

Frik, Alisa; Gaudeul, Alexia

**Working Paper**

## The relation between privacy protection and risk attitudes, with a new experimental method to elicit the implicit monetary value of privacy

cege Discussion Papers, No. 296

**Provided in Cooperation with:**

Georg August University of Göttingen, Department of Economics

*Suggested Citation:* Frik, Alisa; Gaudeul, Alexia (2016) : The relation between privacy protection and risk attitudes, with a new experimental method to elicit the implicit monetary value of privacy, cege Discussion Papers, No. 296, University of Göttingen, Center for European, Governance and Economic Development Research (cege), Göttingen

This Version is available at:

<https://hdl.handle.net/10419/148055>

**Standard-Nutzungsbedingungen:**

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

**Terms of use:**

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*

**THE RELATION BETWEEN PRIVACY  
PROTECTION AND RISKS ATTITUDES,  
WITH A NEW EXPERIMENTAL METHOD  
TO ELICIT THE IMPLICIT MONETARY  
VALUE OF PRIVACY**

---

Alisa Frik, Alexia Gaudeul

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

# The Relation Between Privacy Protection and Risk Attitudes, with a New Experimental Method to Elicit the Implicit Monetary Value of Privacy

Alisa Frik · Alexia Gaudeul

November 4th, 2016

**Abstract** We investigate the decision of experimental subjects to incur the risk of revealing personal private information to other participants. We do so by using a novel method to generate personal information that reliably induces privacy concerns in the laboratory. We show that individual decisions to incur privacy risk are correlated with decisions to incur monetary risk. We find that partially depriving subjects of control over the revelation of their personal information does not lead them to lose interest in protecting it. We also find that making subjects think of privacy decisions after financial decisions reduces their aversion to privacy risk. Finally, surveyed attitude to privacy and explicit willingness to pay or to accept payment for personal information correlate well with willingness to incur privacy risk. Having shown that privacy loss can be assimilated to a monetary loss, we compare decisions to incur risk in privacy lotteries with risk attitude in monetary lotteries to derive estimates of the implicit monetary value of privacy. The average implicit monetary value of privacy is about equal to the average willingness to pay to protect private information, but the two measures do not correlate at the individual level. We conclude by underlining the need to know individual attitudes to risk to properly evaluate individual attitudes to privacy as such.

**Keywords** privacy · disclosure · risk · control · personal information · experiment

**JEL Classifications** C91 · D81 · O30

---

The authors thank Marco Tecilla for technical assistance, Luigi Mittone, Matteo Ploner, Michele Vescovi, Michele Caraviello, Lorenzo Cordin, Alessandro Acquisti, Caterina Giannetti, Alex Imas, Gerhard Riener and other colleagues and faculty members for valuable comments and feedback that helped us to improve the manuscript. Funding for the doctoral scholarship of Alisa Frik is supported by a fellowship from TIM - Telecom Italia.

---

Alisa Frik

School of Social Sciences, Università degli Studi di Trento, Via Inama 5, 38123, Trento, Italy. TIM – Telecom Italia, SKIL Joint Open Lab (Trento). E-mail: [alisa.frik@unitn.it](mailto:alisa.frik@unitn.it)

Alexia Gaudeul

Faculty of Economic Sciences, Georg-August-Universität Göttingen, Platz der Göttinger Sieben 3, 37073, Göttingen, Germany. E-mail: [alexia.gaudeul@wiwi.uni-goettingen.de](mailto:alexia.gaudeul@wiwi.uni-goettingen.de)

## 1 INTRODUCTION

The inspiration for this paper comes from our dissatisfaction with the currently established methods for assessing the value of privacy. The most popular methods include 1) experiments asking participants for their willingness to pay (WTP) to avoid getting private information revealed to others (alternatively, willingness to accept (WTA) payment to reveal their information), 2) surveys asking respondents for their feelings about a range of possible scenarios involving privacy, and for information about the way they handle various privacy concerns. While indeed suitable for a variety of applications, those methods suffer from two main weaknesses: 1) they are not incentivized (surveys) and 2) they do not correspond to the type of decisions that most people face when thinking about privacy (WTP and WTA experiments). Indeed, it rarely happens in real life to get offered payment for private information or to be asked to pay for information protection from a well identified, immediate and certain threat. Most of the time instead, people have to decide how much to invest to protect their information from a non-specific threat that may or may not be realized in the future and that has uncertain consequences. This means that actual privacy decisions are motivated by a mix of risk aversion and a desire to protect private information. We propose to disentangle those two aspects.

We make three main contributions in this paper:

1. We offer a new method to generate a privacy concern in the laboratory. We ask our subjects to fill a questionnaire about their opinions on a set of controversial, sensitive and socially relevant topics. This method overcomes the disadvantages of other methods used in privacy-related lab experiments, such as measuring and disclosing intelligence test scores, which create a dichotomous division between bad and good types and also suffer from an overconfidence bias. By covering multiple contexts, our questionnaire makes it very likely that at least one issue will be sensitive for an individual and, hence, induce a privacy concern for that individual. Our method does not require that individuals tell the truth about their own opinion. While eliciting information that is sensitive in the laboratory context, the personal information we obtained cannot be misused to damage the subjects materially, which helps overcome legal constraints in the collection, storage, and use of personal information.
2. We test the analogy between standard financial risk attitudes and attitudes to privacy risk in a laboratory setting. We measure privacy attitudes in a context of risk by letting participants decide whether to take part in privacy lotteries, where the loss is a loss of privacy. Namely, we offer participants the option to play privacy lotteries that result in personal information disclosure with a certain probability. We compare decisions in such lotteries with decisions to incur risk in lotteries involving monetary outcomes. We find that attitudes to privacy risk correlate with attitudes to financial risk, as the best predictor for decisions in privacy lotteries is attitude to financial risk. We test this result for robustness by introducing the risk of a privacy shock in one treatment – there might be personal information disclosure regardless of the in-

- dividual's effort to protect it. This does not alter choices in privacy lotteries. We also test this result for an order effect, and find that subjects lose interest in protecting their privacy if preferences in privacy lotteries are elicited after the monetary ones.
3. Based on those findings, we offer a novel methodology of implicit elicitation of equivalent monetary values for one's personal information by comparing choices in monetary and in privacy lotteries. Our two-step indirect elicitation method allows us to obtain implicit monetary values for privacy, corrected for risk preferences in so far as those influence the decision to incur privacy risk. Our method can be applied for any type of private information; it is not limited to the particular type of personal information about opinion on sensitive social topics that we used in our experiment. Indeed, the loss of privacy can be in the financial domain, about health, about one's social network, etc.... Moreover, this method is not limited to the exposure of subjects to a risk of personal information revelation but may be applied to a range of other risks, such as unauthorized sharing with third parties, use of contact details for unsolicited marketing purposes, exposure to fraudulent activity, *etc.* We argue that our method is more suitable than direct and explicit valuation methods for the purpose of accurately evaluating and comparing the perceived dis-utility of privacy risk in various domains, especially when direct elicitation is not feasible or may undermine the validity of the study.

The paper is organized as follows: section 2 reviews related literature and presents our hypotheses; section 3 describes the experimental design and methodology; section 4 provides an analysis of the data and tests of the hypotheses; section 5 provides a discussion and robustness check of our results; section 6 describes our method of estimation of monetary value for privacy; and section 7 summarizes our findings and concludes.

## 2 RELATED WORK AND HYPOTHESES

With the more widespread use of the Internet for a wider range of daily activities, the interest in privacy issues has spread beyond a personal concern, raising a debate about privacy issues from economic, legislative, technological and policy perspectives.

The empirical validation of privacy models, and further elaboration of policies and solutions in terms of regulation, protection, exchange and use of personal information raise a serious measurement challenge: what value does personal information have, to whom, and under what conditions? Two main approaches that researchers took to investigate these issues are surveys and experiments.

A Jupiter Research survey (Leathern, 2002) reported that 36% of US respondents would allow tracking of their Internet activities for a US\$5 discounts. A similar fraction of European respondents agreed to trade their e-mail addresses for money or a chance to win a prize (Symantec, 2015). However, another survey found that 91% of Americans disagree with the statement that "If companies give me a discount, it is a fair exchange for them to collect information about me without my knowing" (Turow et al., 2015, p.

3). Although numerous surveys report high privacy concerns in the general population of both the U.S. and Europe (see [Turow et al., 2015](#); [Madden and Rainie, 2015](#); [Eurobarometer, 2015](#)), the hypothetical questions in surveys and the complexity of privacy attitudes make it difficult for the researchers to quantify the preferences of participants and predict their behavior. [Acquisti et al. \(2016\)](#) remark that stated preferences usually differ from observed behavior and suggest that privacy attitudes are idiosyncratic, subjective, context-dependent, and dynamic, *i.e.* change over time (see also [John et al., 2011](#)).

In order to address issues in quantifying privacy preferences and to estimate the value people assign to their personal information, researchers have turned to experimental and empirical methods. A field experiment of [Beresford et al. \(2012\)](#) elicited an average willingness to accept 1 Euro in discounts in order to provide date of birth and monthly income to an online DVD store. [Gideon et al. \(2006\)](#); [Tsai et al. \(2011\)](#); [Egelman et al. \(2013\)](#) demonstrated that some customers were willing to pay a premium to purchase from privacy protective websites, while [Hann et al. \(2007\)](#) found that “among U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth between US\$30.49 and US\$44.62” (p. 29). Anecdotal evidence in [Grossklags and Acquisti \(2007\)](#) suggests that people accept even small rewards of 25 cents to sell their personal information, but are not ready to spend the same amount for its protection. [Huberman et al. \(2005\)](#), using experimental auctions, found a correlation between trait’s desirability and bid for protection from revelation of information about this trait. For instance, they showed that young people were more likely to reveal their age than the older population (on average, for US\$3.62 and US\$18.05, respectively). Similarly, the higher is the perceived discrepancy between one’s own and the average weight of other subjects, the lower is the willingness to reveal the information about one’s weight. [Benndorf et al. \(2014\)](#) elicit a willingness to sell contact details for 15 Euro and Facebook data for 19 Euro in their incentivized experiment using a DBM mechanism. 10 to 20% of their participants did not want to sell personal information for any price. As one can see even from the limited sample of findings presented above, privacy preferences differ dramatically across individuals and studies.

All those studies ask people directly for their willingness to sell or protect information. However, [Wilson and Brekke \(1994\)](#) claim that explicit measurements may limit the motivation, opportunity, and ability of people to retrieve, translate and report mental contents. Sometimes such contents are even not accessible to introspection. Moreover, subjects are more inclined towards extreme values in explicit measures than in implicit measures ([Schwarz, 1999](#)). In contrast, implicit measures provide an assessment of mental content without intentional deliberate processing and awareness about the relation between derived response and mental content ([Nosek and Greenwald, 2009](#)), and therefore, avoid limitations typical for self-reported estimations ([Nosek et al., 2011](#)). Empirical studies showed that neither of the measuring techniques is “truer” than another ([Banaji et al., 2004](#)), and that both explicit and implicit measures may have a stronger or weaker predictive power in various domains ([Nosek et al., 2011](#)). Therefore, in our study

we develop a new, implicit measurements of personal information (dis)utility but we also elicit the same measurements as previous studies for comparison (*e.g.*, Westin’s Privacy Index, WTA/WTP, general privacy concern). We do not claim to find an absolute value for privacy, but offer a novel experimental approach of eliciting behavior in an incentive compatible way that can be applied in various domains for a better understanding of individuals’ preferences.

To the best of our knowledge, our experiment is the first attempt to test the relation between risk and privacy attitudes in a laboratory setting. [Dinev and Hart \(2006\)](#) found that privacy risks and concerns are closely and positively related. Our first hypothesis is that decisions to protect personal information will be correlated with attitude to risk; participants who are risk-averse in monetary lotteries will also be risk-averse in privacy lotteries.

**Hypothesis 1:** *The willingness to protect personal information from the risk of revelation will increase with aversion to the risk of a monetary loss.*

We will test this hypothesis by checking if there is a correlation between the willingness to protect personal information elicited in privacy lotteries and the risk tolerance level elicited in monetary lotteries. We will test this result for robustness by running a treatment with an unavoidable risk of privacy shock – under the assumption that losing control on the decision to take a privacy risk changes attitudes to that risk. We will also check if the order of elicitation (first monetary risk then privacy risk *vs.* vice versa) primes our subject to think of privacy like a monetary good.

Our second hypothesis is that direct valuation methods and privacy attitudes elicited in surveys will correlate with the willingness to incur a privacy risk.

**Hypothesis 2:** *The willingness to protect personal information from the risk of revelation will increase with WTA/WTP for privacy protection and will correlate with survey measures of privacy attitudes.*

If the above hypotheses are verified, then we will feel justified in deriving an implicit monetary value of privacy by comparing decisions in monetary and privacy lotteries. We will compare this indirect elicited implicit value of privacy, as derived from decisions in our experiment, with directly elicited explicit values of privacy.

### 3 EXPERIMENTAL DESIGN

Subjects were asked to make a sequence of binary choices between safe and risky options. Subjects faced two types of lotteries: *monetary* lotteries that imply changes in monetary outcome; and *privacy* lotteries that imply the disclosure of personal information.

#### 3.1 Personal information

In order to create privacy concern, we combine different sources of data (that we will collectively refer to as *personal information*): *standard* personal information and personal

information that was elicited in the lab. Our standard privacy items were the name and surname of participants. Those remained unknown to others unless the outcome of the experiment was such that the subject had to reveal them at the very end of the experiment. We also took photos of each subject upon arrival in the laboratory. Combined together, those pieces of data can be classified as personally identifiable information according to [McCallister \(2010\)](#). Moreover, from full name and photo one could potentially infer additional information, *e.g.*, gender, age, ethnicity, and sometimes even religious views and health issues (for example, myopia due to the use of eyeglasses).

Our source of private information consisted of answers to a questionnaire (appendix D), with 14 questions about opinion on potentially sensitive or socially relevant topics, such as abortion, illegal immigration, and appropriate methods of birth contraception. This questionnaire was filled in before subjects received instructions about the experiment (appendix F). This personal information was then put under the risk of disclosure in the laboratory experiment.

There is no right or wrong answer in such a survey, and opinions create a “personal image”, potentially exposing differences in opinion among the subjects.<sup>1</sup> The psychological literature states that the fear of being isolated from other people imposes a psychological cost on subjects expressing unpopular opinion (see [Noelle-Neumann, 1974](#); [Kim, 1999](#); [Clemente and Roulet, 2015](#)).<sup>2</sup> Behaviors and opinions that deviate from group’s norms and expectations are also more likely to be ridiculed or even punished by the group ([Griskevicius et al., 2006](#); [Janas and Olson, 2000](#); [Kruglanski and Webster, 1991](#)). As the summary of responses was revealed only in the end of the experiment, uncertainty about the answers of other participants increased the psychological discomfort of expressing an opinion. There was no way to escape the possibility that one’s expressed opinion will conflict with the opinion of a portion of other participants, and this did not depend on whether one’s expressed opinion corresponds to one’s truthfully held opinion. Moreover, since questionnaire questions were presented in the form of multiple choice options rather than open questions, participants did not have opportunity to explain or defend their positions.<sup>3</sup> Therefore, no matter whether the subject answered truthfully or not, the risk of public revelation of the opinions together with name, surname and photo is expected to cause privacy concern.

There are a few other experimental studies that *synthetically* produce personal information for the purpose of investigating privacy attitudes. [Rivenbark \(2012\)](#) used a public good game to endogenously generate valuable private information for further elicitation

<sup>1</sup> Even if a participant did not report a truthful answer, he sent a signal about his type that would contradict the position of people from an opposite group. Intra-class correlation coefficient among answers on preliminary questionnaire equal to 0.56, proving that we managed to achieve this goal with a good level of nonconformity among participants, in the sense that a large proportion of subjects expressed opinions that differed from others. See shares of answers to the preliminary questionnaire, mean and standard deviation in appendix D.

<sup>2</sup> Nonetheless, nonconformity could appear advantageous in certain circumstances, *e.g.*, if subjects attempt to emphasize their uniqueness or individuality (see [Argyle, 1957](#); [Hollander, 1958](#); [Maslach et al., 1985](#); [Snyder and Fromkin, 2012](#), *etc.*).

<sup>3</sup> Indeed, during the experiment several participants raised the question about such a possibility and expressed concern about absence of such.



of values and beliefs. [Grossklags and Acquisti \(2007\)](#) used quiz performance to estimate willingness to sell or protect personal information. [Feri et al. \(2016\)](#) created sensitive information via a logic test score connected to the real name of the participant. The personal information we elicit in the lab is less artificial and more broadly relevant than the synthetic information generated in those experiments. Our method overcomes the disadvantages of using intelligence test scores, which create a dichotomous division between bad and good types and are affected by an overconfidence bias ([Griffin and Varey, 1996](#); [Wallsten, 1996](#)), whereby people have a tendency to believe that they belong to a group with a test score above median. Moreover, our questionnaire covers multiple contexts, thus increasing the probability of capturing an issue that is sensitive for an individual and, hence, of inducing a privacy concern without falling into issues with truth-telling. While eliciting information that is sensitive in the laboratory context, the personal information we obtained cannot be misused to damage the subjects materially, which helps overcome legal constraints in the collection, storage, and use of personal information.

### 3.2 Elicitation method

We elicited risk attitude by asking subjects to make choices between gambles in a variation of multiple price list (MPL) designs that are commonly used in experimental economics. MPLs are easy to understand for participants and are incentive compatible ([Miller et al., 1969](#); [Holt and Laury, 2002](#); [Harrison and Rutström, 2008](#); [Andersen et al., 2006](#)). Subjects were offered 8 lists, each requiring 11 decisions between two options: safe options and risky lotteries (fig. 1). Subjects were asked to indicate the option they preferred to play for every row. The order of MPL menus within each task was randomized across participants.

Fig. 1: Screenshot of one of the MPL menus in the privacy task

TABELLA n. 5	Opzione A		Opzione B
RIGA 1	Ricevi 65 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 2	Ricevi 62 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 3	Ricevi 59 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 4	Ricevi 56 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 5	Ricevi 53 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 6	Ricevi 50 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 7	Ricevi 47 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 8	Ricevi 44 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 9	Ricevi 41 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 10	Ricevi 38 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri
RIGA 11	Ricevi 35 UMS	<input type="radio"/> A <input type="radio"/> B	Ricevi 35 UMS. Ma con una probabilità del 30% i tuoi dati personali verranno divulgate agli altri

PROSEGUI

The option A offered a safe payoff  $x$ , while option B offered an outcome  $y$ , which was decreased by  $c$  with probability  $1 - p$  in monetary tasks. In privacy tasks, outcome  $y$  came with a probability  $1 - p$  of having to disclose private information. We varied option B across tables, while safe payoffs  $x$  in option A was lowered from the top row to the bottom row. According to [Maier and Rüger \(2010\)](#), keeping the probabilities fixed and varying only the outcomes helps to avoid the issue of probability weighting, assumed in standard parametric prospect theory ([Tversky and Kahneman, 1992](#)). Moreover, comparison of numeric outcomes is easier for participants than comparison of event probability. We set  $p = 70\%$  (so the probability of a loss of money or of privacy disclosure equals 30%) because while 50/50 chance is more neutral and rather suitable for monetary lotteries, a 50% probability of personal information disclosure is too high with respect to what may be consistent with real world probabilities of privacy breaches. However, setting  $p$  higher would lead us into a domain of probabilities that are difficult for subjects to grasp intuitively.

**Monetary lotteries:** In the monetary task we presented to subjects menus of choices between safe payoffs  $x$  and lottery  $L$ , while varying payoff  $y$  and the loss  $c$ .  $c$  was either a loss of 10 ECU, 30 ECU, or 50 ECU ( $c = 10, 30$  or  $50$ ), or a gain of 30 ECU ( $c = -30$ ). Payoffs  $x$  varied from slightly above  $y$  to slightly above  $y - c$  if  $c$  was

a loss, and from  $y - c$  to  $y$  if  $c$  was a gain. Appendix H.1 shows MPL menus as they were presented to the subjects. We varied losses and gains to be able to condition our measure of risk aversion for a subject to the level of loss he is facing. This is because we do not know in advance what value a subject attaches to privacy, and we therefore need to consider risk aversion for a range of possible values.

**Privacy lotteries:** In the privacy task, we showed to the subjects the same menus of choices as in monetary lotteries, except that we replaced monetary loss  $c$  with an obligation to reveal private information. That is, in the risky options, subjects got  $y$  ECU, but with probability  $1 - p$  their personal information was disclosed to other participants in the lab. Values of  $x$ ,  $y$ , and  $p$  were the same as in monetary task (see the corresponding MPL menus in appendix H.2).

The proposed risk elicitation technique is not limited to the type of data used in our experiment and can be easily adapted and applied to other kinds of personal information. For example, privacy lotteries could also imply revelation of financial and health information or of information from social network accounts. Our method allows the measurement of the (dis)utility of privacy risk in various domains.

### 3.3 Treatments

We designed two conditions to check robustness to an order effect: in the first, the privacy lotteries appeared prior to the monetary lotteries; in the second, the monetary lotteries appeared before the privacy lotteries. We also ran two treatments to test the effect of control deprivation: in the *basic* treatment the outcome of the experiment depends solely on the choice of the participants, providing them with full control over their personal information; in the *shock* treatment participants faced a risk of privacy shock, *i.e.* probability of revelation of their personal information independently from the choices in the experiment. We discuss those treatments in section 6.

We thus have a  $2 \times 2$  treatment design (basic *vs.* shock, and privacy first *vs.* monetary first). Subjects were assigned to each of the four groups at random. Treatments were implemented as between-subject, so that each participant faced either a situation where the risk of privacy shock was present or absent and either the monetary or the privacy task appeared first. Within-subject analysis allows comparison between the choices of every participant across the two tasks (monetary and privacy lotteries).

### 3.4 Procedure

The experiment was conducted in the Cognitive and Experimental Economics Laboratory between May, 4<sup>th</sup> and June, 8<sup>th</sup> 2015. A total of 148 subjects were recruited for 8 experimental sessions, in groups of 15-21 participants per one-hour session, among undergraduate students at the University of Trento, Italy. Appendix C summarizes the

demographic characteristics<sup>4</sup>. On average subjects obtained 8.83 Euro per person, including a 3.00 Euro participation fee.

When invited to participate, our subjects were not told that the scope of the study was related to privacy. However, they were given an opportunity to decline participation in the experiment after reading instructions for the experiment and the questions of our preliminary opinion questionnaire. The payment of show-up fee was guaranteed independently on that decision. Thus, we controlled for self-selection related to reluctance to respond to the questionnaire or jeopardize privacy. All invited subjects decided to go through with the experiment.

To improve the clarity of decision consequences, we employed the prior incentive system (PRINCE) (Johnson et al., 2015). Instead of picking one of the decisions for payment only at the end of the experiment, we distributed closed envelopes with a description of the real choice situation that will determine an individual's payoff *before* the experiment started.<sup>5</sup> This system makes it more obvious to the participants that any situation might be relevant for them, and which decision is relevant depends on the chance that has already realized at the moment they picked an envelope. Therefore, it was more obvious to participants that they have to consider each decision they make as potentially payoff-relevant. Johnson et al. (2015) claims that PRINCE system improves understanding that the payoff-relevant decision is chosen at random, and gives better reassurance that this is true randomization, *i.e.* that the experimenter is not deceitful. This also makes isolation of each decision “maximally salient” (p. 3) and makes the issue of hedging across decisions (Holt, 1986) less important.

We introduced the risk of privacy shock in the shock treatment by adding 24 envelopes that determined the payoff independently from the choices made in the experiment. Thus, with 21% probability subject would pick up an envelope, which implies sure payoff of 35, 55, 65 or 75 ECU and revelation of personal information, no matter which choice they had made in the tables.<sup>6</sup>

After subjects picked at random an envelope, they entered the laboratory and took their randomly assigned seat. After completion of the preliminary questionnaire subjects read the instructions for the first part of the experiment. Once all participants answered correctly to the control questions (appendix G) they proceeded to the first task of the experiment. After participants finished the first task, they read instructions for the second part of the experiment. Upon completion of the second task participants answered a final questionnaire (appendix E) about the experiment, basic demographic information, attitudes towards privacy, WTA and WTP for personal information, risk, self-disclosure, fairness, and trust.

<sup>4</sup> The demographic characteristics were similar across all sessions.

<sup>5</sup> Decision-makers find it easier to condition on the events determined in the past rather than in the future (see Keren, 1991; Shafir and Tversky, 1992; Cubitt et al., 1998; Hey and Lee, 2005; Bardsley, 2010).

<sup>6</sup> Note, that our design avoids an issue of compound lottery. Since subject picks an envelope at random before the experiment, the presence of privacy shock is determined by the state of the nature. Thus, the only risky decision a subject is free to make is to choose option B in MPL menus instead of safe option A.

At the end of each session subjects came one-by-one to the experimenter’s table and opened their envelopes. The situations described in the envelope were implemented. In the situations, where personal information had to be disclosed to other participants, the subjects stood in front of the audience in the lab, experimenter verified his name and surname from the ID card and announced it aloud. Other participants saw on the screen the personal photo and the answers that subject gave in the preliminary questionnaire. To emphasize the inequality aspect mentioned in section 3.1, we presented the summary of the answers to the preliminary questionnaire in a form of comparison with the fraction of participants who answered in a different way, *e.g.*, “John Smith agrees that it is morally justified to abort after discovering serious disability in the fetus, while 93% of other participants does not agree”.

We now proceed to the description and analysis of the experimental results.

## 4 RESULTS

In total our data set is made out 88 binary choices made by 148 individuals. In 95.86% of cases participants switched from the safe to the risky option in a MPL table only once.<sup>7</sup> They thus demonstrated monotonic preferences across lotteries.

### 4.1 Risk preferences

For our measurements of risk attitude, we calculate the *rate of return* (“*ror*”) required by each subject to take the lottery. A subject who is indifferent between safe payoff  $x$  and monetary lottery  $L = (y, 1 - p; y - c, p)$  requires a rate of return of:

$$ror = \frac{y \cdot p + (y - c) \cdot (1 - p) - x}{x} \quad (1)$$

Expressed another way,  $x \cdot (1 + ror) = y \cdot p + (y - c) \cdot (1 - p)$ .

We use the midpoint of the interval in which a subject switches between the safe and the risky option as our measurement of  $x$ , the certainty equivalent of  $L$ . Adopting the idea that back-and-forth switching behavior could be the result of indifference (see [Andersen et al., 2006](#); [Harrison et al., 2012](#); [Charness et al., 2013](#)), we use the mean value between the lower bound of the first switch and the upper bound of the last switch in MPL table as our estimate of  $x$  in cases where subjects switched more than once.

Table 1 shows that with our choice of monetary lotteries, we are able to obtain an estimate of the risk premium even for very high or low values of *ror*. If a subject never switched in a table then we consider the level of *ror* to be unobserved for that subject in that table. If a subject never chose to play a lottery in any table for any value of the safe alternative then we consider this subject to be infinitely risk-averse. If a subject always chose the lottery rather than any safe option then we consider this subject to be infinitely risk-loving.

<sup>7</sup> This is consistent with proportions of 93.4-94.5% observed by [Holt and Laury \(2002\)](#).

Table 1: Interval estimation of  $ror$  across MPL tables.

MPL table	Range of safe outcomes (in ECU)	Lottery option	Elicitation interval for $ror$
1	46 - 56	Get 55, but Pr=.3 to lose 10	$-7\% < ror < 13\%$
2	38 - 68	Get 65, but Pr=.3 to lose 30	$-18\% < ror < 47\%$
3	30 - 80	Get 75, but Pr=.3 to lose 50	$-25\% < ror < 100\%$
4	35 - 65	Get 30, but Pr=.3 to gain 30	$-32\% < ror < 26\%$

We compute  $\overline{ror}$ , the average  $ror$  by individual. On average, the level of  $\overline{ror}$  was 11%. We find that 127 subjects (86% of the total) were risk averse ( $\overline{ror} > 1\%$ ), 16 subjects (11% of the total) were risk seeking ( $\overline{ror} < -1\%$ ), and 5 subjects (3% of the total) were risk neutral ( $\overline{ror} \in [-1\%, 1\%]$ ). Of the risk averse subjects, 3 subjects (2% of the total) never took any risk ( $\overline{ror} > 100\%$ ). We did not observe any subject always taking a risk ( $\overline{ror} < -32\%$ ).

Those results are consistent with [Holt and Laury \(2002\)](#), which find that about two-thirds of the subjects in their experiments were risk averse when all prizes are below US\$4.00. They note that risk aversion increases when payoffs are scaled up. This explains our higher proportion of risk-averse subjects since the highest possible outcome was 8 Euro in our experiment (plus 3 Euro as show-up fee). We will discuss the dependence of  $ror$  on the magnitude of the loss  $c$  in the lottery in section 7.

#### 4.2 Privacy preferences

We compute an *index of attitude to privacy risk* (“IAPR”) defined as the value that equates the certainty equivalent  $x$  of the lottery and the *expected value* of the lottery,  $y \cdot p + (y - IAPR) \cdot (1 - p)$ , whereby the value of privacy is IAPR. The IAPR is therefore an implicit monetary measure of the (dis)utility of privacy risk:

$$IAPR = \frac{y - x}{1 - p} \quad (2)$$

This value represents the equivalent in monetary terms of the risk of a “loss of privacy” (*i.e.* personal information disclosure). Positive value of the IAPR can be translated into a dis-utility of the risk of personal information disclosure, while negative value of the IAPR can be attributed to the utility of the risk of personal information disclosure (“privacy exhibitionism”). We draw the reader’s attention to the fact that the IAPR is not a monetary equivalent of privacy loss, but of the *risk* of such a loss. In other words, the IAPR takes into account both the value attached to privacy by a subjects and his level of aversion to risk. We explain later how we disentangle the two.

We compute an interval estimate of the value of the IAPR as implied by individual switching points in the MPL menus of the privacy task (table 2). Namely, we use the midpoint of the switching interval as our measurement of  $x$  when subjects switched only

once, and the mean value between the lower bound of the first switch and the upper bound of the last switch in MPL tables when subjects switched more than once. Table 2 shows that with our choice of privacy lotteries, we are able to obtain a value of  $IAPR$  as long as it is no higher than 150 ECU (15 Euro) and no lower than -100 ECU (-10 Euro).

Table 2: Interval estimation of  $IAPR$ , in Experimental Currency Unit (ECU). (1 ECU = 0.1 Euro).

MPL table	Range of safe outcomes	Lottery option	Elicitation interval for the IAPR
5	46 - 56	Get 55, but Pr=.3 of personal information disclosure	$-3 < IAPR < 30$
6	38 - 68	Get 65, but Pr=.3 of personal information disclosure	$-10 < IAPR < 90$
7	30 - 80	Get 75, but Pr=.3 of personal information disclosure	$-17 < IAPR < 150$
8	35 - 65	Get 30, but Pr=.3 of personal information disclosure	$-100 < IAPR < 0$

Of the 148 subjects in our experiment, 49 subjects or about 33% of our sample had a mean value of  $IAPR = 5$  ECU, which corresponds to 0.5 Euro. This value corresponds to the mean IAPR for subjects who consistently preferred a safe payoff to the same safe payoff with a risk of privacy disclosure, but switched to the risky option as soon as the lottery outcome exceeded the safe payoff.  $IAPR = 5$  ECU is therefore the cut-point separating subjects who liked the opportunity of disclosing their information in at least one table from subjects who disliked doing so on average.

In total, 94 subjects (64% of the total) had mean values of IAPR higher than 5 ECU (*privacy protective*), of which 14 never took any privacy risk ( $IAPR > 150$  ECU), 49 subjects (33% of the total) were close to indifferent to the risk of personal information disclosure ( $IAPR = 5$  ECU) and 5 subjects (3% of the total) had a mean value of IAPR lower than 5 ECU (*exhibitionists*). There were no subjects who always chose the risky option ( $IAPR < -100$  ECU). The mean of IAPR for those subjects for which it was measured (90% of the total) was 25 ECU (2.5 Euro).

The majority of our subjects were thus averse to privacy disclosure, a large minority was indifferent and a small minority appeared to enjoy privacy disclosure and was ready to pay for it. This contrasts with WTA and WTP which were all higher than or equal to zero. It might be that subjects did not realize they could express negative values for their WTA or their WTP; future experiments on privacy should be careful to make participants aware that they can also express willingness to pay to disclose personal information rather than assuming that all participants are unwilling to disclose.

With the exception of a few subjects, most of our subjects were not comfortable with personal information disclosure. A substantial number of participants chose safe options in privacy lotteries, demonstrating the presence of privacy concerns. This is

because even though synthetically generated personal information can hardly be misused to harm participants after the end of the study, reputations created on the basis of expressed opinions remains even outside of the lab after the experiment. The salience of conformist opinion was increased by presenting opinions along with statistics on the opinion of peers on the same issue. Together with observed diversity of opinions this served to reinforce privacy concern. We indeed observed some degree of nervousness and anxiety for subjects whose information was eventually disclosed to others in the lab. Many participants also mentioned privacy concerns in the open-ended question of the exit survey.

While the majority of people attributed a positive value to personal information and did tend to protect it from disclosure, we found, as a number of studies suggest, that some people, in contrast, wanted to make their personal information and opinions public. Such differences reflect differences in goals, attitudes personality traits and other factors (see Zywicki and Danowski, 2008; Krasnova et al., 2009; Ross et al., 2009; Correa et al., 2010). This minority tendency to disclose is consistent with the use of social technologies, such as online social networks, blogs, *etc.*, and could be especially prevalent for the active users of such technologies, extensively present in the population of students, and, consequently, in our sample.<sup>8</sup>

## 5 Are individuals who are more risk-averse also less willing to reveal private information?

To test the first hypothesis stated in section 2, we run a first set of interval regression to take account of right-censoring in our data on  $\overline{IAPR}_i$ . The first set of regressions take the following form:

$$\overline{IAPR}_i = \beta_0 + \beta_1 \cdot \overline{ror}_i + \beta_2 \cdot Shock_i + \beta_3 \cdot Order_i + \beta_4 \cdot Table_k + \dots + \epsilon_{ik} \quad (3)$$

where  $\overline{IAPR}_i$  is average  $IAPR$  for individual  $i$  across tables  $k \in [5, 8]$ , except if the individual never switched in any table, in which case we code  $\overline{IAPR}_i > 150$  ECU.  $\overline{ror}_i$  is average  $ror$  for subject  $i$  from his choices in tables  $k \in [1, 4]$  – we include in our regressions a dummy equal to 0 if  $\overline{ror}_i > 100\%$ , 1 else, which we interact with  $\overline{ror}_i$ .  $Shock_i$  takes value 0 for participants assigned to the basic treatment and value 1 for those assigned to the shock treatment;  $Order_k$  takes value 0 if monetary task appeared before privacy task, 1 otherwise;  $Table_k$  is a control for differences in  $IAPR$  across tables.

We also include other variables measuring attitudes to privacy from survey responses. In particular, we use explicit self-reported WTA for privacy disclosure (Q6 in the final questionnaire, appendix E) and WTP for privacy protection (Q7). Socio-demographic indicators include gender, age, field of study, level of education, nationality, parents'

<sup>8</sup> Only about 5% of our participants indicated they were not members of any online social network.



education, size of the locality (city, town, village...) and income level (monthly spending) (Q8 to Q15). Other measures of privacy attitudes include general privacy concern (Q16), experience of privacy invasions (Q21), questions to compute Westin's Privacy Index (Q22, see [Westin, 1968](#)), and questions to compute a self-disclosure index (Q30<sup>9</sup>). Based on [Fogel and Nehmad \(2009\)](#), we also asked how subjects deal with private information online (Q17 to Q20, summarized in an index of online information revelation<sup>10</sup>), the number of their offline and online friends (Q23 and Q25), the online social network they use (Q24)<sup>11</sup>, and their privacy settings in online networks (Q26 to Q29, summarized in index "privacy online"<sup>12</sup>). We also collected other variables related to privacy concerns in the experiment: number of known other participants (Q3), trust in the use of information by the experimenter (Q5), and an index of *conformity* to the opinion of others in the preliminary questionnaire (average percentage of participants who agree with one's opinion). This latter variable is designed to take account of a possible exacerbated privacy concern for those subjects who know or think that their opinion does not fit with the majority. Finally, we elicit general and domain specific risk attitude (Q31 and Q32, summarized in index "risk"<sup>13</sup>) and level of trust in others (Q33 to Q37, summarized in index "trust"<sup>14</sup>).

We also run a second set of regressions using a panel random-effects interval-data regression model where we input the number of safe choices made in privacy risk tables as our dependent variable, and the average number of safe choices made in monetary risk tables instead of  $\overline{ror}_i$  as an independent variable. This regression method allows us to take account of censoring below and above if a subject always chose option A or option B in a given MPL table. This second set of regressions takes the following form:

$$safe\_privacy_{ik} = \beta_0 + \beta_1 \cdot \overline{safe\_monetary}_i + \beta_2 \cdot Shock_i + \beta_3 \cdot Order_i + \beta_4 \cdot Table_k + \dots + \epsilon_{ik} \quad (4)$$

whereby  $safe\_privacy_{ik}$  is the number of safe choices made by individual  $i$  in table  $k$ ,  $k \in [5, 8]$  and  $\overline{safe\_monetary}_i$  is the average number of safe choices made by individual  $i$  in tables  $k$ ,  $k \in [1, 4]$ .

Table 5 shows results of various specifications for our first set of regressions (appendix B). Table 6 shows results of various specifications for the second set of regressions (ap-

<sup>9</sup> The self-disclosure index is computed as sum of a, c, d, f, and i minus b, e, g, h and j.

<sup>10</sup> The index of "online information revelation" is computed using a single-factor measurement model whereby answers to questions Q17 and Q19 are modeled as ordered logit and answers to questions Q18 and Q20 are modeled as logit.

<sup>11</sup> 80% indicated Facebook, so the variable is coded as 1 for Facebook, 0 for others.

<sup>12</sup> In the "privacy online" index, Q26 to Q29 are coded as 1 if a subject answered 1 in Q26, 1 or 2 in Q27, 1 in Q28 and 1 in Q29, and 0 otherwise. We then sum those variables.

<sup>13</sup> The "risk index" is computed using a single-factor measurement model whereby answers to questions Q31 and Q32 are modeled as ordered logit.

<sup>14</sup> The trust index is computed using a single-factor measurement model whereby answers to questions Q33, Q34 and Q35 are modeled as ordered logit and answers to questions Q36 and Q37 are modeled as logit.

pendix B). We first discuss the impact of risk and privacy preferences on the decision to incur privacy risk before discussing treatment and order effects.

Our regressions show that the *ror* measure of aversion to risk in monetary tasks is a significant positive predictor of the *IAPR* measure of aversion to risk in privacy task. We find the same positive significant relation between the number of safe choices made in monetary lotteries and in privacy lotteries. This confirms the first part of our first hypothesis: subjects who are more risk-averse in monetary lotteries are also more risk-averse in privacy lotteries.

We also find that WTA and WTP both predict higher IAPR, whereby the IAPR increases by an average of 0.5 ECU (= 0.05 Euro) for every Euro increase in WTA, and by an average of 2 ECU (= 0.20 Euro) for every Euro increase in WTP. 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. The weak relation with WTA shows that WTA is not only overstated<sup>15</sup> but also less tightly related with observed behavior than WTP. Another factor that independently relates to the IAPR is the experience of a violation of privacy in the past (Q21). Westin’s fundamentalists have significantly higher values of the IAPR under some specifications. The general question about privacy concern Q16 is significantly related to the IAPR in the panel random-effect regressions. The results of our regressions show that none of the socio-demographic questions influences the IAPR or the number of safe choices made, except being a foreigner (non-Italian), which increases the number of safe choices made in privacy lotteries. Those additional findings confirm our second hypothesis: subjects 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.

In terms of contributions of privacy and monetary risk attitudes to explaining attitudes to privacy risk, the McFadden’s pseudo  $R^2$  of our full model is 10.7% for IAPR regressions and 8.9% for safe choice regressions.<sup>16</sup> Of this, about 40% is contributed by measures of risk attitude in monetary lotteries, 40% by the combination of WTA and WTP, and the rest by survey measures of privacy attitudes and socio-demographic variables.<sup>17</sup>

Overall, therefore, attitudes to privacy risk do not appear to fundamentally differ from attitudes to monetary risk: 1) subjects 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 also less likely to take a risk in privacy lotteries, in the same way as they are less likely to take

<sup>15</sup> WTA observed in our experiment is 8 times higher than WTP, which is in line with the 7.17 mean WTA/WTP ratio found by Horowitz and McConnell (2002) across 45 studies about a variety of goods. Grossklags and Acquisti (2007) reports ratios between 4 and 36 times depending on type of information (quiz results, weight, favorite vacation destination, and number of sexual partners). For a review, see Horowitz and McConnell (2002); Roth (2006).

<sup>16</sup> McFadden’s pseudo  $R^2$  compare the log-likelihood  $LL_0$  of the null model with only an intercept to the log-likelihood  $LL_{Full}$  of the full model:  $R^2 = 1 - LL_{Full}/LL_0$ .

<sup>17</sup> We measure contribution as the percentage of the difference in log-likelihood between the null model and the full model that is achieved by a model with the respective variable alone. An alternative measure of contribution is by considering by how much the log-likelihood decreases when removing one variable. In that case, the contribution of the measure of monetary risk attitude is lower.

risk when potential losses are higher. 2) subjects who are more risk averse when faced with monetary lotteries are also more risk averse when faced with privacy lotteries, which is also consistent with privacy having a monetary equivalent. We discuss this hypothesis further in section 6, where we measure the effect of our shock treatment and how the order of elicitation affects preferences.

While we do find some correlation between WTA/WTP and the IAPR or number of safe choices in privacy tasks in our regressions, and while this correlation is robust to a number of regression specifications, this pattern holds only in the aggregate. Indeed, we find large divergences between WTA and WTP at the individual level, and wide discrepancies between those values and the IAPR. Different measures of aversion to private information disclosure are certainly not always consistent at the individual level; many individuals behave in ways that are inconsistent with their expressed WTA and WTP. In other words, implicit and explicit measures do not always coincide, even though they do correlate at the aggregate level.

Our results should not be interpreted to mean that subjects who are more risk-averse have a higher utility for personal information. Indeed, *IAPR* is only a way to index decisions in privacy lotteries, and does not take into consideration risk-tolerance levels. It is not an estimate of a subject's utility of personal information. It reflects both value for personal information and readiness to take risk in lotteries (and possibly some other factors, *e.g.*, loss aversion). The true value for privacy of a risk averse subject is lower than *IAPR*. We offer later a method to retrieve monetary values of privacy corrected for risk aversion but we first check that the relation between monetary and privacy risk aversion is robust across treatments.

## 6 Treatment effects

Before trying to retrieve monetary values of privacy from decisions under risk, we need to check that behavior under privacy risk is of the same nature as behavior under monetary risk. Indeed, it is not at all obvious that subjects deal with privacy risk in the same way as with monetary risk. We were particularly concerned about the issue of control over private information. Prior research has indeed identified control or the lack thereof as an important driver of risk attitudes and behaviors (Weinstein, 1984; Harris, 1996; Slovic, 2000; Nordgren et al., 2007). It could be that privacy has worth only in so far as one has got control over its probability of disclosure. Suppose indeed that you know that whatever you do, your private information is at risk of being revealed. Then you have to mentally anticipate this disclosure and prepare for it. Avoiding having to anticipate privacy disclosure may be a large part of why some people are averse to privacy risk. Therefore, forcing our subjects to have to anticipate privacy disclosure might reduce their willingness to protect their information. One can make opposite arguments however. Some subjects may have a maximum allowable level of risk they are ready to take with their private information, and may therefore take more care to protect their information if it is already under risk so as not to exceed this threshold.

In order to settle the question, we therefore test the effect of depriving participants of control over their personal information in a complementary treatment.

As an additional robustness check we also tested whether the order of elicitation of attitudes to monetary and privacy risk had an effect on subjects' decisions. Indeed, asking subjects first about monetary risk and then about privacy risk may induce them to think of a loss of privacy in the same way as of a monetary loss, so we need to check whether the correlation between attitudes to monetary and privacy risk also holds when privacy risk attitudes are elicited first.

### 6.1 Loss of control

Control over personal information flows is often seen in the privacy literature as a prerequisite for privacy protection (*e.g.*, Kang, 1998; Solove, 2006). A Madden and Rainie (2015) survey found that while 74% of Americans thought that control over personal information is very important, only 9% of them believed they had such control. Online social networks have moved towards providing a more granular control over privacy settings to their users, which seems to be a response to their privacy concerns. However, a “control paradox” arises, whereby higher perceived control over personal information can lead to a decline in concerns about privacy and an increase in information disclosure, even when the associated risks are very high (John et al., 2011; Brandimarte et al., 2013). Using dynamic lotteries in a lab experiment, Feri et al. (2016) found that subjects were less likely to disclose their personal information after receiving a breach notification, which jeopardized their personal information. Unlike Feri et al. (2016), which focused on the dynamic effect of breach notifications, we focus on differences between treatments with and without the possibility of a privacy shock. Furthermore, instead of measuring subjects' willingness to sell their personal information, we look into their willingness to take the risk of revealing it.

In our experiment, we therefore test the effect of reducing control over the release of personal information by introducing the possibility of a “privacy shock” (probabilistic disclosure of personal information, even when the participant always chose the safest option in privacy lotteries). We compare treatments with the possibility of such a shock to treatments where participants can guarantee through their decisions that no revelation of private information will occur. We look at the number of safe choices and IAPR taking into account all individual decisions and controlling for individual effects. Neither the panel regression of the number of safe choices nor the regression on IAPR in appendix B, nor the tests on the cumulative distribution function of safe choices and IAPR by treatment show any treatment effect.<sup>18</sup>

<sup>18</sup> Tests of the difference in the number of safe choices: two-sample Wilcoxon rank-sum test:  $\text{Prob} > |z| = 0.84$ ; t-test:  $\Pr(|T| > |t|) = 0.9996$ ; Kolmogorov-Smirnov equality-of-distributions test: corrected p-value is 0.99; ANOVA: coefficient is -0.0002,  $P > |t| = 1.00$ ; Kruskal-Wallis equality-of-populations rank test:  $\text{Prob} = 0.84$ .  $N = 592$  (268 and 324 in shock and basic treatments, respectively). Statistical power is 0.05.

Tests of the difference in IAPR: two-sample Wilcoxon rank-sum test:  $\text{Prob} > |z| = 0.41$ ; t-test:  $\Pr(|T| >$

Thus, we conclude that the introduction of a privacy shock does not lead people to change their attitude towards protection of personal information. In other words, even when complete control over personal information is taken away, whereby one introduces a risk of information disclosure that is independent of one's choices, people keep on considering the level of risk that remains under their control in the same way as if they had full control over whether to incur this risk.

## 6.2 Order effect

Theories of selective information processing state that focus on a primary task reduces attention to a secondary task (Kahneman, 1973). If the monetary lotteries are presented prior to the privacy ones, subjects could keep their focus on monetary outcomes and calculation of expected values, "learned" from the monetary lotteries, when making decisions in the privacy lotteries. In this case, due to selective attention, the emphasis on monetary values could drive away attention to the evaluation of personal information utility. The latter could be even perceived as irrelevant for decision-making when the monetary context is set up in advance (Broadbent, 1957, 1982; Pashler and Sutherland, 1998; Dukas, 2004; Lachter et al., 2004).

In contrast, playing privacy lotteries first could draw more attention to the personal information (dis)utility. Moreover, the time delay between generation of personal information by answering the sensitive questions, and putting these responses under risk of disclosure, is shorter when the privacy lotteries are played right after the completion of the preliminary questionnaire rather than in the second part of the experiment. Adjerid et al. (2013) found that even 15-second delay between demonstration of privacy notice and disclosure decisions was sufficient to distract participants and mute the risk perception.

To test the order effect we consider the number of safe choices and IAPR across different ordering of monetary and privacy tasks in the experiment. Statistical tests and cumulative distribution function show a significant order effect in privacy task: subjects made more safe choices in the privacy lotteries and had higher IAPR when privacy tasks appeared before the monetary tasks.<sup>19</sup> A similar effect is observed also in terms of the percentage of subjects who took only safe alternative in privacy tables (20% when

---

$|t| = 0.91$ ; Kolmogorov-Smirnov test: corrected p-value is 0.79; ANOVA: coefficient is -0.30,  $P > |t| = 0.91$ ; Kruskal-Wallis rank test: Prob=0.41. N=375 (171 and 204 in shock and basic treatments, respectively). Estimated statistical power is 0.05.

<sup>19</sup> Tests of the difference in the number of safe choices: two-sample Wilcoxon rank-sum test: Prob  $> |z| = 0.01$ ; t-test:  $\Pr(T < t) = 0.01$ ; Kolmogorov-Smirnov equality-of-distributions test: corrected p-value is 0.04; ANOVA: coefficient is 0.77,  $P > |t| = 0.02$ ; Kruskal-Wallis equality-of-populations rank test: Prob=0.01. N=592 (312 and 280 in monetary and privacy tasks first conditions, respectively). Estimated statistical power is 0.66.

Tests of the difference in IAPR: two-sample Wilcoxon rank-sum test: Prob  $> |z| = 0.028$ ; t-test:  $\Pr(T < t) = 0.03$ ; Kolmogorov-Smirnov equality-of-distributions test: corrected p-value is 0.10; ANOVA: coefficient is 5.53,  $P > |t| = 0.06$ ; Kruskal-Wallis equality-of-populations rank test: Prob=0.03. N=375 (206 and 169 in monetary and privacy tasks first conditions, respectively). Estimated statistical power is 0.45.

privacy task first *vs.* 12% when monetary task first).<sup>20</sup> The proportion of people who behaved as if they had close to zero value for privacy – switching to the risky choice as soon as its payoff was higher than the safe choice – was significantly lower when privacy lotteries appeared first than when monetary lotteries appeared first (25% *vs.* 36%, respectively).<sup>21</sup> One of the possible explanations is that doing the monetary task first could prime people to consider personal information in the same terms as money, while doing the privacy task first induces people to think about personal information in a different way that translates into more privacy risk aversion.

While cumulative distribution function and statistical tests show that values of the IAPR are greater when privacy task appears first, coefficients on this condition dummy in regressions (appendix B) are not consistently significant. However, we find that the relation between the IAPR and *ror* is stronger when privacy task appeared first (fig. 5b in appendix A).<sup>22</sup> This suggests that in the condition where the privacy task was presented before the monetary one, the decision in privacy task was largely driven by risk attitudes, while risk aversion played a smaller role when the privacy task was presented after the monetary task. In the latter case, the attention of participants may have been drawn to monetary outcomes rather than to risk evaluation or privacy concerns.

## 7 Implicit monetary values for privacy

We showed that risk attitudes are of a similar nature in the monetary and the privacy context; subjects react to the risk of a privacy loss in ways that are consistent with privacy loss being of the same nature as a monetary loss. We can therefore estimate monetary values of privacy by taking account of the risk tolerance level that was elicited in the monetary task. Since we elicited both monetary and privacy risk aversion, we can disentangle risk preferences from the (dis)utility of personal information disclosure.

Willingness to take risk depends both on how large relative variation in payoffs are in the lottery (standard deviation  $\sigma$ ) and on whether the lottery involves gains or losses. In our menu of lotteries, there is a linear relation between  $\sigma$  and  $|c|$  – standard deviation in lottery outcomes increases linearly with the absolute value of the loss/gain  $c$  – so we can simply replace the relation between *ror* and  $\sigma$  with a relation between *ror* and  $|c|$  to take into account standard deviation. As for differences in risk attitude when faced with gains *vs.* when faced with losses, a visual inspection of individual *ror* as a function of  $c$  reveals that *ror* increases with  $c$ , the size of the loss (fig. 2). A regression of *ror* on  $c$  and  $|c|$ , whereby  $ror(c) = ror_\alpha \cdot |c| + ror_\beta \cdot c$  gives out an estimate of average  $ror_\alpha = 1.96\%$

<sup>20</sup> Excluding MPL table 4, proportion test  $\Pr(Z < z) = 0.01$ . Pearson  $\chi^2(1) = 5.32$  ( $\Pr = 0.021$ ). Estimated power is 0.63.

<sup>21</sup> Two-sample test of proportions:  $\Pr(Z > z) = 0.00$ . Estimated power is 0.83.

<sup>22</sup> Results from regressions confirm that there is no significant relation between *ror* and the IAPR if monetary lotteries are presented first, while the relation is significant if privacy lotteries are presented first.

and  $ror_\beta = 3.47\%$  ( $N = 534$ ,  $R^2 = 57\%$ ,  $F(2, 532) = 353$ ,  $p < 1\%$ ).<sup>23</sup> This implies that subjects require a rate of return that increases by  $3.47 + 1.96 = 5.43\%$  for each additional unit of loss ( $c > 0$ ), and *decreases* by  $3.47 - 1.96 = 1.51\%$  for each additional unit of gain ( $c < 0$ ). Subjects are thus risk-loving, on average, when faced with a lottery that involves gains, while they are risk averse when faced with a lottery that involves losses of the same magnitude. This is predicted by prospect theory when, as in our case, probabilities of loss or gain are low (Tversky and Kahneman, 1992).

We can therefore obtain per-subject estimates of  $ror$  for different possible levels of valuation of privacy by estimating individual by individual a regression of the form  $ror(c) = ror_\alpha \cdot |c| + ror_\beta \cdot c$ .<sup>24</sup> Consider thus an individual with level of risk aversion represented by the couple  $(ror_\alpha, ror_\beta)$ . Suppose this individual is indifferent between safe payoff  $x$  and a risky option with payoff  $y$  and a probability  $1 - p$  of personal information disclosure. Then, for this individual, privacy loss is equivalent to a monetary loss of magnitude  $v_p$  such that  $x \cdot (1 + ror_\alpha \cdot |v_p| + ror_\beta \cdot v_p) = y \cdot p + (y - v_p) \cdot (1 - p)$ .

Solving for  $v_p$ , the implied equivalent monetary loss (or gain) from personal information disclosure corrected with risk attitude is thus<sup>25</sup>:

$$v_p = \frac{y - x}{1 - p + x \cdot (ror_\alpha + ror_\beta)} \text{ if } v_p > 0 \quad (5)$$

$$v_p = \frac{y - x}{1 - p + x \cdot (-ror_\alpha + ror_\beta)} \text{ if } v_p < 0 \quad (6)$$

Our method for correcting the IAPR with  $ror$  to obtain a value of privacy  $v_p$  has the advantage of being able to easily condition the level of  $ror$  on the level of  $v_p$ . The value of  $v_p$  can differ significantly from the value of the IAPR. Indeed, unwillingness to take a risk of personal information disclosure may be due to either high risk aversion or high dis-utility from such disclosure. We saw that aversion to privacy risk and aversion to monetary risk were positively related, but as figure 5 shows, there are a number of individuals with high monetary risk aversion and low privacy risk aversion, and vice-versa. There are many participants with the same aversion to privacy risk but they have distinct risk attitudes, and therefore will have different values of  $v_p$ . A subject who values privacy positively but has a high level of risk aversion (high  $ror_\alpha$  and  $ror_\beta$ ) will have lower value of  $v_p$  than a subject who also values privacy positively but is less risk-averse.

Using formula 5, we obtain values of average individual  $v_p$  that are distributed more smoothly than the uncorrected average IAPR (fig. 3). Average individual  $v_p$  is 1.50 Euro, compared with an average WTP of 1.92 Euro and an average WTA of 16.12 Euro. The

<sup>23</sup> We do not want to allow for a constant in such regressions as then we would have  $ror(0) \neq 0$  which implies requiring a return on an asset with no risk. Allowing a constant in our regressions does not change the results and the constant is not significantly different from zero.

<sup>24</sup> This is subject however to having individual estimates of  $ror$  when the lottery implies a gain and when the lottery implies a loss. If not, then either  $ror_\alpha$  or  $ror_\beta$  is set equal to 0.

<sup>25</sup> Those formulas imply that it is possible theoretically that we would obtain values of  $v_p$  that are positive if we assume  $v_p$  is positive, and negative if we assume that  $v_p$  is negative. This happens however only for one subject with our data. In that case, we assume that  $v_p$  is positive if  $y - x$  is positive and vice-versa.



distribution of values of  $v_p$  is also more consistent with those of WTP than with those of WTA.

We identify 4 individuals with negative values of privacy, compared with 126 with positive values for privacy. This does not include the 14 individuals who never took privacy risks, neither does this include 3 individuals who never took monetary risk, both type of individual for whom only a lower bound (resp. upper bound) estimate of  $v_p$  is available. Our estimates of  $v_p$  show that there are individuals with implicit negative values of privacy (see fig. 3). This implies that enjoying revelation of private information may occur, at least in our sample and given our method for generating private information.

We find no significant correlation between estimates of  $v_p$ , those of WTA and those of WTP. The lack of consistency is surprising given that WTA and WTP were elicited after the experiment was finished, so the subjects had had time to evaluate their attitude to privacy. This underlines again the difficulty for people to give direct monetary equivalents for something like privacy which is not generally experienced as being a tradable good. Welfare evaluations of the impact of privacy losses should therefore not be based on valuations derived from direct elicitation of WTP or WTA payment for private information disclosure. Rather, they should be elicited, like in this experiment, indirectly and in such a way that one can retrieve implicit monetary equivalents from similar decisions involving money rather than privacy. We showed in this experiment that at least in the case of information about opinion on sensitive social topics, people seemed to behave when faced with privacy risk in similar ways as they behaved when faced with monetary risk, thus allowing us to compute monetary equivalents of the value of privacy.

We test our estimates of  $v_p$  for robustness by measuring risk aversion levels when assuming that our subjects have a CRRA utility function  $u(x) = x^r$  and when assuming that our subjects have a CARA utility function  $u(x) = 1 - e^{-\alpha x}$ . Given a risk aversion coefficient  $r$  in the CRRA case, we obtain  $v_p = y - (\frac{x^r - p \cdot y^r}{1-p})^{1/r}$ . Given a risk aversion coefficient  $\alpha$  in the CARA case, we obtain  $v_p = y - \ln(\frac{e^{-\alpha x} - p \cdot e^{-\alpha y}}{1-p})^{-1/\alpha}$ . Estimates of  $v_p$  with those alternative methods are consistent and very highly correlated with our main estimates.

## 8 CONCLUSION

We presented novel methods for (1) the generation of privacy concerns in a laboratory setting, (2) the elicitation of the (dis)utility of the risk personal information disclosure, and (3) the disentangling of risk attitudes from privacy attitudes in decisions involving risk of personal information revelation. We found that implicit and explicit measures of the value of privacy differ substantially. Implicit elicitation technique may help to avoid the expressions of socially desirable answers and beliefs, thus revealing the true preferences of the subjects.



We ran a laboratory experiment with 148 subjects and collected 13,024 observations on choices made between sure monetary payoff and lotteries of two types. Lotteries in monetary domain served to elicit monetary risk preferences, while privacy lotteries elicited willingness to protect from disclosure the personal information that included name, surname, photo, and responses to the preliminary questionnaire about opinion on sensitive and socially relevant topics. Additionally we manipulated the order in which monetary and privacy lotteries were presented to the subjects and the level of control they had over personal information by introducing privacy shocks in the form of a chance of eventual personal information disclosure regardless of the choices made. We applied the prior incentive system to provide transparent and tangible economic incentive (Johnson et al., 2015).

We found a consistent positive relationship between monetary and privacy risk aversion. This supports the idea that willingness to protect personal information may be driven at least in part by risk aversion rather than only, or even mainly, by differences in values for personal information and privacy attitudes. This may also serve as an explanation of the privacy paradox: when people take risks of personal information revelation even though they express high levels of privacy concerns, this may be due to their high level of risk tolerance rather than being an inconsistency. When asked about their privacy attitude or WTP/WTa for privacy, people respond both based on their value for privacy and their attitude to risk. This is why it is very important to know individual attitude to risk in order to properly evaluate individual attitudes to privacy as such.

We also found that the introduction of a privacy shock, under which personal information was compromised independently of the choices of participants, did not affect the willingness to take risk in privacy tasks. Taking control over privacy away from participants did not either encourage or discourage them from protecting it. Finally, we found qualified support for the existence of an order effect, whereby presenting privacy lotteries prior to monetary ones leads to a more privacy-protective behavior. We interpret this to mean that either privacy attitudes are affected by an immediacy effect (subjects make more privacy protective decisions right after answering private questions), or that thinking about financial risk first leads subjects to think of privacy in monetary terms, thus possibly leading to less risk averse behavior. This finding may find application in the creation of privacy policies, in the timing of privacy decisions and in the design of personal data marketplaces. Emphasizing monetary benefits before asking for privacy-related choices may lead to higher disclosure. Conversely, asking for privacy choices first may result in more protection of one's personal data.

Our proposed elicitation method can be applied to different types of private data that could allow future research to compare the inferred (dis)utility of privacy risk in various domains, for example, towards financial, health, social network and other personal information. The method is also applicable to various types of privacy risk, *e.g.*, sharing data with third parties, hacking attacks, use of personal information for marketing purposes and unsolicited advertising, *etc.*

To the best of our knowledge, ours is the first work trying to separate two determinants of attitudes to privacy risk - basic willingness to disclose personal information and risk aversion. We found many risk-averse people who were comparatively ready to take risks with personal information disclosure. This indicates that they were actually quite willing to disclose this information. Indeed, for a risk-averse person to take a decision that is risky for his privacy, the willingness to disclose his personal information should be high enough to outweigh his general tendency to avoid risk. In contrast, people with a high value for personal information (and thus large dis-utility from its disclosure) should love risk enough to “convince” them to expose their privacy to risk. This observation suggests that many choices that aim to protect privacy may be mistakenly attributed to a concern about personal information disclosure, while in fact being driven by general risk aversion. Such mistaken attribution would lead to inaccurate evaluations of the (dis)utility of personal information disclosure. Indeed, correction with risk attitude in our study reveals the existence of some people who are “privacy exhibitionists”, *i.e.* subjects with negative utility for personal information. This subset of people does not appear when considering other measures. Privacy researchers should make sure that their methods to elicit attitudes to privacy risk allow for the expression of preferences consistent with privacy exhibitionism.

## References

- Acquisti, A., Taylor, C. R., and Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 52(2):442–492. [4](#)
- 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*, pages 9:1–9:11. ACM. [19](#)
- Andersen, S., Harrison, G. W., Lau, M. I., and Rutström, E. E. (2006). Elicitation using multiple price list formats. *Experimental Economics*, 9(4):383–405. [7](#), [11](#)
- Argyle, M. (1957). Social pressure in public and private situations. *Journal of Abnormal and Social Psychology*, 54(2):172–175. [6](#)
- Banaji, M. R., Nosek, B. A., and Greenwald, A. G. (2004). No place for nostalgia in science: A response to Arkes and Tetlock. *Psychological Inquiry*, 15(4):279–310. [4](#)
- Bardsley, N. (2010). *Experimental economics: Rethinking the rules*. Princeton University Press. [10](#)
- Benndorf, V., Normann, H.-T., et al. (2014). *The willingness to sell personal data*. Düsseldorf Institute for Competition Economics (DICE). [4](#)
- Beresford, A. R., Kübler, D., and Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters*, 117(1):25–27. [4](#)
- Brandimarte, L., Acquisti, A., and Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science*, 4(3):340–347. [18](#)
- Broadbent, D. E. (1957). A mechanical model for human attention and immediate memory. *Psychological Review*, 64(3):205–215. [19](#)
- Broadbent, D. E. (1982). Task combination and selective intake of information. *Acta Psychologica*, 50(3):253–290. [19](#)
- Charness, G., Gneezy, U., and Imas, A. (2013). Experimental methods: Eliciting risk preferences. *Journal of Economic Behavior & Organization*, 87:43–51. [11](#)
- Clemente, M. and Roulet, T. J. (2015). Public opinion as a source of deinstitutionalization: A “spiral of silence” approach. *Academy of Management Review*, 40(1):96–114. [6](#)
- 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*, 26(2):247–253. [14](#)
- Cubitt, R. P., Starmer, C., and Sugden, R. (1998). On the validity of the random lottery incentive system. *Experimental Economics*, 1(2):115–131. [10](#)
- Dinev, T. and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1):61–80. [5](#)
- Dukas, R. (2004). Causes and consequences of limited attention. *Brain, Behavior and Evolution*, 63(4):197–210. [19](#)
- Egelman, S., Felt, A. P., and Wagner, D. (2013). Choice architecture and smartphone privacy: There’s a price for that. In *The Economics of Information Security and*

- Privacy*, pages 211–236. Springer. 4
- Eurobarometer (2015). Data Protection. Special Eurobarometer 431, Eurobarometer. Available at: <https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf>. 4
- Feri, F., Giannetti, C., and Jentzsch, N. (2016). Disclosure of personal information under risk of privacy shocks. *Journal of Economic Behavior & Organization*, 123:138–148. 7, 18
- Fogel, J. and Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1):153–160. 15
- Gideon, J., Cranor, L., Egelman, S., and Acquisti, A. (2006). Power strips, prophylactics, and privacy, oh my! In *Proceedings of the Second Symposium on Usable privacy and security*, pages 133–144. ACM. 4
- Griffin, D. W. and Varey, C. A. (1996). Towards a consensus on overconfidence. *Organizational Behavior and Human Decision Processes*, 65(3):227–231. 7
- Griskevicius, V., Goldstein, N. J., Mortensen, C. R., Cialdini, R. B., and Kenrick, D. T. (2006). Going along versus going alone: When fundamental motives facilitate strategic (non) conformity. *Journal of Personality and Social Psychology*, 91(2):281–294. 6
- Grossklags, J. and Acquisti, A. (2007). When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In *Proceedings of the Sixth Workshop on the Economics of Information Security (WEIS'07)*, pages 7–18. 4, 7, 16
- 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*, 24(2):13–42. 4
- Harris, P. (1996). Sufficient grounds for optimism?: The relationship between perceived controllability and optimistic bias. *Journal of Social and Clinical Psychology*, 15(1):9–52. 17
- Harrison, G. W., Lau, M. I., Rutström, E. E., and Tarazona-Gómez, M. (2012). Preferences over social risk. *Oxford Economic Papers*, 65(1):25–46. 11
- Harrison, G. W. and Rutström, E. E. (2008). *Risk Aversion in the Laboratory*, volume 12, chapter Risk Aversion in Experiments, pages 41–196. Emerald Group Publishing Limited. 7
- Hey, J. D. and Lee, J. (2005). Do subjects separate (or are they sophisticated)? *Experimental Economics*, 8(3):233–265. 10
- Hollander, E. P. (1958). Conformity, status, and idiosyncrasy credit. *Psychological Review*, 65(2):117–127. 6
- Holt, C. A. (1986). Preference reversals and the independence axiom. *American Economic Review*, 76(3):508–515. 10
- Holt, C. A. and Laury, S. K. (2002). Risk aversion and incentive effects. *American Economic Review*, 92(5):1644–1655. 7, 11, 12
- Horowitz, J. K. and McConnell, K. E. (2002). A review of WTA/WTP studies. *Journal of Environmental Economics and Management*, 44(3):426–447. 16

- Huberman, B. A., Adar, E., and Fine, L. R. (2005). Valuating privacy. *IEEE Security & Privacy*, 3(5):22–25. 4
- Janes, L. M. and Olson, J. M. (2000). Jeer pressure: The behavioral effects of observing ridicule of others. *Personality and Social Psychology Bulletin*, 26(4):474–485. 6
- John, L. K., Acquisti, A., and Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, 37(5):858–873. 4, 18
- Johnson, C. A., Baillon, A., Bleichrodt, H., Li, Z., Van Dolder, D., and Wakker, P. P. (2015). Prince: An improved method for measuring incentivized preferences. SSRN Working Paper 2504745. 10, 23
- Kahneman, D. (1973). *Attention and effort*. Englewood Cliffs, NJ: Prentice-Hall. 19
- Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review*, pages 1193–1294. 18
- Keren, G. (1991). Calibration and probability judgements: Conceptual and methodological issues. *Acta Psychologica*, 77(3):217–273. 10
- Kim, S.-H. (1999). Opinion expression as a rational behavior. In *Annual Meeting of the Association for Education in Journalism and Mass Communication, New Orleans*. 6
- Krasnova, H., Kolesnikova, E., and Guenther, O. (2009). "It won't happen to me!": Self-disclosure in online social networks. *Amcis 2009 Proceedings*. Paper 343. 14
- Kruglanski, A. W. and Webster, D. M. (1991). Group members' reactions to opinion deviates and conformists at varying degrees of proximity to decision deadline and of environmental noise. *Journal of Personality and Social Psychology*, 61(2):212–225. 6
- Lachter, J., Forster, K. I., and Ruthruff, E. (2004). Forty-five years after Broadbent (1958): Still no identification without attention. *Psychological Review*, 111(4):880–913. 19
- Leathern, R. (2002). Online privacy: Managing complexity to realize marketing benefits. *Jupiter Research*, 17. 3
- Madden, M. and Rainie, L. (2015). Americans' attitudes about privacy, security and surveillance. Report, Pew Research Center. 4, 18
- Maier, J. and Rüger, M. (2010). Measuring risk aversion model-independently. Munich Discussion Paper No. 2010-33, Ludwig-Maximilians-Universität München. 8
- Maslach, C., Stapp, J., and Santee, R. T. (1985). Individuation: Conceptual analysis and assessment. *Journal of Personality and Social Psychology*, 49(3):729–738. 6
- McCallister, E. (2010). *Guide to protecting the confidentiality of personally identifiable information*. Diane Publishing. 6
- Miller, L., Meyer, D. E., and Lanzetta, J. T. (1969). Choice among equal expected value alternatives: Sequential effects of winning probability level on risk preferences. *Journal of Experimental Psychology*, 79(3p1):419–423. 7
- Noelle-Neumann, E. (1974). The spiral of silence a theory of public opinion. *Journal of Communication*, 24(2):43–51. 6
- Nordgren, L. F., Van Der Pligt, J., and Van Harreveld, F. (2007). Unpacking perceived control in risk perception: The mediating role of anticipated regret. *Journal of*

- Behavioral Decision Making*, 20(5):533–544. [17](#)
- Nosek, B. A. and Greenwald, A. G. (2009). (Part of) the case for a pragmatic approach to validity: Comment on De Houwer, Teige-Mocigemba, Spruyt, and Moors. *Psychological Bulletin*, 135:373–376. [4](#)
- Nosek, B. A., Hawkins, C. B., and Frazier, R. S. (2011). Implicit social cognition: From measures to mechanisms. *Trends in Cognitive Sciences*, 15(4):152–159. [4](#)
- Pashler, H. E. and Sutherland, S. (1998). *The psychology of attention*, volume 15. MIT press Cambridge, MA. [19](#)
- Rivenbark, D. R. (2012). Valuing the risk from privacy loss: Experimentally elicited beliefs explain privacy behavior. Working Paper, University of Central Florida, Orlando, FL. [6](#)
- Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., and Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in Human Behavior*, 25(2):578–586. [14](#)
- Roth, G. (2006). *Predicting the Gap between Willingness to Accept and Willingness to Pay*. PhD thesis, Ludwig-Maximilians-Universität München. [16](#)
- Schwarz, N. (1999). Self-reports: how the questions shape the answers. *American Psychologist*, 54(2):93–105. [4](#)
- Shafir, E. and Tversky, A. (1992). Thinking through uncertainty: Nonconsequential reasoning and choice. *Cognitive Psychology*, 24(4):449–474. [10](#)
- Slovic, P. E. (2000). *The perception of risk*. Earthscan publications, London. [17](#)
- Snyder, C. R. and Fromkin, H. L. (2012). *Uniqueness: The human pursuit of difference*. Springer Science & Business Media. [6](#)
- Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, pages 477–564. [18](#)
- Symantec (2015). The state of privacy. Report, Symantec. Available at: <https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf>. [3](#)
- 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):254–268. [4](#)
- Turow, J., Hennessy, M., and Draper, N. (2015). The trade off fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Working Paper, The Annenberg School for Communication, University of Pennsylvania. [3](#), [4](#)
- Tversky, A. and Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, 5(4):297–323. [8](#), [21](#)
- Wallsten, T. S. (1996). An analysis of judgment research analyses. *Organizational Behavior and Human Decision Processes*, 65(3):220–226. [7](#)
- Weinstein, N. D. (1984). Why it won’t happen to me: perceptions of risk factors and susceptibility. *Health Psychology*, 3(5):431–457. [17](#)
- Westin, A. F. (1968). *Privacy and freedom*. Atheneum, New York. [15](#)

- 
- Wilson, T. D. and Brekke, N. (1994). Mental contamination and mental correction: unwanted influences on judgments and evaluations. *Psychological Bulletin*, 116(1):117–142. [4](#)
- Zywica, J. and Danowski, J. (2008). The faces of Facebookers: Investigating social enhancement and social compensation hypotheses; predicting Facebook and offline popularity from sociability and self-esteem, and mapping the meanings of popularity with semantic networks. *Journal of Computer-Mediated Communication*, 14(1):1–34. [14](#)

## A Summary statistics

	$\overline{ror}$	$\overline{IAPR}$	$\overline{v_P}$	WTA	WTP
Min	-11%	-1.17	-0.64	0	0
Max	41%	12.50	11.51	200	30
Mean	11%	2.52	1.50	16.12	1.92
Std. deviation	10%	2.89	1.87	25.33	4.85
N	145	134	130	144	146

Table 3: Measures of risk aversion (in %) and (dis)utility of personal information disclosure (in Euros)

Note: Outliers for WTA and WTP (values that are 2 standard deviations away from the mean) are excluded. Before exclusion WTA and WTP range between 0 Euro and 1000 Euro.

	By treatment		By condition		Total
	Basic	Shock	Monetary first	Privacy first	
$\overline{ror}$					
Mean	10%	12%	10%	12%	11%
Std. deviation	10%	11%	10%	11%	10%
Observations	80	65	78	67	145
$\overline{IAPR}$					
Mean	2.53	2.52	2.25	2.85	2.52
Std. deviation	2.91	2.88	2.71	3.08	2.89
Observations	73	61	73	61	134
$\overline{v_P}$					
Mean	1.53	1.47	1.51	1.49	1.50
Std. deviation	1.80	1.98	1.49	1.38	1.88
Observations	72	58	72	58	130

Table 4: Explicit and implicit measures of (dis)utility of personal information disclosure and privacy risk, in Euros.



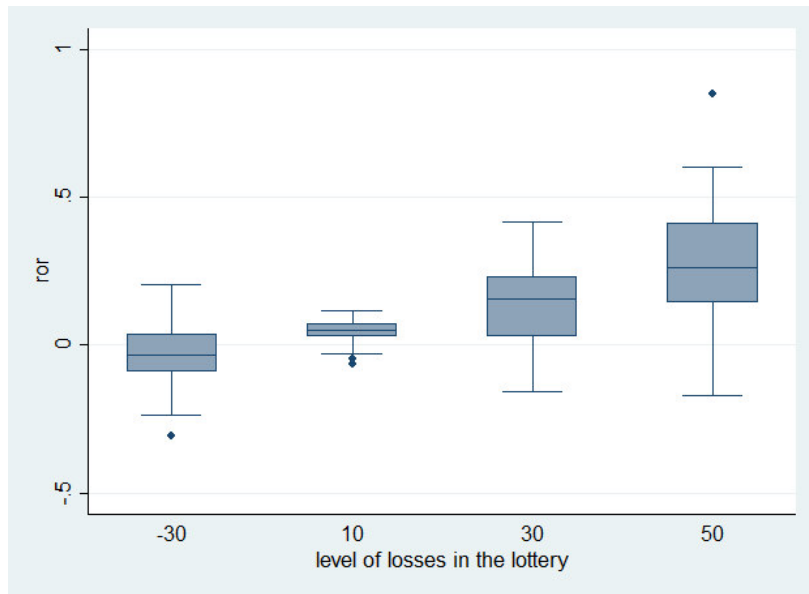


Fig. 2: Boxplot of the individual level of *ror* by level of loss in monetary lotteries.

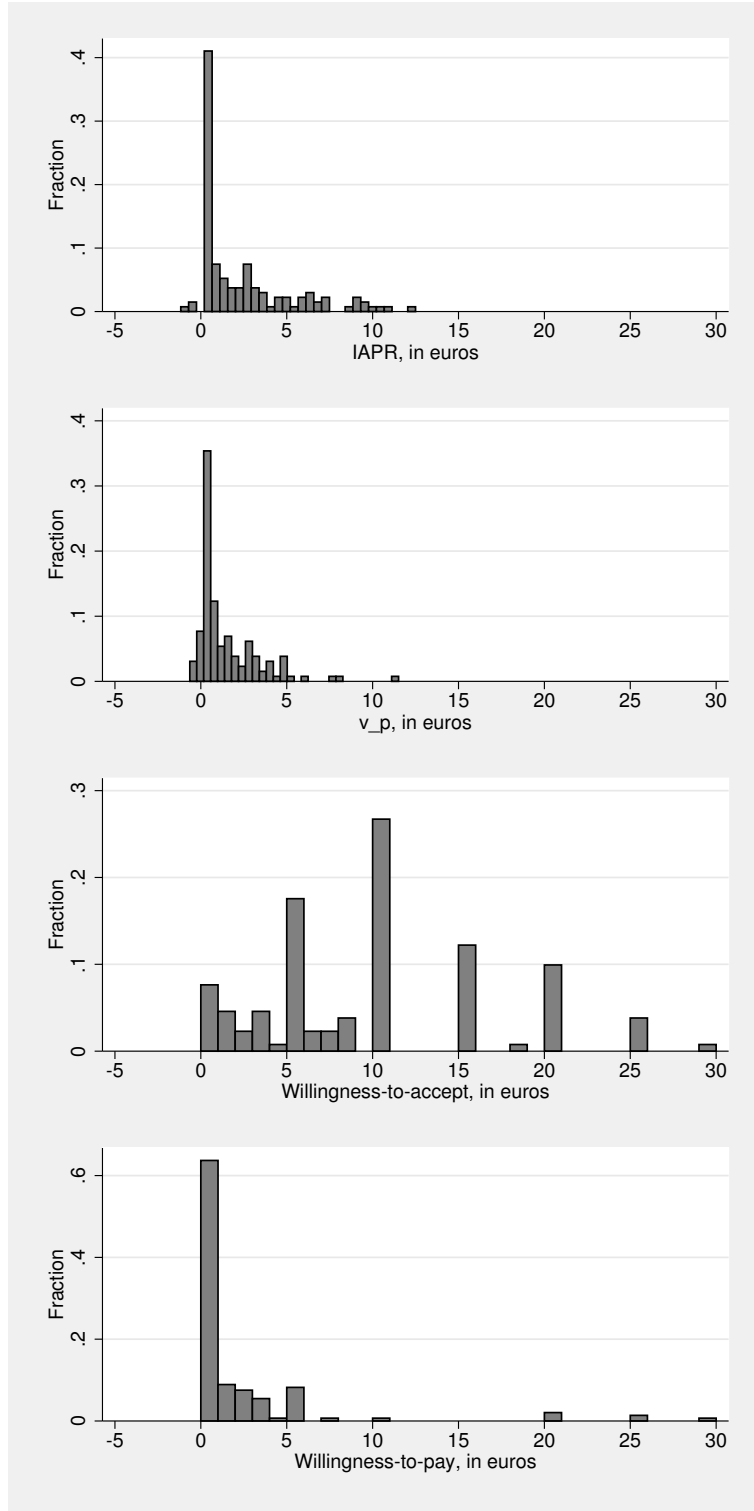


Fig. 3: Distribution of explicit and implicit measures of (dis)utility of personal information disclosure

Note: Outliers (values that are 2 std. deviations away from the mean) are not shown.

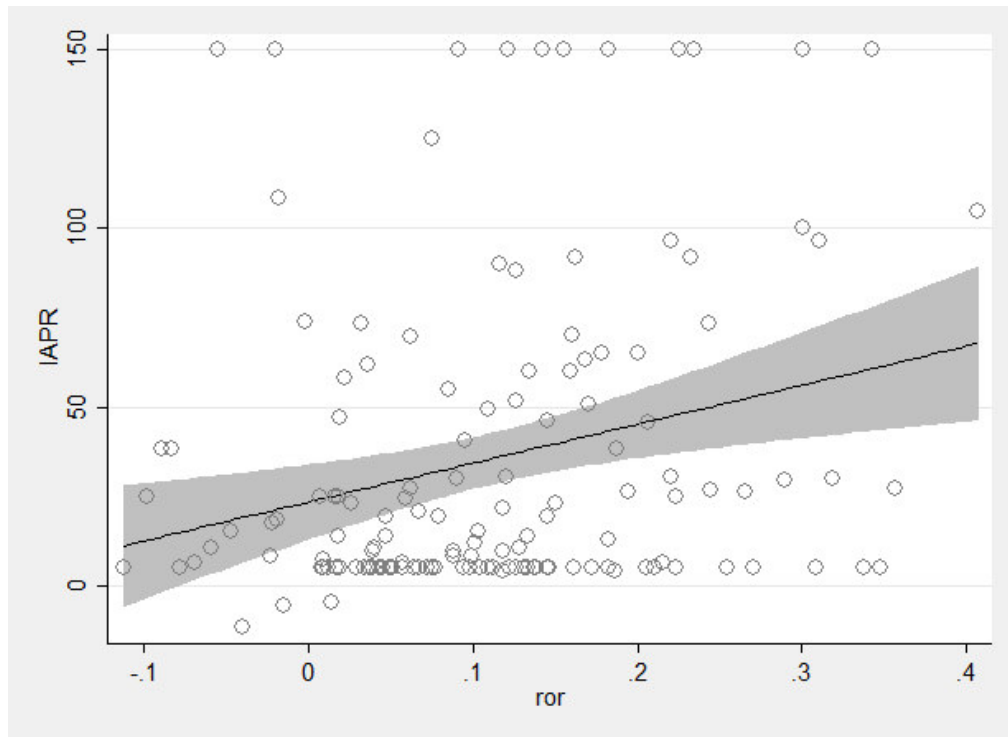
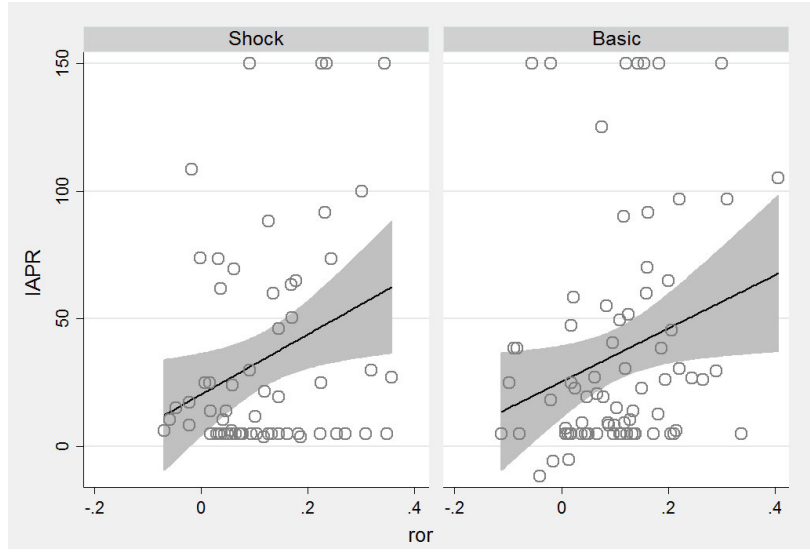


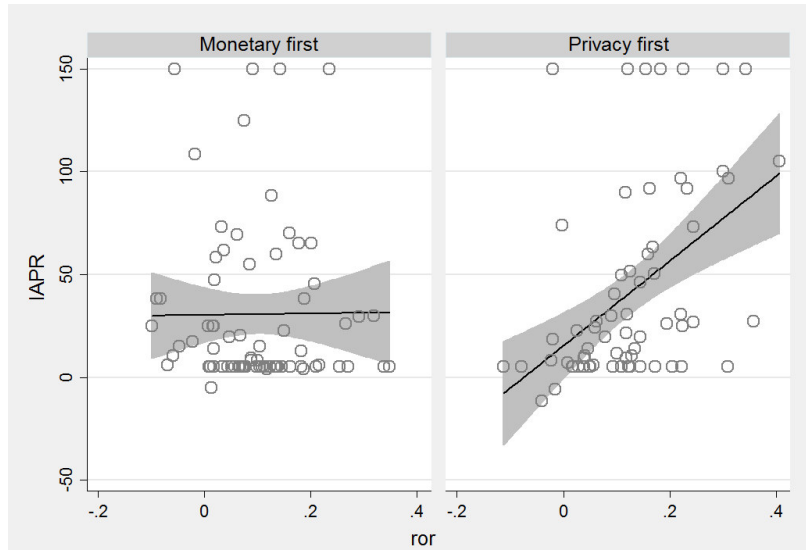
Fig. 4: Scatterplot of individual average values of *ror* and of *IAPR*.

Subjects with values of *IAPR* > 150 *ECU* are shown as having *IAPR* = 150.

We show prediction lines of linear regressions and 95% confidence interval.



(a) By treatment



(b) By order of elicitation

Fig. 5: Scatterplot of  $\overline{ror}$  and (dis)utility of privacy risk,  $\overline{IAPR}$ , by treatment and by order of elicitation

Subjects with values of  $IAPR > 150$  ECU are shown as having  $IAPR = 150$ .

We show prediction lines of linear regressions and 95% confidence interval.

## B Regressions

Table 5: Interval regression of  $\overline{IAPR}_i$  over  $\overline{ror}_i$ .

Model	(1)	(2)	(3)	(4)	(5)
$\overline{ror}_i$	116.62** [42.63,190.62]	113.62** [39.21,188.02]	127.33*** [54.70,199.96]	122.54*** [50.27,194.81]	118.53*** [48.13,188.93]
$\overline{ror}_i > 100$	109.76*** [49.29,170.23]	106.08*** [44.92,167.25]	67.47* [10.01,124.93]	67.91* [9.89,125.93]	75.08* [12.79,137.36]
Treatment with privacy shock		-4.47 [-19.81,10.86]	-11.65 [-25.87,2.56]	-12.44+ [-26.88,2.00]	-12.88+ [-27.62,1.86]
Condition with privacy elicited first		8.11 [-7.36,23.58]	3.19 [-11.51,17.89]	5.50 [-9.22,20.23]	-1.47 [-15.95,13.01]
Q3: Nr of participants known			-1.81 [-7.27,3.64]	-1.03 [-6.77,4.71]	0.20 [-5.91,6.31]
Q5: Trust in experimenters			-6.63 [-58.31,45.05]	-16.45 [-68.94,36.03]	-1.78 [-63.95,60.39]
WTA			0.53** [0.21,0.86]	0.52** [0.20,0.85]	0.59*** [0.27,0.92]
WTP			1.72* [0.25,3.20]	2.17* [0.45,3.88]	2.38** [0.62,4.14]
Q16: General privacy concern			7.28+ [-0.93,15.50]	5.42 [-3.06,13.90]	6.12 [-2.39,14.64]
Index of online information revelation (Q17-Q20)			5.02 [-4.18,14.22]	3.01 [-6.28,12.29]	-2.53 [-12.10,7.03]
Q21: Victim of invasion of privacy			17.40* [0.30,34.50]	14.93+ [-2.85,32.70]	22.06* [4.02,40.11]
Q22: Westin's pragmatist			-4.01 [-21.06,13.05]	-3.53 [-20.92,13.85]	-1.33 [-18.77,16.10]
Q22: Westin's fundamentalist			11.23 [-8.89,31.35]	15.44 [-5.92,36.80]	30.97** [9.06,52.89]
Index for privacy settings online (Q26-Q29)			-4.51 [-12.85,3.82]	-3.30 [-11.89,5.28]	1.36 [-7.64,10.35]
Q30: Index of self-disclosure			1.23 [-0.75,3.21]	1.01 [-1.00,3.02]	0.81 [-1.26,2.89]
Index of conformity in preliminary questionnaire			-1.69 [-120.53,117.16]	-8.12 [-128.38,112.14]	-21.86 [-146.45,102.74]
Index of risk attitude (Q31-Q32)				-4.42+ [-9.22,0.38]	-6.56* [-11.63,-1.50]
Index of trust (Q33-Q37)				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	23.88*** [12.67,35.09]	22.47** [8.10,36.83]	8.88 [-75.89,93.64]	7.83 [-77.93,93.58]	-55.72 [-157.99,46.54]
Socio-demographic controls	No	No	No	No	Yes
N	148	148	143	140	140
of which right-censored	14	14	13	13	13
log likelihood	-725.56	-724.83	-685.57	-668.16	-655.90
LR $\chi^2$ (degrees of freedom)	19*** (2)	21*** (4)	51*** (16)	55*** (20)	80*** (39)

95% confidence intervals in brackets

+  $p < 0.1$ , \*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

Table 6: Panel random-effects interval-data regression, number of safe choices in privacy lotteries by table.

Model	(1)	(2)	(3)	(4)	(5)	(6)
Safe choices in monetary lotteries	0.632*** [0.29,0.98]	0.659*** [0.30,1.02]	0.617** [0.24,0.99]	0.530** [0.17,0.89]	0.489** [0.13,0.85]	0.517** [0.18,0.86]
Table 6		-1.332*** [-1.81,-0.86]	-1.332*** [-1.81,-0.86]	-1.321*** [-1.81,-0.83]	-1.356*** [-1.85,-0.86]	-1.358*** [-1.86,-0.86]
Table 7		-1.799*** [-2.27,-1.33]	-1.800*** [-2.27,-1.33]	-1.795*** [-2.28,-1.31]	-1.840*** [-2.34,-1.35]	-1.841*** [-2.34,-1.35]
Table 8		9.500*** [8.70,10.30]	9.498*** [8.70,10.30]	9.498*** [8.68,10.32]	9.427*** [8.59,10.26]	9.426*** [8.59,10.26]
Treatment with privacy shock			-0.226 [-1.44,0.99]	-0.791 [-1.90,0.32]	-0.843 [-1.97,0.28]	-1.070+ [-2.20,0.06]
Condition with privacy elicited first			0.701 [-0.53,1.94]	0.255 [-0.92,1.43]	0.449 [-0.73,1.62]	-0.0883 [-1.22,1.04]
Q3: Nr 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]
WTA				0.0434*** [0.02,0.07]	0.0434*** [0.02,0.07]	0.0483*** [0.02,0.07]
WTP				0.134* [0.02,0.25]	0.168* [0.03,0.30]	0.164* [0.03,0.30]
Q16: Generally privacy concern				0.721* [0.09,1.36]	0.599+ [-0.06,1.25]	0.781* [0.13,1.43]
Index of online information revelation (Q17-Q20)				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]
Index for privacy settings online (Q26-Q29)				-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]
Index of risk attitude (Q31-Q32)					-0.292 [-0.67,0.08]	-0.472* [-0.86,-0.08]
Index of trust (Q33-Q37)					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	3.231** [0.78,5.68]	1.672 [-0.92,4.27]	1.737 [-0.86,4.33]	2.705 [-4.69,10.10]	2.956 [-4.50,10.41]	-1.400 [-9.81,7.01]
Socio-demographic controls	No	No	No	No	No	Yes
N observations	592	592	592	572	560	560
of which left-censored	5	5	5	5	5	5
of which right-censored	212	212	212	204	201	201
N individuals	148	148	148	143	140	140
log likelihood	-1386	-1030	-1030	-982	-959	-944
Wald $\chi^2$ (degrees of freedom)	13*** (1)	810*** (4)	812*** (6)	803*** (18)	776*** (22)	802*** (41)

95% confidence intervals in brackets

+  $p < 0.1$ , \*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$

## C Summary of answers to the post-experimental questionnaire

	Mean	SD	Min	Max
<b>Part A: About the experiment</b>				
Q2. Ease of understanding (0 very difficult, 3 not difficult at all)	2.14	0.61	0	3
Q3. Number of known other participants Share which knew another participant (s)	1.28 66%	1.31	0	5
Q4. Appropriate remuneration (0 No, 1 Yes)	70%			
Q5. Trust experimenters (0 No, 1 Yes)	97%			
Q6. WTA, Euro	36.2	142	0	1000
WTA excluding outliers, Euro	16.1	25.4	0	200
Q7. WTP, Euro	10	83.7	0	1000
WTP excluding outliers, Euro	1.92	4.85	0	30
<b>Part B: Demographics</b>				
Q8. Males	66%			
Q9. Age				
18-25 years	94%			
26-30 years	6%			
Q10. Field of study: Social sciences, 82%, Technical sciences, 10%, Humanities and Arts, 5%, Natural sciences, 1%, Other 1%				
Q11. Education level: Secondary education 82% Bachelor's degree 15% Master's degree 3%				
Q12. Italians	93%			
Q13. Parents completed secondary education: None of the parents 16% One of the parents 25% Both parents 59%				
Q14. Size of city (inhabitants): > 1 million, 3% 100 001 - 1 000 000, 16% 10 001 - 100 000, 49% 1 001 - 10 000, 28% < 1 000, 4%				
Q15. Expenses per month: < Euro500, 43% Euro501-800, 41% Euro801-1200, 11% Euro1201-2000, 1% >Euro2000, 0% No answer, 4%				
<b>Part C: Privacy preferences, activities in online social networks and self-disclosure</b>				
Q16. General privacy concern (0 not concerned at all, 3 very concerned)	1.12	.90	0	3
Q17. Willingness to provide Personal Identifying Information ("PII") to websites (0 very willing, 4 not willing at all)	2.68	.91	0	4
Q18. Provide PII to websites if compensated (0 No, 1 Yes)	57%			
Q19. Willingness to provide information about tastes, interests and preferences to websites (0 very willing, 4 not willing at all)	1.57	1.18	0	4
Q20. Provide information about tastes, interests and preferences if compensated (0 No, 1 Yes)	86%			
Q21. Victim of privacy invasion (0 No, 1 Yes)	34%			

	Mean	SD	Min	Max
Q22. Westin's Privacy Index				
Unconcerned	44%			
Pragmatist	28%			
Fundamentalist	28%			
Q23. Number of close friends offline	6.37	4.79	1	30
Q24. Primary online social network (POSN)				
Facebook, 80%, Google+, 2%, Twitter, 1%, Pinterest, 1%, LinkedIn, 1%, Instagram, 10%,				
Not a member, 5%				
Q25. Number of connections in POSN	545	488	0	3200
Q26. Name in POSN (if use)				
Real name	94%			
Pseudonym, and nobody knows who I am in real life	2%			
Pseudonym, but everybody knows who I am in real life	4%			
Q27. Profile picture in POSN (if use)				
Real photo	74%			
Real photo with other people	19%			
Photo of other person	2%			
Image of non human being	4%			
No photo at all	1%			
Q28. Privacy settings in POSN (if use)				
Public	13%			
Private	57%			
Mostly public	11%			
Mostly private	19%			
Q29. Changed privacy settings in POSN (if use)				
Never	15%			
Immediately after registration	34%			
Several times	48%			
After misuse	3%			
Other	1%			
Q30. Self-disclosure index	-1.86	3.61	-13	10
<b>Part D: Attitudes to risk and trust</b>				
Q31. General risk attitude (0 averse, 10 risk seeking)	5.91	1.6	1	10
Q32. Risk attitude in: (0 averse, 10 risk seeking)				
Driving	3.6	2.66	0	10
Finance	4.28	2.31	0	10
Sports	6.69	2.18	0	10
Career	4.63	2.34	0	10
Health	3.03	2.65	0	10
Trusting strangers	4.41	2.54	0	10
Q33. Trust people (0 agree, 3 disagree)	1.6	.71	0	3
Q34. Cannot rely on people (idem)	1.82	.72	0	3
Q35. Should not trust strangers (idem)	.85	.65	0	3
Q36. People try to be fair (0 No, 1 Yes)	33%			
Q37. People follow their own interests (idem)	83%			



## D Preliminary questionnaire on opinions about potentially sensitive and socially relevant topics

This questionnaire is translated from the Italian original. We show options that were offered to participants and the percentage of participants who chose each option.

1. Experimentation of medications on animals can have an important implication for development of drugs for humans and is often distressing and fatal for animals. Are you in favor or against medical experiments on animals?  
(a) 0. In favor - 72%; 1 Against - 28%
2. Using genetically modified organisms in agriculture can help to fight hunger in the world and can present a great danger to ecosystem. Are you in favor or against implementation of such agricultural practices?  
(a) 0. In favor - 46%; 1 Against - 54%
3. Which of the following is the more appropriate penalty for rape?  
(a) 0. Death - 1%; 1. Chemical castration - 34%; 2. Life imprisonment - 35%; 3. Prison sentence, less than life imprisonment - 30%
4. Albeit rare, there are observed cases of serious complications as consequences of vaccination. The choice not to undergo vaccination significantly increases the risk of getting and transmitting potentially dangerous diseases. Are you in favor or against obligatory vaccination?  
(a) 0. In favor - 83%; 1. Against - 17%
5. Billions of Euros are spent each year for aerospace research. Do you think that this money should or should not be spent in other way?  
(a) 0. Should - 52%; 1. Should not - 48%
6. Would you for any reason read your mate's email, SMS or pose as him/her online, without his/her knowledge and permission?  
(a) 0. Yes, they shouldn't be keeping secrets anyway - 14%; 1. Yes, I'd be too curious not to - 6%; 2. Yes, if I suspected them of something - 35%; 3. Never - 45%
7. Do you think it is morally justified or not justified to abort after discovering serious disability in the fetus?  
(a) 0. Justified - 58%; 1. Not justified - 42%
8. Are you in favor or against legislation of prostitution?  
(a) 0. In favor - 82%; 1. Against - 18%
9. Which of following substances should be prohibited? (More than one answer is allowed)  
(a) Alcohol - 3%  
(b) Tobacco - 7%  
(c) Cannabis - 22%  
(d) Cocaine - 85%  
(e) Acids (LSD, ecstasy, etc.) - 82%  
(f) Heroin - 89%  
(g) None - 9%
10. Are you in favor or against adoption of children by homosexual couples?  
(a) 0. In favor - 56%; 1. Against - 44%
11. Are you in favor or against the closure of Italian borders as a solution for the problem of illegal immigration?  
(a) 0. In favor - 25%; 1. Against - 75%
12. Are you in favor or against euthanasia (i.e. the painless killing of a patient suffering from an incurable and painful disease or in an irreversible coma)?  
(a) 0. In favor - 84%; 1. Against - 16%
13. Some people believe that the trails left by aircrafts in the sky contain chemicals that are inserted specifically to influence the population. Do you think this is a plausible theory or not?  
(a) 0. Plausible - 10%; 1. Not plausible - 90%

14. Which of the following methods of birth contraception do you consider as the most appropriate?
  - (a) 0. Hormonal (oral pills, implants, injections, patches, etc.) - 26%;
  - (b) 1. Barrier (condoms, cervical caps, diaphragms, sponges with spermicide, etc.) - 67%;
  - (c) 2. Intrauterine devices - 1%;
  - (d) 3. Sterilization (surgical or chemical) - 3%;
  - (e) 4. Behavioral (interrupted intercourse, fertility awareness method based on the menstrual cycle, sexual abstinence) - 2%;
  - (f) 5. None - 1%

## E Final questionnaire

1. What do you think was the purpose of the experiment?
2. How difficult was it for you to make a decision? (1. Very difficult, 2. Somewhat difficult; 3. Not very difficult; 4. Not difficult at all)
3. Please, indicate how many of today's participants you knew before the experiment? If you did not know anybody in the lab please write zero.
4. Do you think that the remuneration for the experiment is appropriate? (1. Yes; 2. No)
5. Do you trust that experimenters will not misuse the personal information you gave in this experiment? (1. Yes; 2. No)
6. Suppose that you do not have to reveal your private information at the end of the experiment, but the experimenter offers you money so that your name, surname, photo, and answers to the preliminary questionnaire are shown to other participants. What is the minimum amount (in Euros) that you would be ready to accept for this?
7. Suppose that you have to reveal your private information at the end of the experiment, but you can pay the experimenter so that your name, surname, photo, and answers to the preliminary questionnaire are not shown to other participants. What is the maximum amount (in Euros) that you would be ready to pay for this?
8. What is your gender? (1. Male; 2. Female)
9. What is your age? (1. < 18 years; 2. 18-25 years; 3. 26-30 years; 4. 31-35 years; 5. 36-40 years; 6. 41-45 years; 7. 46-50 years; 8. 51-55 years; 9. 56-60 years; 10. > 61 years)
10. What is your field of study? (1. Social Sciences (Economics, Sociology, Law, etc.); 2. Technical sciences (Informatics, Engineering, Architecture, etc.); 3. Medical sciences (Medicine, Nursing, Pharmaceutics, etc.); 4. Humanities and Arts (Literature, Languages, Arts, etc.); 5. Natural Sciences (Chemistry, Physics, Mathematics, etc.); 6. Education science and pedagogics; 7. Agriculture (Agriculture, Veterinary, etc.); 8. Other applied sciences (specify))
11. What is the highest level of education you have completed up to now? (1. Secondary education; 2. Bachelor's Degree; 3. Master's Degree; 4. PhD; 5. Other (specify))
12. What is your nationality? (1. Italian; 2. Other (specify))
13. Did your parents complete their secondary education? (1. None of my parents completed secondary education; 2. Only one of my parents completed secondary education; 3. Both parents completed secondary education)
14. Where did you live for most part of your life? (1. Big city with population > 1 million inhabitants; 2. City with 100.001 - 1.000.000 inhabitants; 3. City with 10.001 - 100.000 inhabitants; 4. Town with 1.000 - 10.000 inhabitants; 5. Village with < 1.000 inhabitants)
15. How much do you spend every month? (including food, clothes, rent, utilities (heating, water), education, entertainment, etc.) (1. < 500 Euro; 2. 501-800 Euro; 3. 801-1200 Euro; 4. 1201-2000 Euro; 5. > 2000 Euro; 6. No answer)
16. Are you generally concerned about your privacy? (1. Not concerned at all; 2. Somewhat unconcerned; 3. Somewhat concerned; 4. Very concerned)
17. How willing are you to provide personally identifiable information and demographics to websites in general? (1. Very willing; 2. I would not mind; 3. I am indifferent; 4. Not very willing; 5. Not willing at all)

18. Would you be more willing to provide personally identifiable information and demographics to websites in general if you were compensated for your information? (1. Yes; 2. No)
19. How willing are you to provide information about your tastes, interests and preferences without personal identification to websites in general? (1. Very willing; 2. I would not mind; 3. I am indifferent; 4. Not very willing; 5. Not willing at all)
20. Would you be more willing to provide personal information about your tastes, interests and preferences to websites in general if you were compensated for your information? (1. Yes; 2. No)
21. Have you personally been the victim of what you felt was an invasion of privacy? (1. Yes; 2. No)
22. Please indicate to which extent you (dis)agree with the following statements (1. Strongly agree; 2. Somewhat agree; 3. Somewhat disagree; 4. Strongly disagree):
  - (a) Consumers have lost all control over how personal information is collected and used by companies
  - (b) Most businesses handle the personal information they collect about consumers in a proper and confidential way
  - (c) Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today
23. Currently in your life, how many close friends would you say you have?
24. If you are a member of online social networks, which do you use the most actively? (The online social network chosen in this questions will be called *your primary social network* hereinafter) (1. Facebook; 2. Google +; 3. Twitter; 4. My Space; 5. Instagram; 6. LinkedIn; 7. FourSquare; 8. Other (specify); 9. I am not a member of any online social network)
25. How many connections do you have in your primary social network? (Write zero if you are not a member of any online social network)
26. What do you use as your user name in your primary social network? (1. Real name; 2. Pseudonym, and nobody knows who I am in real life; 3. Pseudonym, but everybody knows who I am in real life; 4. I am not a member of any online social network)
27. What do you use as profile picture in your primary social network? (1. Real photo of me; 2. Real photo of me with other person/people; 3. Photo of other person or celebrity; 4. Photo/image of non human being; 5. No photo at all; 6. I am not a member of any online social network; 7. Other (specify))
28. What are your privacy settings in your primary social network? (1. Public. Everybody can get access to my profile and read my entries; 2. Private. Only my friends can get access to my profile and read my entries; 3. My profile and entries are mostly public and partially private; 4. My profile and entries are mostly private and partially public; 5. I have different accounts for public and private entries; 6. I am not a member of any online social network; 7. Other (please describe in details))
29. Did you ever change your privacy settings in primary social network? (1. Never; 2. I changed privacy settings immediately after registration; 3. I changed privacy settings several times; 4. I changed privacy settings after someone misused my personal information; 5. I am not a member of any online social network; 6. Other (please describe in details))
30. Please, read the following statements and using the scale below rate how accurately each statement describes **you**, as you generally are now, not as you wish to be in the future. Apart from being anonymous, your responses will be kept in absolute confidence. (1. Very Inaccurate; 2. Moderately Inaccurate; 3. Neither Inaccurate nor Accurate; 4. Moderately Accurate; 5. Very Accurate)
  - (a) I am open about myself.
  - (b) I don't talk a lot.
  - (c) I disclose my intimate thoughts.
  - (d) I show my feelings.
  - (e) I reveal little about myself.
  - (f) I talk about my worries.
  - (g) I bottle up my feelings.
  - (h) I prefer to deal with strangers in a formal manner.
  - (i) I act wild and crazy.
  - (j) I have little to say.

31. How do you see yourself: Are you generally a person who is fully prepared to take risks or do you try to avoid taking risks? Please, indicate a number on the scale from 0 to 10, where the value 0 means: *Unwilling to take risks* and the value 10 means *Fully prepared to take risk*.
32. In different areas you can behave differently too. How would you assess your risk tolerance with respect to the following areas (please, indicate a number on the scale from 0 to 10, where the value 0 means: *Unwilling to take risks* and the value 10 means *Fully prepared to take risk*).
  - (a) in car driving
  - (b) in financial matters
  - (c) in leisure and sports
  - (d) in you professional career
  - (e) in your health
  - (f) in trusting strangers
33. "In general, one can trust people ..." (1. I totally agree; 2. I somewhat agree; 3. I somewhat disagree; 4. I totally disagree)
34. "Nowadays one cannot rely on anyone ..." (1. I totally agree; 2. I somewhat agree; 3. I somewhat disagree; 4. I totally disagree)
35. "When dealing with strangers it's better to be careful before trusting them..." (1. I totally agree; 2. I somewhat agree; 3. I somewhat disagree; 4. I totally disagree)
36. Do you think that the majority of people... (1. ... would exploit you if they had an opportunity; 2. ... would try to be fair to you)
37. Do you think that people most of the times... (1. ... try to be considerate of others; 2. ... follow their own interests)

## F Instructions

The following instructions are for the shock treatment, "privacy task first" condition and are translated from the Italian original.

### Welcome to the experiment!

The experiment will last about 60 minutes. Please make sure that you can stay until the end. You will be paid 3 Euros for showing up on time (participation fee). You can earn more money but this depends on the choices you make in this experiment and on chance. It is therefore important that you read the following instructions carefully.

#### General rules

You are not allowed to communicate with other participants during the experiment. If you have any doubts or questions, please raise your hand. An assistant will then come to you and answer your question privately.

You received an envelope before the experiment. You are not allowed to open it before the end of the experiment. You will have to open it in front of an assistant.

If you do not follow those rules or disturb the experiment in other ways, then we will ask you to leave the room and we will not pay you.

#### The Experiment

There are two parts in the experiment: the first part is described in a separate sheet now, while you will get the description of the second part only after completing the first task. You will be presented with tables of choices between two options, one of which gives a certain payoff while the other gives an outcome that depends on chance.

#### Payment

At the beginning of the experiment, you were asked to pick an envelope from a bag. In total there were 112 envelopes. 88 of those envelopes describe a choice situation that you faced during the

experiment. If you got one of those envelopes, then you will get the payoff corresponding to the choice you made in the situation described in your envelope. This means that any of your choices during the experiment could be the one that determines your payoff.

The other 24 envelopes give you a payoff that does not depend on your choice (to be described later).

After having completed both tasks your final payoff will be calculated, each ECU earned will be converted into Euro at the rate of 1 euro for 10 ECUs and paid together with the show-up fee (30 ECUs = 3 euros). For example, if you earned 48 ECUs from your decision during the experiment, then you will receive  $48 + 30 \text{ ECUs} = 78 \text{ ECUs} = 7,8 \text{ Euro}$  in cash.

### Anonymity

Since your position in the lab corresponds to the number on a ball taken from a box randomly we only know you by the number of your seat and not by your name, surname or other credentials. Thus, we cannot establish any link between your identity and the decisions you made in the lab, unless the outcome of the experiment suggests revelation of your personal information so that we need to check your name and surname from the ID card.

## I. First part of the experiment

In the first part of the experiment, you are asked to make choices between two options of the type described in the following table:

Row	Option A	Option B	Choice
1	You get 13 ECUs	You get 35 ECUs but with probability 50% your personal information is revealed to others	
...	...	...	...

Option A guarantees you a certain payoff, while option B is a lottery that gives out a certain amount of ECUs, but implies some probability of having to disclose your name, surname, photo and answers in the preliminary questionnaire (from then on "personal information") to other participants in the room at the end of the experiment.

You will face 44 choice situations of the type described above. In each of those situations, you must choose the option (A or B) that you prefer. Any of those decisions might be the one that determines your payoff.

### Random draw

If you chose option B in which your payoff depends on chance, then you will have to toss a 10-sided die. Each side of the die shows a number, between 0 and 90 in steps of 10 (you can check that the die shows all possible numbers, 0, 10, 20, 30, 40, 50, 60, 70, 80, 90). The probability of personal data revelation defined in this option will be compared with the outcome of this toss:

1. If the outcome of the toss is strictly less than the probability of revelation then your information will be disclosed;
2. If the outcome of the toss is more or equal to the probability of revelation then your information will not be disclosed.

### Envelopes

As explained before, you will get a payoff at the end of the experiment that depends on what is in the envelope that you drew at the beginning of the experiment. There were 112 envelopes, of which 68 relate to the first part of the experiment:

a) 44 of the envelopes describe a choice situation from the first part of the experiment. If you drew an envelope from those 44, then it will look as follows:

Option A: You get 13 ECUs  
 Option B: You get 65 ECUs but with probability 50% your personal information will be revealed to others.

*Example:* If you have chosen the option B in this situation, you will get 35 ECUs. Then if the outcome of the toss is strictly less than 50, your personal information is revealed to others. If the outcome of the toss is more or equal to 50 then your personal information is not revealed to others.


b) 24 of the envelopes say that you have to reveal your personal information to others, independently from your decisions during the experiment. You also then get a certain payoff. The certain payoff may be either 55, 65 or 75 ECUs, and each of those value is as likely as the other. If you drew an envelope from those 24, then it will look as follows:

You get 65 ECUs but your personal information will be revealed to others.

In this case you get 65 ECUs and your personal information will be revealed to others.

#### Procedure for personal information disclosure

If your personal information has to be disclosed to other participants, then you will be asked to stand in front of the audience in the lab, we will verify your name and surname from your ID card and we will announce your name. Other participants will see on the screen your personal photo and the answers that you gave in preliminary questionnaire, along with a short descriptive comment comparing your answers with the answers of others as in an example below:



Seat #23:

- ... agrees it is morally justified to abort after discovering serious disability in the fetus, while 36 % of other participants do not agree
- ... is in favor of chemical castration as appropriate penalty for rape, while 87% of other participants did not choose this option
- ...

## II. Second part of the experiment

You have finished the first part of the experiment. Now, please, read carefully the description of the second part of the experiment.

In this part you are also asked to make several choices between two options. Consider the following table:

Row	Option A	Option B	Choice
1	You get 37 ECUs	You get 52 ECUs but with probability 50% you lose 14 of those ECUs	
...	...	...	...

Option A guarantees you a certain payoff, while option B is a lottery that gives out a certain amount of ECUs, but implies some probability of having to give back some of those ECUs at the end of the experiment. In some tables, option B gives out a certain amount of ECUs and some probability of getting some more ECUs at the end of the experiment.

You must choose the option (A or B) that you prefer.

#### Random draw

If you chose option B in which your payoff depends on chance, then you will have to toss the 10-sided die. Each side of the die shows a number, between 0 and 90 in steps of 10 (you can check that the die shows all possible numbers, 0, 10, 20, 30, 40, 50, 60, 70, 80, 90). The probability of gaining or losing ECUs that is defined in this option will be compared with the outcome of this toss:

1. If the outcome of the toss is strictly less than the probability of loss/gain then you will lose/gain some ECUs;

2. If the outcome of the toss is more or equal to the probability of loss/gain then you will not lose/gain any ECUs.

### Envelopes

As explained before, you will get a payoff at the end of the experiment that depends on what is in the envelope that you drew at the beginning of the experiment. There were 112 envelopes, of which 44 relate to the second part of the experiment. If you drew an envelope from those 44, then it will look as follows:

Option A: You get 37 ECUs  
 Option B: You get 52 ECUs but with probability 50% you lose/gain 14 of those ECUs.

*Example:* If you chose option B in this case, then you will have to toss the 10-sided die. If the outcome of the toss is strictly less than 50, then you get  $52-14=38$  ECUs if the loss was indicated or  $52+14=66$  ECUs if the gain was indicated. If the outcome of the toss is more or equal to 50 then you get 52 ECUs.

## G Control questions.

The following control questions are for the shock treatment, “privacy task first” condition and are translated from the Italian original.

We want to make sure that you understand what each option means and let you become familiar with interface of experimental tasks. Therefore, please answer the questions in the examples below. Note that you will not be paid for this.

You will be able to proceed to the next screen only after giving the correct answer. You can try to answer each question several times. If you have questions, please, raise your hand and an assistant will come to you to give you an answer.

### Question 1.

Please now make choices for each row of the following table. We remind you that this is for training only so it will not be taken into account when determining your payment.

Row	Option A	Option B	Choice
1	You get 29 ECU	You get 62 ECU but with probability 10% you lose 24 of those ECU	--
2	You get 6 ECU	You get 10 ECU but with probability 0% you lose 2 of those ECU	--
3	You get 14 ECU	You get 25 ECU but with probability 50% you lose 5 of those ECU	--

### Question 2.

Suppose you are told: “You get 39 ECU but with probability 10% you lose 25 of those ECU”. How many ECU will you get?

I will get with probability 90%..... ECU and with probability 10% ..... ECU

*Correct answer:* 39 ECU; 14 ECU.

### Question 3.

Suppose you have chosen the following option: “You get 13 ECU but with probability 70% your personal information is disclosed to others”. You toss the die and the outcome of the toss is number 70. What is your payoff in this case?

1. I get 13 ECU and the participation fee, my personal information remains anonymous.

2. I get 13 ECU plus the participation fee, but my personal information will be disclosed to other participants in the room in the end of experiment.
3. I get only participation fee.
4. I get nothing.

*Correct answer: 2.*

**Question 4.**

Please consider the two options in table below and write down your choice in the box to the right

Row	Option A	Option B	Choice
1	You get 37 ECU	You get 53 ECU but with probability 10% you lose 14 of those ECU	
...	...	...	...

Suppose this choice is the one that is in your envelope, so it determines your payoff.

Given your choice, what will be your payoff (in ECU) if the outcome of the toss of the die is the number 50, and show up fee is 30 ECU?

1. 67 ECU
2. 83 ECU
3. 69 ECU
4. 37 ECU
5. 53 ECU
6. 39 ECU
7. 30 ECU
8. 0 ECU

*Correct answer: 1 (if A is chosen), 2 (if B is chosen).*

**Question 5.**

Consider the table below:

Row	Option A	Option B	Choice
1	You get 20 ECU	You get 40 ECU but with probability 20% your personal information is disclosed	A
...	...	...	...

Imagine that you have chosen Option A. Then in the end of the experiment you open your envelope and it is written the following:

You get 40 ECU but your personal information is disclosed to others

What will be your payoff in this case including show up fee of 30 ECU?

1. 20 ECU, personal information remains anonymous
2. 20 ECU, personal information is disclosed
3. 30 ECU, personal information remains anonymous
4. 30 ECU, personal information is disclosed
5. 50 ECU, personal information remains anonymous
6. 50 ECU, personal information is disclosed
7. 40 ECU, personal information remains anonymous
8. 40 ECU, personal information is disclosed
9. 40 ECU, personal information is disclosed if the outcome of the toss of the die is less of equal to 20
10. 70 ECU, personal information remains anonymous
11. 70 ECU, personal information is disclosed
12. 70 ECU, personal information is disclosed if the outcome of the toss of the die is less of equal to 20
13. I get nothing

*Correct answer: 11.*



## H Multiple price list menus of choices

### H.1 Monetary lotteries (MPL tables 1 to 4)

Row	Option A	Option B
1	You get 56 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
2	You get 55 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
3	You get 54 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
4	You get 53 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
5	You get 52 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
6	You get 51 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
7	You get 50 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
8	You get 49 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
9	You get 48 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
10	You get 47 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU
11	You get 46 ECU	You get 55 ECU, but with probability 30 % you lose 10 of those ECU

Table 8: MPL table 1

Row	Option A	Option B
1	You get 68 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
2	You get 65 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
3	You get 62 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
4	You get 59 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
5	You get 56 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
6	You get 53 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
7	You get 50 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
8	You get 47 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
9	You get 44 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
10	You get 41 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU
11	You get 38 ECU	You get 65 ECU, but with probability 30 % you lose 30 of those ECU

Table 9: MPL table 2

Row	Option A	Option B
1	You get 80 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
2	You get 75 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
3	You get 70 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
4	You get 65 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
5	You get 60 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
6	You get 55 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
7	You get 50 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
8	You get 45 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
9	You get 40 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
10	You get 35 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU
11	You get 30 ECU	You get 75 ECU, but with probability 30 % you lose 50 of those ECU

Table 10: MPL table 3

Row	Option A	Option B
1	You get 65 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
2	You get 62 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
3	You get 59 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
4	You get 56 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
5	You get 53 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
6	You get 50 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
7	You get 47 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
8	You get 44 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
9	You get 41 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
10	You get 38 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU
11	You get 35 ECU	You get 35 ECU, but with probability 30 % you gain 30 additional ECU

Table 11: MPL table 4

## H.2 Privacy lotteries (MPL tables 5 to 8)

Row	Option A	Option B
1	You get 56 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
2	You get 55 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
3	You get 54 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
4	You get 53 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
5	You get 52 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
6	You get 51 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
7	You get 50 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
8	You get 49 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
9	You get 48 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
10	You get 47 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed
11	You get 46 ECU	You get 55 ECU, but with probability 30 % your personal information is disclosed

Table 12: MPL table 5

Row	Option A	Option B
1	You get 68 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
2	You get 65 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
3	You get 62 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
4	You get 59 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
5	You get 56 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
6	You get 53 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
7	You get 50 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
8	You get 47 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
9	You get 44 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
10	You get 41 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed
11	You get 38 ECU	You get 65 ECU, but with probability 30 % your personal information is disclosed

Table 13: MPL table 6

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

Table 14: MPL table 7

Row	Option A	Option B
1	You get 65 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
2	You get 62 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
3	You get 59 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
4	You get 56 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
5	You get 53 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
6	You get 50 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
7	You get 47 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
8	You get 44 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
9	You get 41 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
10	You get 38 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed
11	You get 35 ECU	You get 35 ECU, but with probability 30 % your personal information is disclosed

Table 15: MPL table 8