

Alisa Frik and Alexia Gaudeul

**Privacy protection, risk attitudes, and the need
for control: An experimental study**

CEEL Working Paper 1-16

Cognitive and Experimental Economics
Laboratory

Via Inama, 5 38100 Trento, Italy

<http://www-ceel.economia.unitn.it>
tel. +39.461.282313



UNIVERSITÀ DEGLI STUDI
DI TRENTO



Privacy protection, risk attitudes, and the need for control: An experimental study

Alisa Frik¹ and Alexia Gaudeul²

WORKING PAPER

February 18, 2016

¹ School of Social Sciences, Università degli Studi di Trento, Italy. Email: alisa.frik@unitn.it

² School of Economics, Chair of Microeconomics, Georg-August-Universität, Göttingen, Germany. Email: alexia.gaudeul@wiwi.uni-goettingen.de

Table of contents

Abstract

1 Introduction

2 Related work and hypotheses

2.1 The problem of valuing privacy protection

2.2 Lack of control and willingness to pay to protect personal information

2.3 Link between risk and privacy attitudes

2.4 Immediacy of privacy shocks

3 Experimental design

3.1 Personal information

3.2 Elicitation method

3.3 Monetary lotteries

3.4 Privacy lotteries

3.5 Payment and personal information disclosure

3.6 Procedure

4 Results

4.1 Risk preferences

4.2 Privacy preferences

4.3 Hypotheses testing

5 Limitations

6 Conclusion

References

Appendixes

Abstract

We expose subjects in our experiment to the risk of having to reveal private information to other participants. We show that the decision to incur this risk is driven mainly by their general attitude to monetary risk. Survey attitudes to privacy play only a marginal role in explaining attitudes to privacy risk. Subjects who are more willing to pay or to accept payment for their personal information do not appear to be more or less likely to incur privacy risks than others once their overall level of risk aversion is taken into account. We further test the relation between privacy and control, that is, whether depriving subjects of full control over whether their personal information will be revealed leads them to lose interest in protecting it. We find that this is not the case. We finally find that subjects who are asked for their preferences over monetary risk before being asked for their preferences over privacy risks tend to choose riskier options in privacy lotteries. This provides evidence of the importance of framing for privacy decisions; inducing subjects to think of privacy decisions in the context of financial decisions reduces their aversion to privacy risk.

Acknowledgements

The authors thank Marco Tecilla for technical assistance, Luigi Mittone, Matteo Ploner, Caterina Giannetti, Alex Imas, Alessandro Acquisti, and other colleagues and faculty members for valuable comments and feedback that helped us to improve the manuscript.

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 have uncertain consequences. This is why in our experiment we elicited the willingness to take risk with one's personal information using choices between lotteries rather than relying solely on the self-reported WTA/WTP. Namely, we offered participants the option to play privacy lotteries that resulted in personal information disclosure with a certain probability. We also asked participants to play lotteries involving monetary outcomes, in order to determine if their attitudes to privacy risk differ in a systematic manner from their attitude to financial risk. Finally, we wanted to test whether, as implied by some existing research, privacy could be defined as a good that has value only in so far as one maintains control over it. We will refer to such goods as "control goods" in the rest of the paper. Unlike a house or a car, which maintains its usage value to us even if it is under threat of being stolen, privacy would, under this hypothesis, lose its value if it is under threat. In other words, under this approach, one would care about privacy only if one feels to be in control of the level of risk to which it is exposed, while one will be more readily to exchange it for

other goods otherwise. If that were the case, attitudes to privacy risk would differ in a radical way from attitudes to monetary risk.

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, and the first to directly test a view of privacy as a “control good”, *i.e.* to test whether personal information has worth only when the risk to which it is exposed is under an individual’s control.

We decided to test the effect of depriving participants of control over their personal information because prior research has identified control or the lack thereof as an important driver of risk attitudes and behaviors (Weinstein, 1984; Slovic, 1987; Harris, 1996; Nordgren *et al.*, 2007, *etc.*). A Pew Research (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.*, 2009; Brandimarte *et al.*, 2013). In our experiment, we therefore test the effect of reducing control over the release of personal information by introducing “privacy shocks” (probabilistic disclosure of personal information, even when the participant always chose the safest option in privacy lotteries). We compare treatments with such shocks to treatments where participants can guarantee through their decisions that no revelation of private information will occur.

We find that behavior in either treatments do not differ in a significant way. The introduction of the risk of a privacy shock does not alter individuals’ choices in privacy lotteries. The best predictor for attitudes to privacy risk is attitude to monetary risk.

Another variation in our experiment was to present privacy lotteries before or after the financial lotteries. We found that if privacy lotteries were presented first, then subjects tended to make safer privacy choices.

The paper is organized as follows: section 2 reviews related literature and presents our hypotheses; section 3 describes our experimental design and our methodology; section 4 provided and analysis of the data and tests of our hypotheses; section 5 provides a discussion of our results; section 6 underlines limitations of our study; 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.

A number of studies developed micro-economic and decision-making models to place privacy issue into an economic framework. One of the most popular approaches assumes that people are engaged in a so-called *privacy calculus* (Laufer and Wolfe, 1977; Culnan and Armstrong, 1999). People are assumed to perform a cost-benefit analysis in order to find a compromise between privacy protection and disclosure of personal information. Acquisti *et al.* (2015) point out that personal information has some properties of a public good, such as non-rivalry and non-excludability (see also Westin, 1970). Farrell (2012) describes privacy as something that is often “valued for its own sake” (p. 252) but also is sometimes valued in a more instrumental way, that is, as protection from price or employment discrimination, identity theft or other negative consequences that are not always related to privacy *per se*.

2.1 The problem of valuing privacy protection

The next step after creating a model in the traditional scientific approach would be to put it to the test. However, 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? Should we consider the value for privacy as the cost of data collection, storage or processing for the firms, as the cost of its protection for the consumer, as the monetary consequences of misuse, as the benefits provided in exchange for personal information, as the psychological pleasure of sharing data or the discomfort of its disclosure? Two main approaches that researchers took to investigate these issues are surveys and experiments.

Although numerous surveys report high privacy concerns in the general population of both U.S. and Europe (see, for example, Turow *et al.*, 2015; Pew Research Center survey, 2015; Special Eurobarometer, 2015), the hypothetical questions in surveys and the complexity of the privacy attitudes make it difficult for the researchers to quantify the preferences of participants and predict their behavior. Indeed, stated preferences usually differ from observed behavior (Acquisti *et al.*, 2015). For instance, a Jupiter Research survey (Leathern, 2002) reported that 36% of the respondents among US population would allow tracking of their Internet activities for a \$5 discounts. Recently the similar fraction of the European respondents agreed to trade their e-mail addresses for money or a chance to win a prize (Symantec, 2015). However, another survey conducted in 2015 by the University of Pennsylvania, 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, 2015, p. 3).

In order to address such issues, researchers have turned to experimental and empirical methods in attempts to estimate the value people assign to their personal information. The 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; and 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). The anecdotal evidence from 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, e.g. weight, and bid for protection from revelation of information about this trait.

Acquisti *et al.* (2015) conclude that privacy attitudes are idiosyncratic, subjective, context-dependent, and dynamic, *i.e.* change over time (see also John *et al.*, 2011). Indeed, as one can see even from the limited sample of findings presented above, privacy preferences differ dramatically across individuals and studies. We believe that the experimental approach is a powerful tool for a better understanding of individuals' preferences by eliciting behavior in an incentive compatible way. We do not claim to find an absolute value for privacy, but the issues with the explicit measuring approach encouraged us to search for novel methods (or application of existing ones in a new fashion), so that in combination with other techniques our findings could eventually contribute to the overall understanding of attitudes and decisions processes behind privacy decision-making.

2.2 Lack of control and willingness to pay to protect personal information

Beyond developing new methods for measuring the value of privacy, we are also interested in testing whether knowing that one's personal information is already under threat influences how much one's willing to pay to protect it. Control over personal information flows in the privacy literature is often viewed as a prerequisite for privacy protection (*e.g.* Kang, 1998; Solove, 2006).

The so called "control paradox" documented in Brandimarte *et al.* (2012), suggests that providing more granular control over personal information can eventually result in a more extensive release of sensitive data, while lower level of perceived control leads to a decreased disclosure behavior. In our experiment, we induce lower control by increasing the risk of disclosure in the treatment condition vs. the baseline. Moreover, we explore the effect of decreased control on one's willingness to take risks with one's

personal information, rather than on one's willingness to disclose information.

Using dynamic lotteries in a lab experiment, Feri *et al.* (2015) studied the reaction of participants to notifications of a privacy breach, which jeopardized their personal information. The disclosure of personal information was a probabilistic event (privacy shock), which happened with some probability if a breach had occurred. They found that subjects were less likely to disclose their personal information after receiving a breach notification. Unlike Feri *et al.* (2015), 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. Finally, we control individual privacy risk attitudes with monetary risk attitudes.

Based on prior findings in the literature, we expect that when control over personal information is exogenously taken away, then subjects would react by moving towards extreme strategies of either more risk averse behavior (total protection) or less risk averse behavior (abandoning any privacy defenses). These two possible but contradictory effects can be summarized in hypotheses 1a and 1b.

Hypothesis 1a (Protective behavior). *The introduction of a privacy shock increases the number of safe choices in privacy lotteries.*

In support of this hypothesis, Dinev and Hart (2006) found that privacy risks and concerns are closely and positively related. There is also some empirical support for this hypothesis in Xu, 2007, Hoadley *et al.*, 2010. We expect the lower perception of control over personal information to increase privacy concerns. Willingness to mitigate the concern could result in a more privacy protective behavior. Moreover, we expect that some of our participants could fall in the pitfall of misunderstanding and miscalculation of objective probability of personal information disclosure due to the composition of two risks: the risk of a privacy shock and the risk from choosing a risky option. Since the latter one is out of their control, they could try to "compensate" for it and focus on the

“controllable” part by reducing the riskiness of their behavior in privacy lotteries.

Alternatively, under the view of privacy as a “control good”:

Hypothesis 1b (Denial behavior). *The introduction of a privacy shock increases the number of risky choices in privacy lotteries.*

As discussed previously, the randomness of this shock by its nature is not under one’s control, which could lead some subjects to lose their motivation to protect their personal information and devalue the control over risk that remains “in their hands”. That would result in taking more risk of personal information disclosure.

2.3 Link between risk and privacy attitudes

As decisions about protection of personal information presume both that a person has a positive value for privacy and a negative attitude to risk, we expect the willingness to protect personal information to increase with risk aversion:

Hypothesis 2 (Positive relation between risk and privacy attitudes). *The willingness to protect personal information is positively correlated with individual risk aversion.*

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.

2.4 Immediacy of privacy shocks

In our experiment, we run two variations whereby in one case, monetary lotteries are played before privacy lotteries and in the other case the opposite. 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, 1998; Dukas, 2004; Lachter *et al.*, 2004). In contrast, playing privacy lotteries first could draw more attention to its 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. Egelman *et al.* (2009) showed that timing has significant impact on privacy decisions. 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. Therefore, we make the following hypothesis:

Hypothesis 3 (Order effect on privacy preferences). *Presenting privacy lotteries before the monetary lotteries – and thus right after answering the privacy questionnaire, leads to behavior that is more privacy protective.*

The hypothesis predicts more safe options being chosen in privacy lotteries when they appear before the monetary lotteries.

3 EXPERIMENTAL DESIGN

Subjects were asked to make a sequence of binary choices between safe and risky options. Our design includes two treatments: 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. 21% probability of revelation of their personal information independently from the choices in the experiment. In each treatment, subjects faced two types of lotteries: *monetary*

lotteries that imply changes in monetary outcome; and *privacy* lotteries that imply the disclosure of personal information. 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. The order of the tables within each task was randomized across participants. Thus, we have a 2×2 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. The order effect was also tested between-subjects, whereby subjects completed either the monetary or the privacy task first. Within-subject analysis allows comparison between the choices of every participant across the two tasks, the ones with privacy risk and the ones with monetary risk.

3.1 Personal information

In order to create a privacy concern, we combined different sources of personal information: *standard* personal information coming from the “real world”, and personal information that was *synthetically generated* in the lab.

As standard privacy items we used name, surname and photo that combined together can be classified as personally identifiable information according to the National Institute of Standards and Technology (2010). Moreover, from full name and photo one could potentially also 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).

Upon arrival in the laboratory we made a photo of each subject that was associated only with the number of their randomly assigned seat and not with any other credentials. Hence, name and surname remained unknown unless the outcome of the experiment was such that the subject had to reveal them at the very end of the experiment.

After this was done and before receiving the instructions about the experiment (appendix H), participants answered a preliminary

questionnaire (appendix G), consisting of 14 questions about opinion on potentially sensitive or socially relevant topics, such as abortion, illegal immigration, and appropriate methods of birth contraception. No matter whether the subject answered truthfully or not, different answers created a “personal image”, dividing the experimental population into adversary groups, leading to nonconformity³ among the subjects being revealed. The psychological literature states that the fear of being isolated from other people imposes a psychological cost⁴ on subjects expressing unpopular opinion (see Noelle-Neuman, 1974; Kim, 1999). 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, 2006; Janes and Olson, 2000; Kruglanski and Webster, 1991). Uncertainty about other participants’ responses increased the psychological discomfort of expressing opinion. Moreover, since questionnaire was presented in the form of multiple choice options rather than open questions, participants did not have opportunity to explain or defend their positions⁵.

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 of values and beliefs. Grossklads and Acquisti (2007) used quiz performance to estimate willingness to sell or protect personal information. Feri *et al.* (2013) created sensitive information via a logic test score connected to the real name of the participant.

The synthetically-produced personal information was then put under the risk of privacy breach in our laboratory experiment. Our

³ 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. Intraclass 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.

⁴ Nonetheless, nonconformity could appear advantageous in certain circumstances, *e.g.* if subjects’ attempt to emphasize their uniqueness or individuality (see Argyle, 1957; Hollander, 1958; Snyder and Fromkin, 1980; Maslach *et al.*, 1985, *etc.*).

⁵ Indeed, during the experiment several participants raised the question about such a possibility and expressed concern about absence of such.

novel method of synthetic personal information creation overcomes the disadvantages of using intelligence test scores, which creates a dichotomous division between bad and good types and also creates an overconfidence bias (Griffin and Varley, 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 to capture an issue that is sensitive for an individual and, hence, 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.

Name, surname, photo, and the responses to the preliminary questionnaire will be referred to as *personal information* in the present study.

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 the experimental economics literature. MPL are easy to understand for participants and are incentive compatible. The MPL design was introduced in Miller *et al.* (1969), popularized by Holt and Laury (2002) and further developed in a number of different studies (see Andersen *et al.* (2006) and Harrison and Rutström (2008) for a more complete review).

In our study subjects were offered 8 lists, each list requiring 11 decisions between two options. Safe options were presented in decreasing order of value on the left and risky lotteries were presented in the right column. They were labeled Option A and Option B, respectively (see the screenshot in figure 1). Subjects were asked to indicate the option they preferred to play for every row. They thus made 88 binary decisions, of which one half were related to the monetary task and another half to the privacy task. An individual with consistent preferences will switch from one option to

another at one point only, so the actual number of decisions – when to switch - could be reduced to only 8 per person.

Figure 1 – Screenshot of one of the MPL menus presented to the subjects in the privacy task

	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 offers a safe payoff X_{ij} . Option B offers an outcome Y_{ij} , which is increased or decreased by V_{ij} (denoted v_M for monetary tasks, v_p for privacy task, respectively) with probability p . $i \in \{1; 4\}$ denotes one of the four MPL menus (tables) of the task and $j \in \{1; 11\}$ denotes one of eleven rows in the MPL menu. In the general form lottery $L(y, v, p) = (y, p; (y - v), 1 - p)$ is a lottery that provides outcome y with probability p , and outcome $(y - v)$ with complementary probability $1 - p$.

We presented subjects with decreasing safe amounts and a given lottery. According to Maier and R  ger (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 could have more transparent interpretation for participants than comparison of event probability.

3.3 Monetary lotteries

In the monetary task we presented to subjects menus of choices between safe payoff X_{ij} and lottery L_i . Appendix J.1 contains information about payoff matrix in the form of MPL menus as they were presented to the subjects. Note, that in the first three MPL tables lottery implies a probability of loss of the part of earnings, while the last table implies a chance to gain some additional money.

For our measurements of risk attitude, we used the implied rate of return required by a subject who is indifferent between X_{ij} and L_i . The required rate of return (RoR) is commonly used in corporate finance and equity valuations for the assessment of the risk investors are willing to accept. RoR_{ij} represents the minimum increase in the certainty equivalent CE_{ij} of the lottery L_i necessary to become even out the expected value EV_i of this lottery:

$$RoR_{ij} = \frac{EV_i - CE_{ij}}{CE_{ij}} \quad (1)$$

In this study we will use the midpoint of estimated interval as measurement of risk tolerance level. Adopting the idea that back-and-forth switching behavior could account for the indifference (see Andersen *et al.*, 2006, Charness *et al.*, 2013; and Harrison *et al.*, 2013), in cases where subjects switched more than once, we will refer to the mean value between the lower bound of the first switch and the upper bound of the last switch in MPL table as to the estimation of his risk tolerance level. In the cases, where subject's response is interval-censored, we consider the risk tolerance level to be unobserved for that subject. We will also use per-subject average value of RoR across all tables of monetary task, \overline{RoR} .

The crossover point in the MPL menu, where subject chooses an option B provides an interval estimate of risk tolerance level. Individuals with negative values of RoR can be classified as risk

seeking, with positive values – as risk averse, and with values equal to zero – as risk neutral.

Table 1 summarizes the information about ranges of safe and lottery outcomes, and interval estimations of RoR across MPL menus of the monetary task.

Table 1 – Ranges of outcomes and interval estimation of RoR across MPL tables, in ECU⁶

MPL table	Range of safe outcomes	Lottery option	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%

RoR and r in a CRRA function vary in similar ways. We chose the non-parametric measurement of risk attitude rather than parametric (*e.g.* constant relative risk aversion coefficient), because RoR ranges between -1 and 1, has a straightforward interpretation, does not make assumptions about the shape and properties of utility function, and can be observed for all rows of MPL menus.

3.4 Privacy lotteries

In the privacy task, we showed to the subjects the menus of choices between safe payoff X_{ij} , and lottery L_i , in which subjects gets Y_i ECU, but with probability p their personal information is disclosed to other participants in the lab. Values of X_{ij} , Y_i , and p are the same as in monetary task (see the correspondent MPL menus in appendix J.2). We denote the (dis)utility of the disclosure of personal information for each subject as v_p . This value represents the equivalent in monetary terms of the “loss of privacy” (*i.e.* personal information disclosure) that makes a risk neutral individual indifferent between two options in the privacy lotteries. The value of this (dis)utility is

⁶ Experimental Currency Unit. In our experiment 1ECU=€0.1.

not known and we try to elicit it through analysis of experimental decisions.

Assuming risk neutrality, we can compute an interval estimate of the value of v_p as implied by the switching points in the MPL menus of the privacy task (table 2). Namely, if a risk-neutral subject is indifferent between safe and risky option for a given safe payoff x , then $x = y \cdot p + (y - v_p) \cdot (1 - p)$, and the implied equivalent monetary loss (or gain) from personal information disclosure is thus:

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

We will use the midpoint of the elicited interval as measurement of v_p 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 table when subjects switched more than once. Table 2 shows for each table the range of v_p that can be elicited. Note that a negative v_p implies that an individual derives positive utility from the risk of disclosing his information (“privacy exhibitionism”).

Table 2 – Interval estimation of implied utility of the risk of personal information disclosure assuming risk neutrality, in ECU

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

Although we expected the majority of people to attribute a positive value for personal information and tend to protect it from disclosure, a number of studies suggest that some people, in contrast,

are willing to make their personal information and opinions public depending on their goals, attitudes personality traits and other factors (see Zywicki and Danowski, 2008; Correa *et al.*, 2010; Krasnova *et al.*, 2009; Ross *et al.*, 2009). This tendency is enhanced by social media technologies, such as online social networks, blogs, etc., and could be especially typical for the active users of such technologies, extensively present in the population of students, and, consequently, in the sample of our participants⁷.

In this study we assume risk neutrality for calculation of v_p . Positive value of v_p can be translated into disutility of personal information disclosure, while negative value of v_p can be attributed to the utility of personal information disclosure.

The choice of fixing $p = 0.7$ was driven by the fact that, although 50/50 chance is more neutral and rather suitable for monetary lotteries, the 50% probability of personal information disclosure is somewhat too high with respect to what is observed in real world. Hence, we decreased it to one third.

Correction of v_p with attitude to risk We elicited both monetary and privacy risk aversion and can therefore disentangle risk preferences from the utility of personal information disclosure. If we assume that risk attitudes are of a similar nature in the monetary and the privacy context, then we can obtain values of v_p that take account of the risk tolerance level that was elicited in the monetary task,

Consider an individual i with average measured level of risk aversion \overline{RoR}_i . This individual is indifferent between safe payoff x and a risky option with payoff y and a probability p of personal information disclosure if $x \cdot (1 + \overline{RoR}_i) = y \cdot p + (y - v_p) \cdot (1 - p)$. The implied *corrected* equivalent monetary loss (or gain) from personal information disclosure is thus:

$$v_{p_{\overline{RoR}_i}} = \frac{y - x \cdot (1 + \overline{RoR}_i)}{1 - p} \quad (3)$$

⁷ Only about 5% of our participants indicated not to be members of any online social network.

This value can differ significantly from the value calculated by assuming risk-neutrality. Indeed, people who are unwilling to take a risk of personal information disclosure may be risk-averse, or they may have high disutility from such disclosure. Two participants with the same switching point x in privacy tasks will have different values of $v_{P_{\overline{RoR}}}$. The risk-averse subject will have lower value of $v_{P_{\overline{RoR}}}$ than a subject who is less risk averse. This can seem counterintuitive but, as we can see from formula (3), the function that determines $v_{P_{\overline{RoR}}}$ is decreasing in \overline{RoR} : the more risk-averse the subject, the bigger the value of \overline{RoR} , so the larger is the value subtracted from y , the lower is the value of $v_{P_{\overline{RoR}}}$ and thus the lower the disutility from personal information disclosure. In particular, as we will see, subjects who are observed to be very risk-averse in monetary tasks but not particularly risk-averse in privacy tasks may have implied values of privacy that are *negative*, *i.e.* their choice may be implying that they *enjoy* revelation of personal information. From formula (3), this happens for y sufficiently close to x (the switching point) and \overline{RoR}_i high enough.

This approach in separating value for privacy from risk preferences is very coarse, of course, but more sophisticated methods do not change its logic. We leave the exposition of other methods to a companion paper.

3.5 Payment and personal information disclosure

To improve the clarity of decision consequences, we employed the prior incentive system (PRINCE) as explained in Johnson *et al.* (2014). Instead of picking one of the decisions for payment only at the end of the experiment, the PRINCE system involves distributing closed envelopes with a description of the real choice situation that will determining an individual's payoff *before* the experiment starts⁸. In other words, the payoff-relevant decision situation has been

⁸ As many studies demonstrate, 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 *et al.* (2010)).

already picked up but participants do not know which situation is described in the closed envelope until the end of the experiment. 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, participants have to consider each decision they make as potentially payoff-relevant. Johnson *et al.* (2014) claims that PRINCE system improves subjects' understanding that the payoff-relevant decision is chosen at random, and gives them better reassurance that this is true randomization, *i.e.* that the experimenter does not deceive them. This also makes isolation of each decision "maximally salient" (p. 3) and makes the issue of hedging across decisions (Holt, 1986) less important.

In the shock treatment, we introduced the risk of privacy shock by adding 24 envelopes that determined the payoff independently from the choices made in the experiment – this is in addition to the $8 \times 11 = 88$ envelopes of the basic treatment. Thus, with $24/112 \cdot 100\% \approx 21\%$ 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 tables⁹.

3.6 Procedure

The experiment was conducted in the Cognitive and Experimental Economics Laboratory of the University of Trento in Italy from the 4th of May to the 8th of June 2015. A total of 148 subjects were recruited for 8 experimental sessions, in groups of 15-21 participants per session, among undergraduate students at the University of Trento. 66% of the subjects were male. Appendix F summarizes the demographic characteristics¹⁰. Experiment lasted for about an hour and participants on average obtained €8.83 (ranging from €5.50 to €11.00), including a €3.00 participation fee.

⁹ 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.

¹⁰ The demographic characteristics were similar across all sessions.

On the days of the experimental sessions and before entering the laboratory participants were collected in the lobby and asked to read the informed consent form and questions from preliminary questionnaire. After that, subjects were given an opportunity to decline participation in the experiment. The payment of €3.00 for showing up on time was guaranteed independently on that decision. Thus, we controlled for self-selection related to reluctance to respond to the questionnaire. No subjects left the experiment and all signed the informed consent form.

Then each subject picked at random an envelope from one bag and a ball with a seat number from another bag and entered the laboratory. Participants were asked to keep the envelope closed till the end of the experiment. An experiment assistant took a photo of each participant. These photos were associated with subjects only by the seat number and not by name, surname or other credentials.

The software for the experiment was programmed in the Delphi programming language. After completion of the preliminary questionnaire subjects read printed out instructions for the first part of the experiment, while assistant read them aloud to ensure common knowledge. Then subjects answered several control questions (appendix I) to familiarize themselves with the software interface and check their understanding of the instructions. Only once all participants had given a correct answer to all control questions they proceeded to the first task of the experiment described in Section 3. After all participants finished the first task, they were given printed out instructions for the second part of the experiment, which assistant also read aloud. Similarly, subjects went through the second task after given correct answers to all control questions related to the second part of the experiment. After they finished the second part of the experiment participants were asked to answer a final questionnaire about the experiment, basic demographic information, attitudes towards privacy, risk, self-disclosure, fairness, and trust.

At the end of each session the subjects came one-by-one to the experimenter's table and opened their envelopes. The situations described in the envelope were implemented. If the subject chose

option B in the described situation, he was then asked to draw a 10-sided die to determine the outcome of the chance.

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 informed subjects, providing also an example in the instructions, that summary of the answers to the preliminary questionnaire would be presented in the form of comparison with the fraction of participants who answered in a different way. For example, if the subject called John Smith answered “yes” to the question 7 of the preliminary questionnaire, his response appeared on the screens of other participants (together with answers to the rest of the questions) as follows: “John Smith agrees that it is morally justified to abort after discovering serious disability in the fetus, while 36% 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 contains 13,024 observations: 88 binary choices made by 148 individuals. Each session lasted for about an hour.

In 95.86% of cases participants switched from one option to another only once ¹¹, demonstrating consistent monotonic preferences across lotteries. This includes 22.97% of cases where there was no switch in a MPL table at all – i.e. always choosing the risky option or always choosing the safe option. Moreover, in privacy task we observed less inconsistent behavior than in monetary task (1% versus 7% of participants switched more than once). One of the possible explanations is that fewer participants were indifferent between options in the privacy task compared to the monetary task

¹¹ Similar to a proportion of 5.5-6.6% observed by Holt and Laury (2002).

(Andersen *et al.*, 2006, Charness *et al.*, 2013; and Harrison *et al.*, 2012).

In general, in monetary task subjects made more safe choices than in privacy task¹². About one third of the participants started with the choice of safe option in privacy task and then switched to a risky one in the third row, as soon as high lottery outcome exceeds the amount of safe payoff, i.e. made decisions as if their personal information had value just slightly larger than zero, under assumption of risk neutrality. We also found that in condition where privacy task appeared first the proportion of people who behaved in this way in the privacy task was significantly lower than in the “monetary lotteries first” condition¹³.

4.1 Risk preferences

After calculation of the average midpoint of RoR elicited from the monetary task per subject, we can conclude that generally participants were risk-averse (82%), some risk-neutral (10%), and a few risk seeking (8%). Similarly, Holt and Laury (2002) found that about two-thirds of the subjects in their experiments were risk averse when all prizes were below \$4.00. They also noted that risk aversion increases when payoffs are scaled up. Since in our experiment the highest possible outcome was €8.00 plus €3.00 of show-up fee, we can justify the higher proportion of risk averse subjects.

¹² Namely, 63.42% vs. 57.80% of subjects chose safe options in monetary and privacy task, respectively. Two-sample Wilcoxon rank-sum test on the number of safe choices: $\text{Prob} > |z| = 0.0111$. Estimated power is 0.9115.

One might argue that this result is driven by the fact that tables 4 and 8 differ from the other tables (*i.e.* lotteries in table 4 implies monetary gains instead of losses and any risky choice in table 8 presumes solely negative values of v_p rather than both positive and negative, and thus one can expect people to make less risky choices in table 8, while it is less unexpected in table 4). However, the difference is even larger (63.17% vs. 44.39%) when we do not take into consideration tables 4 and 8. Two-sample Wilcoxon rank-sum test on the number of safe choices: $\text{Prob} > |z| = 0.0000$. Estimated power is 1.0000.

¹³ Two-sample test of proportions: $\text{Pr}(Z > z) = 0.0019$. Estimated power is 0.8314. When table 8 is excluded: $\text{Pr}(Z > z) = 0.0006$, power is 0.9052.

4.2 Privacy preferences

Here we will examine the privacy values measured in two different ways: as implicitly derived from the choices in privacy task assuming risk-neutrality, and as explicit self-reported willingness-to-pay (WTP) and willingness-to-accept (WTA) payments for privacy disclosure.

Implicit measures We start with implicit measure of the risk of personal information disclosure assuming risk neutrality. Using formula (2) we computed values of v_p .

Appendix A and B summarize results of estimation of v_p . The mean is about €0.02. About 93% of subjects had consistently positive value of v_p in all 4 MPL tables in privacy task. The distribution of v_p is shown in appendix C.

Explicit measures of WTA and WTP We compare implicit and explicit estimates, by confronting measures derived from what subjects claimed and what they actually did.

Questions 6 and 7 in the final questionnaire (appendix K) intended to measure WTA/WTP for disclosure/protection of personal information. See appendix A and B for summary of results. In line with numerous empirical evidences from the literature, average WTA was higher than average WTP¹⁴.

We find that the mean v_p is 6.4 times lower than the mean WTA and 1.3 times higher than mean WTP. The WTA is thus overstated compared to decisions that subjects made in the experiment. While WTA and WTP were all higher than or equal to zero, elicited values revealed that some subjects also derived positive utility from personal information disclosure. It might be that subjects

¹⁴ For instance, WTA observed in our experiment is 8 times higher than WTP, which is in line with 7.17 mean WTA/WTP ratio found by Horowitz and McConnell (2002) across 45 studies about a variety of goods. Grossklag and Acquisti (2007) provide evidence of the gap between 4 and 36 times depending on type of information (quiz results, weight, favorite vacation destination, and number of sexual partners). This finding supports high context dependency of such measures. For review, see, for example, Horowitz and McConnell (2002), and Roth (2005).

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 disclose personal information rather than assuming that all participants are unwilling to disclose.

4.3 Hypotheses testing

To test the hypotheses stated in section 2 we run a panel random GLS regression of the following general form:

$$Safe_{Privacy_{ij}} = \beta_0 + \beta_1 \cdot Shock_i + \beta_2 \cdot Order_i + \beta_3 \cdot RoR_{ij} + \beta_4 \cdot WTA_i + \beta_5 \cdot WTP_i + \beta_6 \cdot Control_{ij} + \varepsilon_i,$$

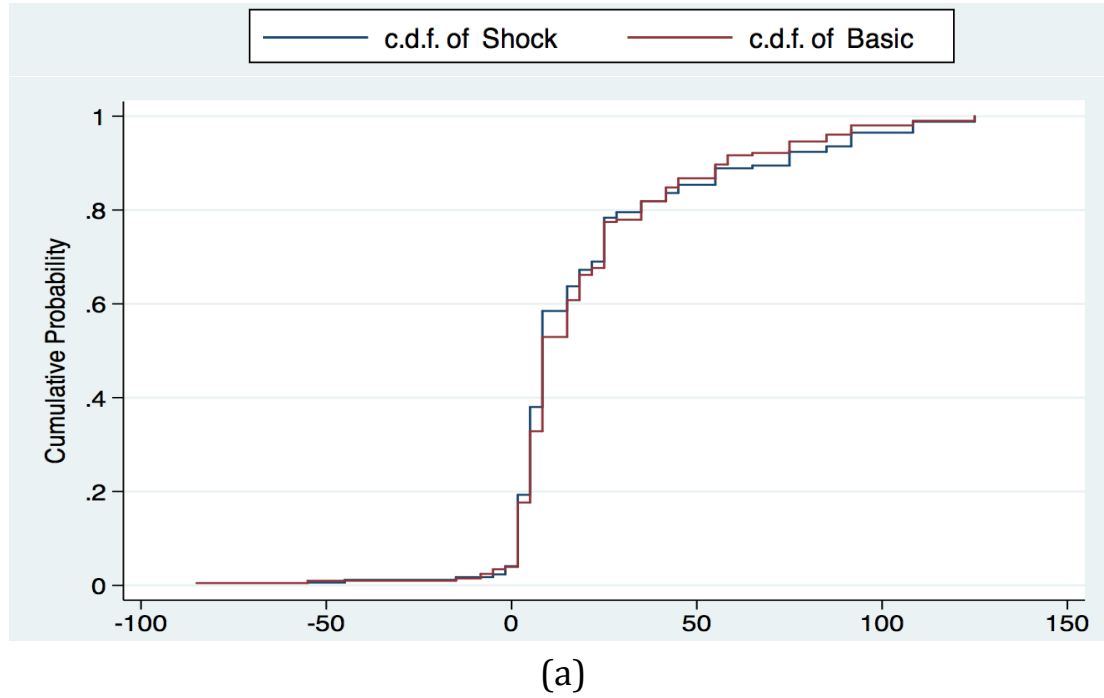
where $Safe_{Privacy_{ij}}$ is a main dependent variable – number of safe choices in privacy task made by participant i in MPL table $j \in (5; 8)$; $Shock_i$ is a dummy variable which takes value 0 for participants assigned to basic treatment and value 1 - to shock treatment; $Order_i$ takes value 0 if monetary task appears before privacy task, 1 otherwise; RoR_{ij} is RoR by subject per table; WTA_i and WTP_i are WTA and WTP per subject, respectively; $Control_{ij}$ includes a list of individual subject characteristics derived from the answers to the exit questionnaire. See table of correspondent regression coefficients in appendix E.1.

Test of hypothesis 1 For the testing of hypothesis 1 we look at the number of safe choices and v_p taking into account all individual decisions and controlling for individual effects. Treatment effect on the number of safe choices in privacy task does not turn out to be significant. Tests on the cumulative distribution function of safe choices and v_p by treatment¹⁵ do not show a significant difference

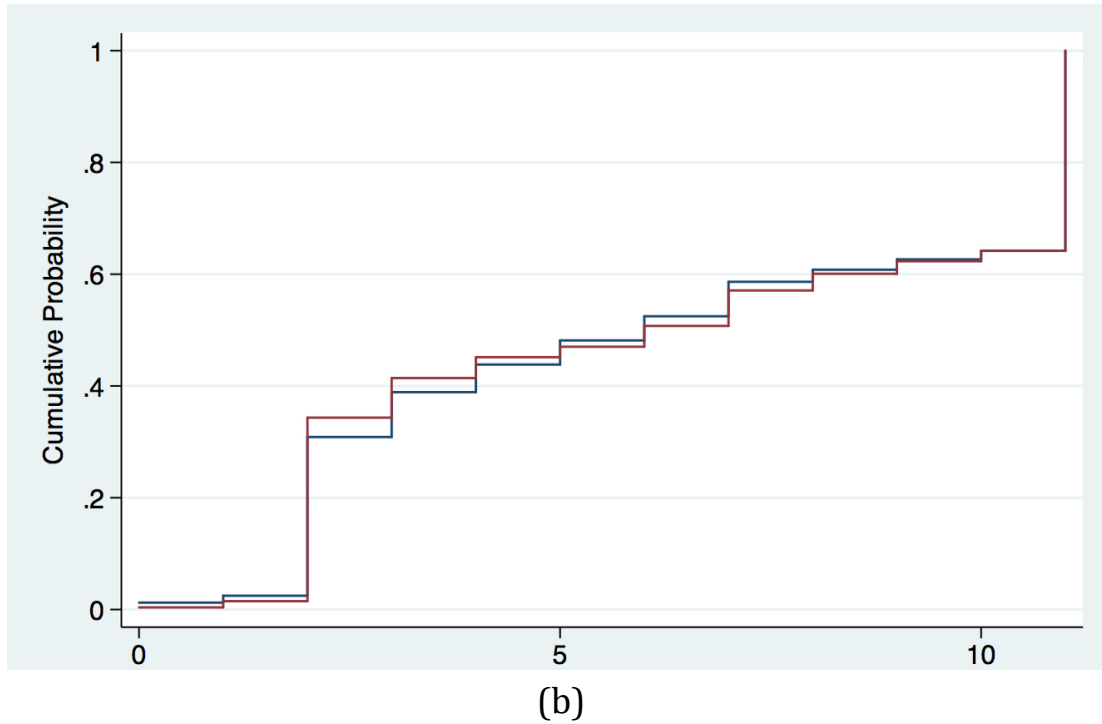
¹⁵ Tests of the difference in the number of safe choices: two-sample Wilcoxon rank-sum test: Prob > |z| = 0.8368; t-test: Pr(|T| > |t|) = 0.9996; Kolmogorov-Smirnov equality-of-distributions test: corrected p-value is 0.993; ANOVA: coefficient is -0.0002, P>|t|=1.000; Kruskal-Wallis equality-of-populations rank test: Prob=0.8368. N=592 (268 and 324 in shock and basic treatments, respectively). Estimated statistical power is 0.05.

between treatments. Fig. 2 shows the c.d.f for v_p and for the number of safe choices by treatment. Neither the panel regression of the number of safe choices in appendix E.1 nor the regression on v_p in appendix E.2 show any treatment effect.

Figure 2 - Cumulative distribution function of: (a) v_p and (b) the number of safe choices across treatments



Tests of the difference in v_p : two-sample Wilcoxon rank-sum test: Prob $> |z| = 0.4878$; t-test: $\Pr(|T| > |t|) = 0.8424$; Kolmogorov-Smirnov test: corrected p-value is 0.921; ANOVA: coefficient is -0.5879, $P > |t| = 0.842$; Kruskal-Wallis rank test: Prob = 0.4878. N = 375 (171 and 204 in shock and basic treatments, respectively). Estimated statistical power is 0.0545.



Thus, we reject the hypothesis 1 that the introduction of a privacy shock leads 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.

Test of hypothesis 2 Regressions in Appendix E.2 and figure 3 show that correlation between RoR and v_p is positive¹⁶. RoR is a significant predictor of the number of safe choices in privacy task (appendix E.1). Regression coefficients are robust to introducing controls. People who knew more participants in the lab and expressed a general tendency to trust strangers had lower values of v_p (appendix E.2). Westin's fundamentalists had higher values of v_p , while the relations of v_p with explicit valuations of personal information (WTA and WTP) were not significant. This confirms that differences in willingness to protect personal information are driven at least in part by risk aversion rather than only, or even mainly, by

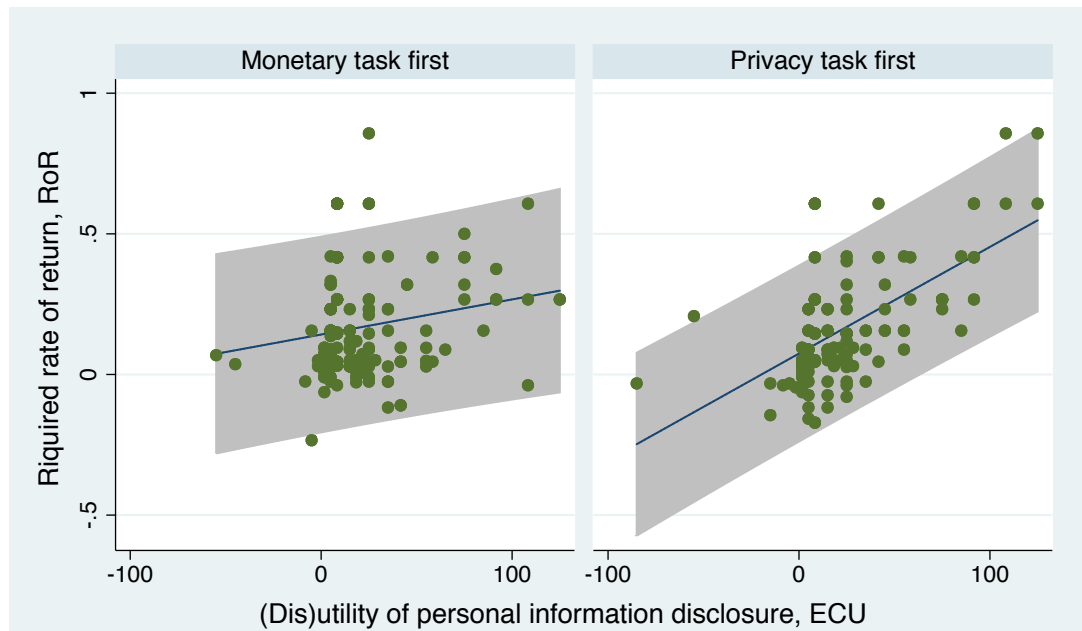
¹⁶ Pairwise correlation coefficient is 0.38 (p-value 0.000).

differences in values for personal information and in privacy attitudes.

This insight is one of the main contributions of this study, as previous studies did not control for subjects or respondents' aversion to risk when asking them to value their personal information.

Note however that this result should not be interpreted to mean that the more risk-averse subjects have a higher utility for personal information. Indeed, v_p is only a way to index decisions in privacy lotteries, and is calculated under an assumption of risk neutrality. It is not an estimate of a subject's utility of personal information¹⁷. 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 v_p ; the more risk averse the subject, the more his risk aversion influences his choices about taking privacy risk.

Figure 3 - Scatterplot of RoR and v_p , by condition, with prediction line of linear regression and 95% confidence interval for forecast



¹⁷ Note that relation between RoR and WTA and WTP is negative but weak and not significant, while a relation between v_p and WTA and WTP is positive, yet weak and not significant. Pairwise correlation coefficient between RoR and WTA is - 0.0123 (p-value 0.7785); between RoR and WTP is - 0.0201 (p-value 0.6453); between v_p and WTA is 0.0424 (p-value 0.4182); between v_p and WTP is 0.0967 (p-value 0.0635).

The regression line is steeper in condition where privacy task appeared first¹⁸. 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. There are no significant differences in the relationships across treatments (appendix D).

Corrected privacy values If we disentangle the (dis)utility from personal information disclosure from the risk tolerance level using formula (3), then we obtain values of $\overline{v_{P_{RoR}}}$ that are distributed more smoothly around zero than uncorrected $\overline{v_P}$. There are many more negative values of privacy than when considering uncorrected $\overline{v_P}$ or WTA and WTP (see relevant statistics in Appendices A, B and C). This implies that enjoying revelation of private information may not be so exceptional, at least in our sample and given our method for generating private information. This also emphasizes the importance of teasing risk preferences out of the actual utility of personal information.

Test of hypothesis 3 We now consider the number of safe choices and v_P across different ordering of monetary and privacy tasks in the experiment. Statistical tests¹⁹ and cumulative distribution function (fig. 4b) show a significant order effect in privacy task when considering the number of safe choices: subjects made more safe choices in the privacy task when it appeared before the monetary task. The p-value is even smaller in the model where table 8 is excluded. A similar effect is observed also in terms of the percentage

¹⁸ Pairwise comparison coefficient is 0.18 (p-value 0.01) for monetary task first and 0.59 (p-value 0.00) for privacy task first conditions.

¹⁹ Tests of the difference in the number of safe choices: two-sample Wilcoxon rank-sum test: Prob > |z| = 0.0141; t-test: Pr(T < t) = 0.0092; Kolmogorov-Smirnov equality-of-distributions test: corrected p-value is 0.035; ANOVA: coefficient is 0.7707, P>|t|=0.018; Kruskal-Wallis equality-of-populations rank test: Prob=0.0141. N=592 (312 and 280 in monetary and privacy tasks first conditions, respectively). Estimated statistical power is 0.6571.

of subjects who took only safe alternative in MPL tables 4-7 (20.48% when privacy task first vs. 12.39% when monetary task first)²⁰. 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 risk-averse behavior.

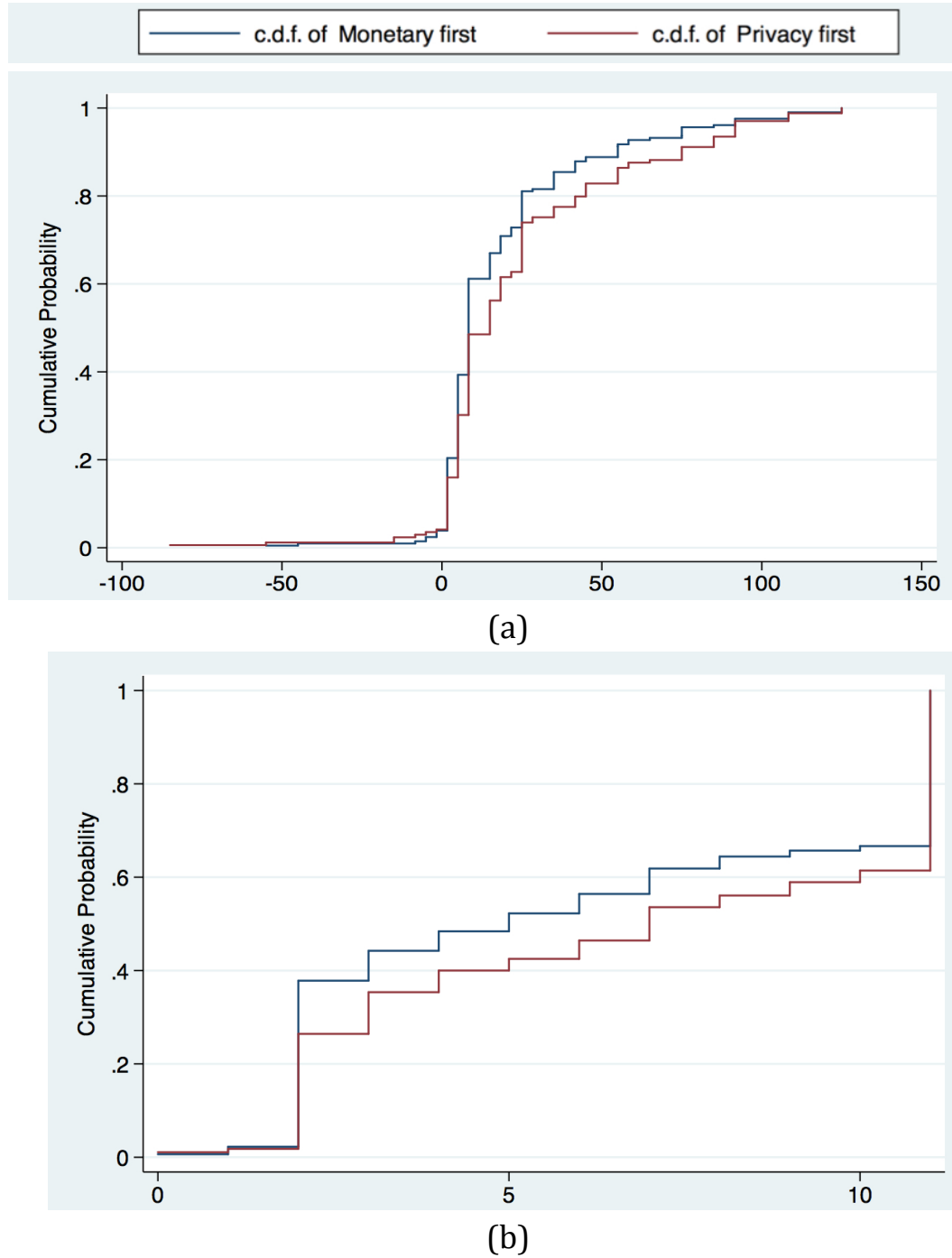
However, the regression in appendix E.1 shows that the order effect vanishes after being controlled for individual characteristics. We found that higher expected lottery outcomes drove participants to make fewer safe choices in privacy task.

Similarly, cumulative distribution function (fig. 4a) and statistical tests²¹ show that values of v_p are greater when privacy task appears first, but the regression coefficients (appendix E.2) are not significant.

²⁰ Excluding MPL table 4, proportional test $\Pr(Z < z) = 0.0105$. Pearson $\chi^2(1) = 5.3222$ ($\Pr = 0.021$). Estimated power is 0.6296.

²¹ Tests of the difference in v_p taking into account within subject variation: two-sample Wilcoxon rank-sum test: $\text{Prob} > |z| = 0.0199$; t-test: $\Pr(T < t) = 0.0282$; Kolmogorov-Smirnov equality-of-distributions test: corrected p-value is 0.082; ANOVA: coefficient is 5.6339, $P > |t| = 0.056$; Kruskal-Wallis equality-of-populations rank test: $\text{Prob} = 0.0199$. $N = 375$ (206 and 169 in monetary and privacy tasks first conditions, respectively). Estimated statistical power is 0.4684.

Figure 4 – Cumulative distribution function of: (a) v_P and (b) the number of safe choices across conditions



To summarize, although the order effect does not appear to be significant in the regressions, the statistical tests and c.d.f. of both v_P and the number of safe choices provide an evidence of the impact of the task order of v_P . Therefore, we have some qualified support of the hypothesis 3.

5 LIMITATIONS

The first possible limitation of our study is whether we managed to create enough privacy concern in the laboratory setting. Positive elicited WTA and WTP and positive implicit values of privacy from privacy lotteries provide evidence that at least some portion of subjects were not comfortable with personal information disclosure. Even though synthetically generated personal information could 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. Additionally, we 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.

A second possible limitation of our study relates to our non-parametric estimates of risk tolerance (RoR for monetary lotteries, v_p for privacy lotteries). Further investigation is warranted to examine whether using parametric estimates better explains observed behavior. However, RoR is very highly correlated with the parameter r in a standard CRRA utility function $u(x) = x^r$.

A third possible limitation relates to context-dependency. As our goal was not to derive directly a value attributed to privacy in the general population, but rather compare behaviors across conditions, we obtained results that are generalizable as far as groups in each treatment were similar in size and demographics, while other factors were kept fixed.

Finally, a fourth possible issue is with the artificiality and complexity of experimental designs in general. We dealt at least in part with this issue by improving the transparency of economic incentives with the use of the PRINCE system. Potential misunderstandings were mitigated by having subjects go through training tasks preceding the real experimental task and giving them the opportunity to ask for clarification at any moment during the

experiment. Low rate of inconsistent behavior (back-and-forth switching within a table) provides support for a high level of participants' attention and understanding of the tasks.

6 CONCLUSION

We presented a novel method for the implicit elicitation of the utility of personal information disclosure based on the choices in multiple price lists. We found that implicit and explicit measures differ substantially, and further research could improve the proposed methodology in predicting the personal information utility.

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 risk preferences. Personal information included individuals' name, surname, photo, and responses to the preliminary questionnaire about opinion on potentially sensitive and socially relevant topics. Additionally we manipulated the order in which monetary and privacy lotteries were presented to the subjects and level of control they had over personal information through introduction of privacy shock in a form of chance of eventual personal information disclosure regardless of the choices made. To provide transparent and tangible economic incentive we applied the prior incentive system (Johnson *et al.*, 2014).

We rejected the hypothesis of a treatment effect, whereby the introduction of a privacy shock under which personal information is compromised independently from participants' choices would have affected the willingness to take risk in privacy task. Taking control over privacy away from participants did not discourage them from protecting it, neither did it encourage them to protect it more. This would imply that privacy decisions are not affected by the current privacy environment where no one is ever sure to be secure about their privacy.

We also found a consistent positive relationship between risk aversion and willingness to take a risk of personal information disclosure. 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.

To the best of our knowledge, ours is the first work trying to separate two determinants of attitudes to privacy risk – risk aversion and basic willingness to disclose personal information. Although the method we use to disentangle those two components is rather coarse, it draws attention to the relevance of this issue. Indeed, we found many risk-averse people who were comparatively quite 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 disutility from its disclosure) should be risk-loving enough to “convince” them to expose their privacy to risk. This observation suggests that many apparently privacy protective choices 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 a larger proportion of “privacy exhibitionists”, *i.e.* subjects with negative utility for personal information, than would be inferred without correction. We need to investigate this relationship further by comparing risk-adjusted values for personal information and risk attitudes in future research.

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.

REFERENCES

Acquisti, Alessandro, Curtis R. Taylor, and Liad Wagman. "The economics of privacy." Conditionally accepted in the *Journal of Economic Literature* (2015).

Adjerid, Idris, *et al.* "Sleights of privacy: Framing, disclosures, and the limits of transparency." *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013.

Andersen, Steffen, *et al.* "Elicitation using multiple price list formats." *Experimental Economics* 9.4 (2006): 383-405.

Argyle, Michael. "Social pressure in public and private situations." *The Journal of Abnormal and Social Psychology* 54.2 (1957): 172.

Bardsley, Nick, Robin Cubitt, Graham Loomes, Peter Moffatt, Chris Starmer, and Robert Sugden. *Experimental economics: Rethinking the rules*. Princeton University Press, 2010.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. "Misplaced confidences privacy and the control paradox." *Social Psychological and Personality Science* 4.3 (2013): 340-347.

Beresford, Alastair R., Dorothea Kübler, and Sören Preibusch. "Unwillingness to pay for privacy: A field experiment." *Economics Letters* 117.1 (2012): 25-27.

Broadbent, Donald Eric. "A mechanical model for human attention and immediate memory." *Psychological review* 64.3 (1957): 205.

Broadbent, Donald Eric. "Task combination and selective intake of information." *Acta psychologica* 50.3 (1982): 253-290.

Charness, Gary, Uri Gneezy, and Alex Imas. "Experimental methods: Eliciting risk preferences." *Journal of Economic Behavior & Organization* 87 (2013): 43-51.

Correa, Teresa, Amber Willard Hinsley, and Homero Gil De Zuniga. "Who interacts on the Web?: The intersection of users' personality and social media use." *Computers in Human Behavior* 26.2 (2010): 247-253.

Cubitt, Robin P., Chris Starmer, and Robert Sugden. "On the validity of the random lottery incentive system." *Experimental Economics* 1.2 (1998): 115-131.

Culnan, Mary J., and Pamela K. Armstrong. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation." *Organization science* 10.1 (1999): 104-115.

Dinev, Tamara, and Paul Hart. "An extended privacy calculus model for e-commerce transactions." *Information Systems Research* 17.1 (2006): 61-80.

Dukas, Reuven. "Causes and consequences of limited attention." *Brain, Behavior and Evolution* 63.4 (2004): 197-210.

Egelman, Serge, et al. "Timing is everything?: the effects of timing and placement of online privacy indicators." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2009.

Egelman, Serge, Adrienne Porter Felt, and David Wagner. "Choice architecture and smartphone privacy: There's a price for that." *The Economics of Information Security and Privacy*. Springer Berlin Heidelberg, 2013. 211-236.

Farrell, Joseph. "Can privacy be just another good." *Journal on Telecommunications and High Technology Law*. 10 (2012): 251.

Feri, Francesco, Caterina Giannetti, and Nicola Jentzsch. "Disclosure of Personal Information under Risk of Privacy Shocks." In Press. Accepted Manuscript. *Journal of Economic Behavior & Organization* (2015).

Gideon, Julia, *et al.* "Power strips, prophylactics, and privacy, oh my!." *Proceedings of the second symposium on Usable privacy and security*. ACM, 2006.

Griffin, Dale W., and Carol A. Varey. "Towards a consensus on overconfidence." *Organizational Behavior and Human Decision Processes* 65.3 (1996): 227-231.

Griskevicius, Vladas, *et al.* "Going along versus going alone: when fundamental motives facilitate strategic (non) conformity." *Journal of Personality and Social Psychology* 91.2 (2006): 281.

Grossklags, Jens, and Alessandro Acquisti. "When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information." *WEIS*. 2007.

Hann, Il-Horn, *et al.* "Overcoming online information privacy concerns: An information-processing theory approach." *Journal of Management Information Systems* 24.2 (2007): 13-42.

Harris, Peter. "Sufficient grounds for optimism?: The relationship between perceived controllability and optimistic bias." *Journal of Social and Clinical Psychology* 15.1 (1996): 9-52.

Harrison, Glenn W., and E. Elisabet Rutstrom. "Risk aversion in the laboratory". 2008.

Harrison, Glenn W., *et al.* "Preferences over social risk." *Oxford Economic Papers* (2012).

Hey, John D., and Jinkwon Lee. "Do subjects separate (or are they sophisticated)?" *Experimental Economics* 8.3 (2005): 233-265.

Hoadley, Christopher M., *et al.* "Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry." *Electronic commerce research and applications* 9.1 (2010): 50-60.

Hollander, Edwin P. "Conformity, status, and idiosyncrasy credit." *Psychological Review* 65.2 (1958): 117.

Holt, Charles A. "Preference reversals and the independence axiom." *The American Economic Review* (1986): 508-515.

Holt, Charles A., and Susan K. Laury. "Risk aversion and incentive effects." *The American Economic Review* 92.5 (2002): 1644-1655.

Horowitz, John K., and Kenneth E. McConnell. "A review of WTA/WTP studies." *Journal of Environmental Economics and Management* 44.3 (2002): 426-447.

Huberman, Bernardo, Eytan Adar, and Leslie R. Fine. "Valuating privacy." *Security & Privacy, IEEE* 3.5 (2005): 22-25.

Janes, Leslie M., and James M. Olson. "Jeer pressure: The behavioral effects of observing ridicule of others." *Personality and Social Psychology Bulletin* 26.4 (2000): 474-485.

John, Leslie K., Alessandro Acquisti, and George Loewenstein. "The best of strangers: Context dependent willingness to divulge personal information." *Journal of Computer Research* (2009).

John, Leslie K., Alessandro Acquisti, and George Loewenstein. "Strangers on a plane: Context-dependent willingness to divulge sensitive information." *Journal of Consumer Research* 37.5 (2011): 858-873.

Johnson, Cathleen A., et al. "Prince: An Improved Method for Measuring Incentivized Preferences." *Available at SSRN 2504745* (2014).

Kahneman, Daniel. *Attention and effort*. Englewood Cliffs, NJ: Prentice-Hall, 1973.

Kang, Jerry. "Information privacy in cyberspace transactions." *Stanford Law Review* (1998): 1193-1294.

Keren, Gideon. "Calibration and probability judgements: Conceptual and methodological issues." *Acta Psychologica* 77.3 (1991): 217-273.

Krasnova, Hanna, Elena Kolesnikova, and Oliver Guenther. "" It Won't Happen To Me!": Self-Disclosure in Online Social Networks." *Amcis 2009 Proceedings* (2009): 343.

Kruglanski, Arie W., and Donna M. Webster. "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 (1991): 212.

Lachter, Joel, Kenneth I. Forster, and Eric Ruthruff. "Forty-five years after Broadbent (1958): still no identification without attention." *Psychological Review* 111.4 (2004): 880.

Laufer, Robert S., and Maxine Wolfe. "Privacy as a concept and a social issue: A multidimensional developmental theory." *Journal of Social Issues* 33.3 (1977): 22-42.

Leathern, Robert. "Online Privacy: Managing Complexity to Realize Marketing Benefits." *Jupiter Research*, 17 (2002).

Kim, Sei-Hill. "Opinion Expression as a Rational Behavior." *Paper presented at the Annual Meeting of the Association for Education in Journalism and Mass Communication, New Orleans, LA* (1999).

Maier, Johannes, and Maximilian R ger. Measuring risk aversion model-independently. No. 2010-33. Munich Discussion Paper, 2010.

Maslach, Christina, Joy Stapp, and Richard T. Santee. "Individuation: Conceptual analysis and assessment." *Journal of Personality and Social Psychology* 49.3 (1985): 729.

Miller, Louis, David Edward Meyer, and John T. Lanzetta. "Choice among equal expected value alternatives: Sequential effects of winning probability level on risk preferences." *Journal of Experimental Psychology* 79.3 (1969): 419-423.

Noelle-Neumann, Elisabeth. "The spiral of silence a theory of public opinion." *Journal of Communication* 24.2 (1974): 43-51.

Nordgren, Loran F., Joop Van Der Pligt, and Frenk Van Harreveld. "Unpacking perceived control in risk perception: The mediating role of anticipated regret." *Journal of Behavioral Decision Making* 20.5 (2007): 533.

Pashler, Harold E., and Stuart Sutherland. *The psychology of attention*. Vol. 15. Cambridge, MA: MIT press, 1998.

Pew Research Center survey. Americans' Attitudes about Privacy, Security and surveillance. 2015. Available at: <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>

Rivenbark, David R. *Valuing the Risk from Privacy Loss: Experimentally Elicited Beliefs Explain Privacy Behavior*. Working Paper. University of Central Florida, Orlando, FL, 2012.

Roth, Gerrit. *Predicting the Gap between Willingness to Accept and Willingness to Pay*. Diss. Ludwig-Maximilians-Universität München Munich, 2006.

Ross, Craig, et al. "Personality and motivations associated with Facebook use." *Computers in human behavior* 25.2 (2009): 578-586.

Shafir, Eldar, and Amos Tversky. "Thinking through uncertainty: Nonconsequential reasoning and choice." *Cognitive psychology* 24.4 (1992): 449-474.

Slovic, Paul. "Perception of risk." *Science* 236.4799 (1987): 280-285.

Snyder, Charles R., and Fromkin, Howard L. *Uniqueness: The pursuit of difference*. New York: Plenum (1980).

Solove, Daniel J. "A taxonomy of privacy." *University of Pennsylvania law review* (2006): 477-564.

Special Eurobarometer 431. Data protection. Report. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf (2015).

Symantec. State of privacy. Report. Available at: <https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf> (2015).

Tsai, Janice Y., et al. "The effect of online privacy information on purchasing behavior: An experimental study." *Information Systems Research* 22.2 (2011): 254-268.

Turow, Joseph, Michael Hennessy, and Nora Draper. "THE TRADEOFF FALLACY How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation." *The Annenberg School for Communication, University of Pennsylvania* (2015).

Tversky, Amos, and Daniel Kahneman. "Advances in prospect theory: Cumulative representation of uncertainty." *Journal of Risk and Uncertainty* 5.4 (1992): 297-323.

Wallsten, Thomas S. "An analysis of judgment research analyses." *Organizational Behavior and Human Decision Processes* 65.3 (1996): 220-226.

Weinstein, Neil D. "Why it won't happen to me: perceptions of risk factors and susceptibility." *Health Psychology* 3.5 (1984): 431.

Westin, Alan F. "Privacy and freedom." *Science and Society* 34 (3): 360-363 (1970).

Xu, Heng. "The effects of self-construal and perceived control on privacy concerns." *ICIS 2007 Proceedings* (2007): 125.

Zywica, Jolene, and James Danowski. "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 (2008): 1-34.

A. Summary of implicit and explicit measures of the utility of personal information disclosure, Euro

	v_P	$v_{P_{\overline{RoR}}}$	$\overline{v_{P_{\overline{RoR}}}}$	WTA [§]	WTP [§]
Observed values, %	90%	63%	90%	97%	99%
Min	-8.5	-7.9	-6.93	0	0
Max	12.5	11.7	11.54	200	30
Mean	2.08	0.02	0.4	16.12	1.92
Std. deviation	2.84	3.3	3.3	25.41	4.85
Median	0.83	-0.36	-0.17	10.0	0.0
Mean of average per subject	2.51	0.4	0.4	16.12	1.92
Proportion of subjects with negative average utility	2%	53%	58%	0%	0%

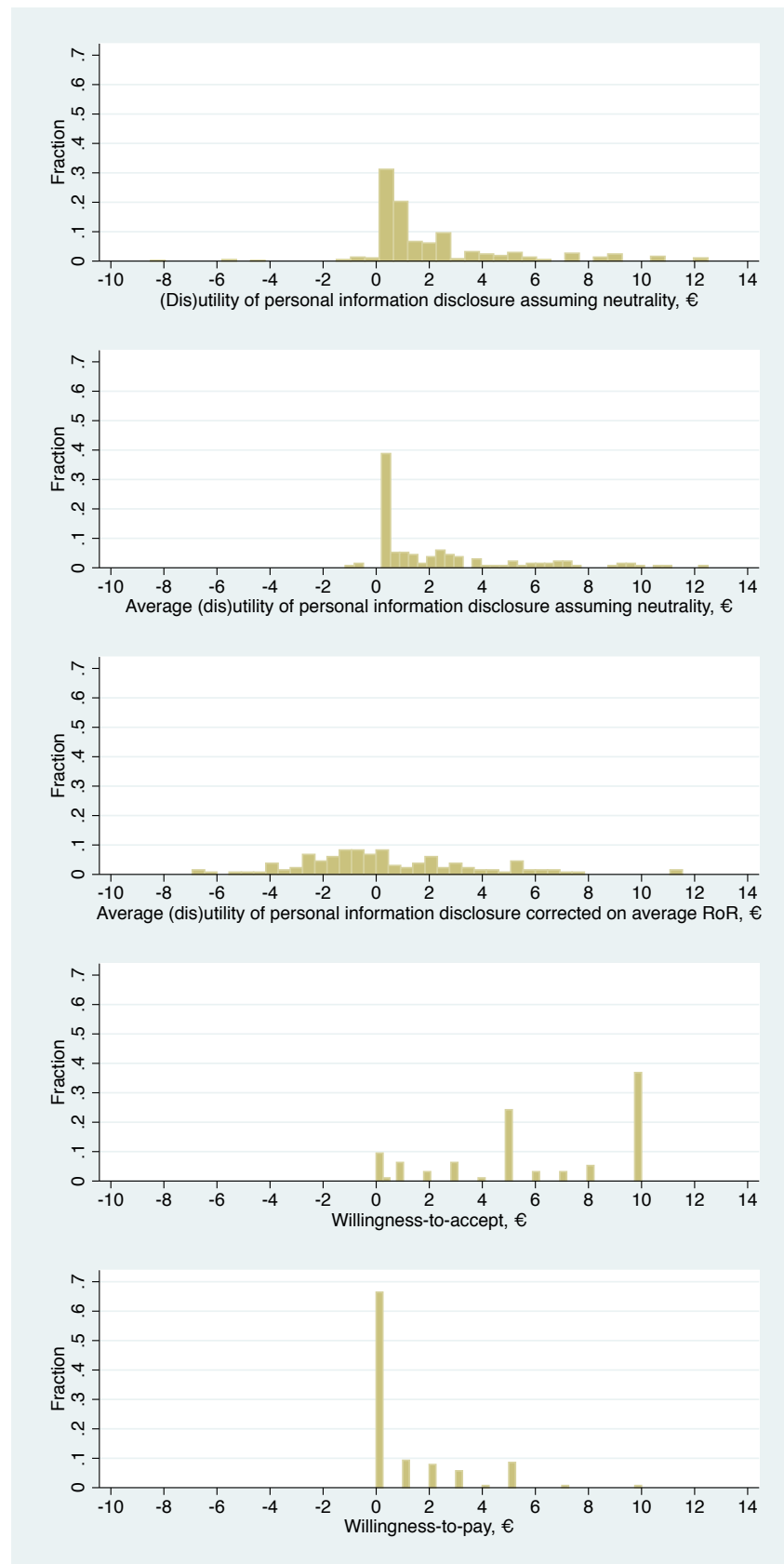
[§] Outliers (values that are 2 standard deviations away from the mean) are excluded. Before exclusion WTA and WTP ranged between €0 and €1000.

B. Basic statistics on explicit and implicit measures of personal information utility, in Euro

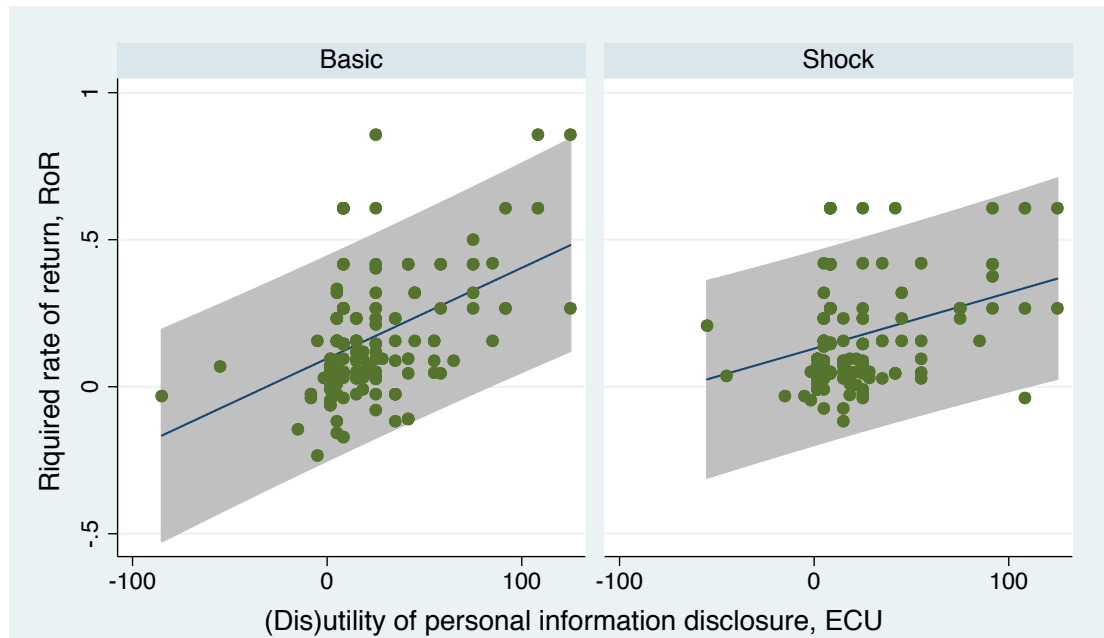
	By treatment		By condition		Total
	Basic	Shock	Monetary first	Privacy first	
v_P					
Mean	2.06	2.12	1.83	2.39	2.08
Median	0.83	0.83	0.83	1.5	0.83
Std. deviation	2.74	2.97	2.59	3.1	2.84
Observations	204	171	206	169	375
$\overline{v_P}$					
Mean	2.50	2.52	2.23	2.84	2.51
Median	1.28	1.06	0.61	1.83	1.06
Std. deviation	2.86	2.86	2.69	3.02	2.86
Observations	73	61	73	61	134
$v_{P_{\overline{RoR}}}$					
Mean	-0.09	-0.08	-0.3	0.41	0.02
Median	-0.25	-0.47	-0.76	-0.13	-0.36
Std. deviation	2.99	3.64	3.39	3.16	3.30
Observations	204	169	206	167	373
$\overline{v_{P_{\overline{RoR}}}}$					
Mean	0.51	0.26	0.14	0.72	0.4
Median	-0.11	-0.29	-0.67	0.16	-0.17
Std. deviation	3.08	3.55	3.57	2.91	3.3
Observations	73	60	73	60	133
WTA [§]					
Mean	16.16	16.02	14.59	17.78	16.12
Median	10.00	10.00	10.00	10.00	10.00
Std. deviation	26.68	23.99	21.64	29.03	25.41
Observations	79	65	75	69	144
WTP [§]					
Mean	1.87	1.98	1.58	2.29	1.92
Median	0	0	0	0	0
Std. deviation	5.29	4.29	3.94	5.67	4.85
Observations	80	66	76	70	146

[§] Outliers (values that are 2 std. deviations away from the mean) are excluded.

C. Distribution of explicit and implicit measures of personal information utility (in range between -€10 and €14, outliers for WTA and WTP excluded)



D. Scatterplot of RoR and utility of personal information disclosure assuming risk neutrality, v_P , by treatment, with prediction line of linear regression and 95% confidence interval for forecast



E.1 Panel random effect GLS regression of number of safe choices in privacy tasks

	Number of safe choices in privacy tasks			
	(1)	(2)	(3)	(4)
Privacy tasks first	0.771 ⁺ [-0.01,1.55]	0.772 ⁺ [-0.01,1.55]	0.772 ⁺ [-0.01,1.55]	0.606 [-0.16,1.38]
Shock treatment		0.0358 [-0.75,0.82]	0.0358 [-0.75,0.82]	-0.371 [-1.14,0.40]
Table 6			-1.088*** [-1.55,-0.62]	-1.383*** [-1.90,-0.86]
Table 7			-1.514*** [-1.98,-1.05]	-2.065*** [-2.69,-1.44]
Table 8			5.034*** [4.57,5.50]	5.203*** [4.70,5.71]
Q3: Familiar participants				-0.186 [-0.47,0.10]
Q6: WTA				-0.000177 [-0.00,0.00]
Q7: WTP				-0.00144 [-0.01,0.00]
Q8: Male				0.413 [-0.39,1.21]
Q16: General privacy concern				0.405 ⁺ [-0.03,0.84]
Westin's Pragmatist				-0.322 [-1.21,0.57]
Westin's Fundamentalist				0.952 ⁺ [-0.00,1.90]
Index of self-disclosure				-0.149 [-0.88,0.58]
Q32: Trust strangers				-0.150 ⁺ [-0.32,0.02]

Index of riskiness	-0.128 [-0.50,0.24]			
RoR	1.677* [0.14,3.21]			
Constant	5.994*** [5.46,6.53]	5.977*** [5.33,6.63]	5.369*** [4.66,6.08]	5.718*** [4.35,7.09]
chi2	3.788 ⁺	4.021	973.0***	973.6***

95% confidence intervals in brackets. Robust to multiple switching behavior.

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

E.2 Panel random effect GLS regression of v_P

	v_P			
	(1)	(2)	(3)	(4)
Privacy tasks first	6.123 [-3.50,15.75]	6.132 [-3.53,15.80]	6.673 ⁺ [-0.63,13.97]	3.470 [-5.13,12.07]
Shock treatment		0.396 [-9.27,10.06]	0.732 [-6.56,8.03]	-3.174 [-11.61,5.26]
Table 6			9.575 ^{***} [5.32,13.83]	6.676 ^{**} [2.46,10.89]
Table 7			17.48 ^{***} [13.25,21.72]	11.59 ^{***} [6.32,16.86]
Table 8			-46.53 ^{***} [-59.86,-33.21]	-48.20 ^{***} [-60.09,-36.31]
Q2: Ease				-6.015 ⁺ [-12.99,0.96]
Q3: Familiar participants				-3.226 [*] [-6.36,-0.10]
Q6: WTA				-0.00777 [-0.04,0.03]
Q7: WTP				-0.0291 [-0.09,0.03]
Q16: General privacy concern				2.095 [-2.71,6.90]
Westin's Pragmatist				-1.735 [-11.56,8.09]
Westin's Fundamentalist				12.06 [*] [1.35,22.77]
Index of self-disclosure				-1.665 [-9.70,6.37]

Q32: Trust strangers				-2.587** [-4.54,-0.63]
Index of riskiness				2.858 [-1.36,7.08]
RoR				17.29* [2.39,32.18]
Constant	21.32*** [14.84,27.81]	21.15*** [13.23,29.06]	11.51*** [4.96,18.07]	39.69*** [18.21,61.16]
chi2	1.555	1.549	142.1***	188.5***

95% confidence intervals in brackets. Robust to multiple switching behavior.

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

F. Summary of answers to the post-experimental questionnaire

Part A: About the experiment

Variables	Mean	Std. dev.	Min	Max
Q2. Ease (0 very difficult, 3 not difficult at all)	2.14	.61	0	3
Q3. Familiar participants	1.28	1.31	0	5
Share which knew another participant (s)	66%			
Q4. Appropriate remuneration	70%			
Q5. Trusting experimenters	97%			
Q6. WTA, €	36.2	142	0	1000
WTA excluding outliers, €	16.1	25.4	0	200
Q7. WTP, €	10	83.7	0	1000
WTP excluding outliers, €	1.92	4.85	0	30

Part B: Demographics

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	
< €500	43%
€501-800	41%
€801-1200	11%
€1201-2000	1%
>€2000	0%
No answer	4%

Part C: Privacy preferences, OSN activities and self-disclosure

Variables	Mean	Std. dev.	Min	Max
Q16. General privacy concern (0 not concerned at all, 3 very concerned)	1.12	.90	0	3
Q17. Provide PII to websites (0 very willing, 4 not willing at all)	2.68	.91	0	4
Q18. Provide PII to websites if compensated	57%			
Q19. 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	86%			

Q21. Victim of privacy invasion ²²	34%				
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%				

²² In the condition where monetary task appeared first the share of participants who personally have been a victim of privacy invasion is higher than in *privacy first* condition (42% versus 24%). Two-sample test of proportions $\Pr(Z < z) = 0.0103$. However, in regression analysis this control variable did never appear significant.

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	19.1	5.44	7	40	
Self-disclosure index	0	.58	-1.39	1.02	
Part D: Attitudes to risk and trust					
Variables	Mean	Std. dev.	Min	Max	
Q31. General risk attitude (0 averse, 10 risk seeking)	5.91	1.6	1	10	
Q32. Risk attitude (idem) in:					
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	
Riskiness index	0	1.14	-3.09	2.21	
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	33%				
Q37. People follow their own interests	83%				
Trustfulness index	0	.42	-1.14	1.01	

G. Preliminary questionnaire on opinions about potentially sensitive or socially relevant topics (translated from the Italian original)

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? (1. In favor; 2 Against)
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? (1. In favor; 2 Against)
3. Which of the following is the more appropriate penalty for rape? (1. Death; 2. Chemical castration; 3. Life imprisonment; 4. Prison sentence, less than life imprisonment)
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? (1. In favor; 2 Against)
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? (1. Should; 2. Should not)
6. Would you for any reason read your mate's email, SMS or pose as him/her online, without his/her knowledge and permission? (1. Yes, they shouldn't be keeping secrets anyway; 2. Yes, I'd be too curious not to; 3. Yes, if I suspected them of something; 4. Never)
7. Do you think it is morally justified or not justified to abort after discovering serious disability in the fetus? (1. Justified; 2. Not justified)

8. Are you in favor or against legislation of prostitution? (1. In favor; 2 Against)
9. Which of following substances should be prohibited? (More than one answer is allowed) (1. Alcohol; 2. Tabaco; 3. Cannabis; 4. Cocaine; 5. Acids (LSD, ecstasy, etc.); 6. Heroin; 7. Neither)
10. Are you in favor or against adoption of children by homosexual couples? (1. In favor; 2 Against)
11. Are you in favor or against the closure of Italian borders as a solution for the problem of illegal immigration? (1. In favor; 2 Against)
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)? (1. In favor; 2 Against)
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? (1. Plausible; 2. Not plausible)
14. Which of the following methods of birth contraception do you consider as the most appropriate? (1. Hormonal (oral pills, implants, injections, patches, etc.); 2. Barrier (condoms, cervical caps, diaphragms, sponges with spermicide, etc.); 3. Intrauterine devices; 4. Sterilization (surgical or chemical); 5. Behavioral (interrupted intercourse, fertility awareness method based on the menstrual cycle, sexual abstinence); 6. Neither)

H Instructions for shock treatment, “privacy task first” condition (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 $48+30$ ECUs = 78 ECUs = 7,8 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. The 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:

- a) If the outcome of the toss is strictly less than the probability of revelation then your information will be disclosed;
- b) 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:

1. 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.

2. 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 of personal information disclosure

If your personal information have 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 does not agree

- is **in favor** of **chemical castration** as appropriate penalty for rape, while 87% of other participants did not choose this option

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:

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

I Training questions for shock treatment, “privacy task first” condition (translated from the Italian original), with answers.

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

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?

- a) I get 13 ECU and the participation fee, my personal information remains anonymous.
- b) 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.
- c) I get only participation fee.
- d) I get nothing.

Answer: b).

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.

Option A: You get 37 ECU
 Option B: You get 53 ECU but with probability 10% you lose 14 of those ECU

Given your choice in Table 1, 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?

- a) 67 ECU
- b) 83 ECU
- c) 69 ECU
- d) 37 ECU
- e) 53 ECU
- f) 39 ECU

g) 30 ECU

h) 0 ECU

Answer: a (if A is chosen), b (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 if show up fee is 30 ECU?

- a) 20 ECU, personal information remains anonymous
- b) 20 ECU, personal information is disclosed
- c) 30 ECU, personal information remains anonymous
- d) 30 ECU, personal information is disclosed
- e) 50 ECU, personal information remains anonymous
- f) 50 ECU, personal information is disclosed
- g) 40 ECU, personal information remains anonymous
- h) 40 ECU, personal information is disclosed
- i) 40 ECU, personal information is disclosed if the outcome of the toss of the die is less of equal to 20
- j) 70 ECU, personal information remains anonymous
- k) 70 ECU, personal information is disclosed
- l) 70 ECU, personal information is disclosed if the outcome of the toss of the die is less of equal to 20
- m) I get nothing

Answer: k).

J Multiple price list menus of choices

J.1 Monetary task (MPL tables 1-4)

MPL table 1

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

MPL table 2

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

MPL table 3

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

MPL table 4

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

J.2 Privacy task (tables 5-8)

MPL

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

MPL table 6

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

MPL table 7

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

MPL table 8

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

K Final questionnaire

Part A.

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?

Part B.

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, Pharmaceuticals, 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)

Part C.

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 extend 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.

Part D.

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)