.43 + [−0.08,2.94]	1.72*[0.25,3.20]
Q16: General privacy concern			9.15* [1.01,17.29]	7.28+[−0.93,15.50]
Q3: No. of participants known				−1.81 [−7.27,3.64]
Q5: Trust in experimenters				−6.63 [−58.31,45.05]
Q17-Q20: Index of online information revelation				5.02 [−4.18,14.22]
Q21: Victim of invasion of privacy				17.40* [0.30,34.50]
Q22: Westin's pragmatist				−4.01 [−21.06,13.05]
Q22: Westin's fundamentalist				11.23 [−8.89,31.35]
Q26-Q29: Index for online privacy settings				−4.51[−12.85,3.82]
Q30: Index of self-disclosure				1.23 [−0.75,3.21]
Index of conformity (from preliminary questionnaire)				−1.69 [−120.53,117.16]
Q31-Q32: Index of risk attitude				
Q33-Q37: Index of trust				
Q23: Number of close friends				
Q25: Number of online connections				
Constant	23.88***[12.67,35.09]	22.47**[8.10,36.83]	2.81[−14.22,19.84]	8.88[−75.89,93.64]
Socio-demographic controls	No	No	No	No
No. of individuals	148	148	143	143
Including right-censored	14	14	13	13
log likelihood	−725.56	−724.83	−690.81	−685.57
LR $\chi2$(degrees of freedom)	19*** (2)	21*** (4)	41*** (7)	51*** (16)

Notes: 95 per cent confidence intervals in brackets; $^{***}p < 0.001$; $^{*}p < 0.05$; $^{**}p < 0.01$.
(a) If a person never took risk in monetary lotteries, $\overline{ror_i}$ n the regression takes value 0, and the dummy highly risk averse ($\overline{ror_i} > 100\%$) takes value 1

(*continued*)

Table AII

Model	(5)	(6)
$\overline{\text{ror}_i}$	122.54***[50.27,194.81]	118.53***[48.13,188.93]
Highly risk averse (=1 if $\overline{\text{ror}_i} > 100\%$ (a))	67.91*[9.89,125.93]	75.08*[12.79,137.36]
Treatment with privacy shock	−12.44 + [−26.88,2.00]	−12.88 + [−27.62,1.86]
Condition with privacy lotteries first	5.50 [−9.22,20.23]	−1.47[−15.95,13.01]
Q6: WTA	0.52**[0.20,0.85]	0.59***[0.27,0.92]
Q7: WTP	2.17*[0.45,3.88]	2.38**[0.62,4.14]
Q16: General privacy concern	5.42 [−3.06,13.90]	6.12 [−2.39,14.64]
Q3: No. of participants known	−1.03 [−6.77,4.71]	0.20 [−5.91,6.31]
Q5: Trust in experimenters	−16.45 [−68.94,36.03]	−1.78 [−63.95,60.39]
Q17-Q20: Index of online information revelation	3.01 [−6.28,12.29]	−2.53 [−12.10,7.03]
Q21: Victim of invasion of privacy	14.93 + [−2.85,32.70]	22.06* [4.02,40.11]
Q22: Westin’s pragmatist	−3.53 [−20.92,13.85]	−1.33 [−18.77,16.10]
Q22: Westin’s fundamentalist	15.44 [−5.92,36.80]	30.97** [9.06,52.89]
Q26-Q29: Index for online privacy settings	−3.30 [−11.89,5.28]	1.36[−7.64,10.35]
Q30: Index of self-disclosure	1.01 [−1.00,3.02]	0.81 [−1.26,2.89]
Index of conformity (from preliminary questionnaire)	−8.12 [−128.38,112.14]	−21.86[−146.45,102.74]
Q31-Q32: Index of risk attitude	−4.42 + [−9.22,0.38]	−6.56* [−11.63, −1.50]
Q33-Q37: Index of trust	1.11 [−3.24,5.46]	0.90 [−3.56,5.36]
Q23: Number of close friends	0.92 [−0.59,2.43]	0.21 [−1.30,1.72]
Q25: Number of online connections	−0.00 [−0.02,0.01]	−0.01[−0.02,0.01]
Constant	7.83 [−77.93,93.58]	-55.72[−157.99,46.54]
Socio-demographic controls	No	Yes
No. of individuals	140	140
Including right-censored	13	13
log likelihood	−668.16	−655.90
LR $\chi 2$(degrees of freedom)	55*** (20)	80*** (39)

Table AIII Panel random-effects interval-data regression, number of safe choices in privacy lotteries by table

Model	(1)	(2)	(3)	(4)
Safe choices in monetary lotteries	0.632***[0.29,0.98]	0.659***[0.30,1.02]	0.617**[0.24,0.99]	0.585**[0.23,0.94]
Table 6		−1.332***[−1.81, −0.86]	−1.332***[−1.81, −0.86]	−1.323***[−1.81, −0.84]
Table 7		−1.799***[−2.27, −1.33]	−1.800***[−2.27, −1.33]	−1.798***[−2.28, −1.31]
Table 8		9.500***[8.70,10.30]	9.498***[8.70,10.30]	9.500***[8.68,10.32]
Treatment with privacy shock			−0.226[−1.44,0.99]	−0.530[−1.66,0.60]
Condition with privacy elicited first			0.701[−0.53,1.94]	0.522[−0.65,1.69]
Q6: WTA				0.0470***[0.02,0.07]
Q7: WTP				0.111+[−0.01,0.23]
Q16: General privacy concern				0.830*[0.20,1.46]
Q3: No. of participants known				
Q5: Trust in experimenters				
Q17-Q20: Index of information revelation				
Q21: Victim of invasion of privacy				
Q22: Westin's pragmatist				
Q22: Westin's fundamentalist				
Q26-Q29: Index for online privacy settings				
Q30: Index of self-disclosure				
Index of conformity in preliminary questionnaire				
Q31-Q32: Index of risk attitude				
Q33-Q37: Index of trust				
Q23: Number of close friends				
Q25: Number of online connections				
Constant	3.231**[0.78,5.68]	1.672[−0.92,4.27]	1.737[−0.86,4.33]	0.310[−2.26,2.88]
Socio-demographic controls	No	No	No	No
No. observations including:	592	592	592	572
Left-censored	5	5	5	5
Right-censored	212	212	212	204
No. of individuals	148	148	148	143
Log likelihood	−1,386	−1,030	−1,030	−988
Wald χ^2 (degrees of freedom)	13*** (1)	810*** (4)	812*** (6)	790*** (9)

Notes: 95 per cent confidence intervals in brackets; $^{****}p < 0.1$; $^{*}p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$

(continued)

Table AIII

Model	(5)	(6)	(7)
Safe choices in monetary lotteries	0.530**[0.17,0.89]	0.489**[0.13,0.85]	0.517**[0.18,0.86]
Table 6	−1.321***[−1.81, −0.83]	−1.356***[−1.85, −0.86]	−1.358***[−1.86, −0.86]
Table 7	−1.795***[−2.28, −1.31]	−1.840***[−2.34, −1.35]	−1.841***[−2.34, −1.35]
Table 8	9.498***[8.68,10.32]	9.427***[8.59,10.26]	9.426***[8.59,10.26]
Treatment with privacy shock	−0.791[−1.90,0.32]	−0.843[−1.97,0.28]	−1.070+[−2.20,0.06]
Condition with privacy elicited first	0.255[−0.92,1.43]	0.449[−0.73,1.62]	−0.0883[−1.22,1.04]
Q6: WTA	0.0434***[0.02,0.07]	0.0434***[0.02,0.07]	0.0483***[0.02,0.07]
Q7: WTP	0.134*[0.02,0.25]	0.168*[0.03,0.30]	0.164*[0.03,0.30]
Q16: General privacy concern	0.721*[0.09,1.36]	0.599+[−0.06,1.25]	0.781*[0.13,1.43]
Q3: No. of participants known	−0.328[−0.75,0.09]	−0.327[−0.77,0.12]	−0.225[−0.69,0.24]
Q5: Trust in experimenters	−1.671[−5.82,2.48]	−2.012[−6.21,2.19]	−0.0322[−4.82,4.76]
Q17-Q20: Index of information revelation	0.457[−0.26,1.17]	0.340[−0.38,1.06]	−0.125[−0.85,0.60]
Q21: Victim of invasion of privacy	1.241+[−0.08,2.56]	0.943[−0.43,2.31]	1.562*[0.20,2.93]
Q22: Westin’s pragmatist	−0.456[−1.78,0.87]	−0.398[−1.75,0.95]	−0.256[−1.58,1.07]
Q22: Westin’s fundamentalist	0.973[−0.58,2.52]	1.168[−0.48,2.82]	2.308**[0.66,3.95]
Q26-Q29: Index for online privacy settings	−0.194[−0.84,0.46]	−0.162[−0.83,0.51]	0.269[−0.42,0.95]
Q30: Index of self-disclosure	0.0313[−0.12,0.19]	0.00860[−0.15,0.17]	0.00305[−0.16,0.16]
Index of conformity in preliminary questionnaire	−2.582[−11.80,6.64]	−3.117[−12.44,6.20]	−4.301[−13.84,5.24]
Q31-Q32: Index of risk attitude		−0.292[−0.67,0.08]	−0.472*[−0.86, −0.08]
Q33-Q37: Index of trust		0.163[−0.18,0.50]	0.124[−0.22,0.46]
Q23: Number of close friends		0.0722[−0.05,0.19]	0.0259[−0.09,0.14]
Q25: Number of online connections		0.0000371[−0.00,0.00]	−0.000180[−0.00,0.00]
Constant	2.705[−4.69,10.10]	2.956[−4.50,10.41]	−1.400[−9.81,7.01]
Socio-demographic controls	No	No	Yes
No. observations including:	572	560	560
Left-censored	5	5	5
Right-censored	204	201	201
No. of individuals	143	140	140
Log likelihood	−982	−959	−944
Wald χ^2 (degrees of freedom)	803*** (18)	776*** (22)	802*** (41)

About the author

Dr Alisa Frik is a postdoctoral researcher at the International Computer Science Institute (ICSI) and the University of California, Berkeley. She works with the Usable Security and Privacy research group, under the direction of Dr. Serge Egelman. Alisa's research interests include Usable Security and Privacy, Human-Computer Interaction, Choice Architecture, and Behavior Change. Her preferred methodological tools include lab and field experiments, surveys, interviews, and participatory design. She holds a Ph. D. degree in Behavioral and Experimental Economics and Social Sciences from the University of Trento, Italy. Alisa Frik is the corresponding author and can be contacted at: afrik@icsi.berkeley.edu

Dr Alexia Gaudeul is a postdoctoral research associate at the Chair of Behavioral Development Economics of the Faculty of Economic Sciences, Georg-August-Universität Göttingen, Germany. She is an experimental economist with a background in industrial organization. She has done research about the impact of privacy concerns in social network formation, the organization of open-source software development, the impact of complexity and confusion in consumer choice and the dynamics of context effects. She holds a PhD in Economics from the Toulouse School of Economics.