LUDWIG-
MAXIMILIANS-
UNIVERSITÄT
MÜNCHEN

VOLKSWIRTSCHAFTLICHE FAKULTÄT

Schudy, Simeon und Utikal, Verena:

'You must not know about me' - On the willingness to share personal data

'You must not know about me' -

On the willingness to share personal data

Simeon Schudy[*]   Verena Utikal[†]

This version: August, 2015

Abstract

Although understanding preferences for privacy is of great importance to economists, businesses and politicians little is known about the factors that shape the individual willingness to share personal data. This article provides three experimental studies with a total of 470 participants that help characterizing individual preferences for sharing personal data varying the characteristics of potential recipients. We find that participants' willingness to share personal data with anonymous recipients decreases with the number of recipients. However, social distance to the recipients and the extent of personal data a single recipient receives do not decrease the willingness to share personal data. Further, we provide a methodological insight by showing that verification of personal data is essential when eliciting privacy preferences.

JEL Classification: C90, C91, D80, D82

Keywords: preference elicitation, data privacy, informational privacy, experiment.

---

[*] Corresponding Author: Department of Economics, University of Munich, Geschwister-Scholl-Platz 1, D-80539 Munich, Germany, simeon.schudy@econ.lmu.de, +49(0)892180 9786.
[†] Department of Economics, University of Erlangen-Nuremberg, Germany, verena.utikal@fau.de.

"If this is the age of information, then privacy is the issue of our times."

Alessandro Acquisti, Laura Brandimarte and George Loewenstein (2015, p. 509)

1 Introduction

Every day people generate and share personal data[1], whether they visit their doctor, carry a smartphone, use an online search engine or share personal information on online social networks.[2] On the one hand, sharing personal data may benefit the individual as well as the society. For instance, sharing personal data on social networks can ease communication, build social capital, increase self-esteem or fulfill ego needs (see e.g. Acquisti et al., 2015; Steinfield et al., 2008; Toma and Hancock, 2013) and sharing GPS data from mobile phones or navigation systems may allow for efficient traffic management. On the other hand, sharing personal data can negatively affect individuals as well as the functionality of markets. Firms who have access to personal data may redistribute rents through price discrimination against a "transparent" consumer (see e.g. Acquisti and Varian, 2005; Odlyzko, 2003) and employers, who are able to access information shared on social networks, may discriminate against equally qualified applicants of certain religion or sexual orientation (Acquisti and Fong, 2013).[3]

Commonly, sharing personal data involves uncertainty about the identity of recipients. Firms may share their customers' data with subsidiaries and business partners.[4] Unknown individuals may access personal information shared on social networks[5] and data breaches may reveal data to unidentified recipients.[6] However, so far, little is known about the individual valuation of

---

[1] Throughout this paper we will understand personal data as "any information relating to an identified or identifiable natural person [...]; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (EU Directive 95/46/EC, EU 1995), Art. 2 (a); which is defined in a similar way in other legal contexts) see also Berendt (2012).

[2] See for instance Almuhimedi et al. (2014), Gross and Acquisti (2005), and Tsai et al. (2011).

[3] For an extensive discussion of the costs and benefits of sharing personal information see e.g. Acquisti et al. (2015). For a scientific discussion on data privacy in social networks see e.g. Warren (2008).

[4] This may happen unnoticed, as many consumers do not take the time to read statements on firms' information practices (see e.g. Beales and Muris, 2008, , p.113).

[5] See for instance Stutzman et al. (2013).

[6] Recent data breaches are documented e.g. at http://news.bbc.co.uk/2/hi/uk_news/7158019.stm (downloaded: February 2015), http://www.theguardian.com/business/2013/dec/19/target-breach-credit-card-accounts (downloaded:

personal data when recipients are unknown. Do people care about sharing their personal data with unknown recipients? Is there a direct disutility of passing on information to others? What are the crucial factors shaping the decision to share personal information? Does it matter how many recipients receive the data, which recipients receive the data and how much the recipients learn about the person sharing the data?

This paper provides three incentivized studies that elicit preferences for privacy[7] when personal data are shared with unidentified recipients. Varian (1997) points out that as soon as personal information has been shared with others, individuals have little control over the secondary use of their personal information. In Study 1, we pick-up Varian's conjecture and investigate whether the willingness to share personal information depends on the number of recipients with whom personal information is shared. Study 2 is related to the social distance hypothesis (see e.g. Akerlof, 1997). It has been shown that social distance plays a major role for economic behavior and can affect generosity, reciprocity and trust towards others (Binzel and Fehr, 2013; Etang et al., 2011; Hoffman et al., 1996; Netzer and Sutter, 2009). As trust in the recipients of personal information may be crucial when sharing personal data, we suspect that privacy valuations also depend on the social distance to recipients. We test this conjecture in Study 2. Study 3 focuses on the conceptualization of privacy. Privacy can be understood as the "control to access to the self" (Altman, 1975) or as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin, 1970). In Study 3 we build Westin's idea and test whether people have a preference for controlling what extent of personal information about them is communicated. Holding the amount of data that is shared and the number of recipients constant,

---

February 2015) or http://www.forbes.com/sites/quickerbettertech/2014/09/22/why-the-home-depot-breach-is-worse-than-you-think/ (downloaded: February 2015).

[7] We focus on information privacy, which encompasses the ability to control the collection, use and proliferation of information about oneself (Bundesverfassungsgericht, 1983; Preibusch, 2013, p. 1134; Stone et al., 1983). Information privacy reflects the definition of privacy as informational self-determination (see e.g.Westin, 1970). Other definitions of privacy relate for instance to physical or spatial understanding of privacy, i.e. to non-intrusion or seclusion (see e.g. Altman, 1975; Tavani, 2007)

we ask whether people care about the extent of personal information a single recipient receives, i.e. whether people care about the fact that their data may be aggregated or combined. In addition to the three studies, we investigate the role data verification when eliciting privacy preferences.

Study 1 shows that people's willingness to share personal information decreases with the number of recipients. Study 2 finds that, contrary to the hypothesis that people are not less willing to share personal information with socially distant recipients. The willingness to share address data with close recipients does not significantly differ from the willingness to share address data with distant recipients. Interestingly, for sharing body measures (weight and height), we even find the opposite tendency. Females request significantly higher monetary amounts for sharing data with close than distant recipients. Study 3 finds that, the willingness to share combined personal data as compared to share single pieces of information does not differ.

Our results speak to economists interested in the drivers of disclosure behavior on markets with asymmetric information and the potential for discrimination, to politicians who have to trade off privacy concerns of citizens with other desirable societal goals, to businesses, who are keen in finding out whether and which improvements in their privacy policies may result in a competitive advantage and which privacy intrusions are most disliked by their customers. Further we provide an important insight for researchers who are interested in understanding, characterizing and measuring preferences for privacy: Verification of personal data is essential when eliciting privacy preferences.

The focus of our studies is on sharing information with unknown recipients. Other incentivized studies on preferences for privacy have focused on sharing personal data with companies (Acquisti et al., 2013; Benndorf and Normann, 2014; Beresford et al., 2012) or focused on the publication of behavioral data from laboratory experiments on an internet website (Hermstrüwer and Dickert, 2013). Measuring the willingness to share personal information with a company is an important contribution to the literature as it directly measures concerns with

respect to commercial use of personal data. However, if data is shared with a company, the obtained privacy measure encompasses general trust or attitudes with respect to a specific company. Publishing behavioral data on a website nicely reflects the threat of the online availability of personal information but comes at the cost of including beliefs about the number of recipients in the elicited preference measure. The advantage of our experimental design is that it reduces confounding factors when measuring privacy concerns and allows us to exogenously vary three central aspects that may shape preferences for sharing personal data: the number of recipients, social distance to recipients, and the extent of personal data that a single recipient receives (i.e. how much combined information is shared).

The rest of the article is organized as follows. First, we explain the general experimental design and procedures of the three studies. Then, we explain the particular design features and results of each study. Additionally, we provide a robustness test that reveals the importance of data verification when eliciting privacy preferences. Finally, we discuss our results and their implications for economists, politicians and businesses.

2 Three studies on the value of data privacy and a robustness test

We conduct three distinct studies on the willingness to share personal data with unknown recipients (Study 1-3). Additionally we provide a robustness test on the importance of verification of personal data when eliciting privacy preferences (Study 4).

2.1 General experimental procedures

Each study is structured into four parts. In all studies, personal data is collected in Part 1 (including participants' full name). Personal data refers - depending on the treatment - either to address data and/or body data (i.e. weight and height), date of birth and eye color.

In *Part 2*, we elicit participants' minimum willingness to accept (WTA) sharing their personal data using the Becker-DeGroot-Marschak mechanism (BDM mechanism, Becker et al., 1964). The BDM is an incentive compatible elicitation mechanism that allows us to measure for what

amount participants are willing to share their personal data. We use a multiple price list format, i.e. participants specify on a decision sheet (BDM-sheet) for k different amounts (up to 13€, in steps of 0.50€)[8] whether or not they are willing to share their personal data with n anonymous recipients. Recipients receive personal data via email but do not participate in any of the studies.[9] Before participants fill in the decision sheet, they learn that at the end of the experiment one of the k amounts is randomly drawn, for which their decision is implemented (see Part 4).

In *Part 3* participants answer a questionnaire for which they receive a payment of 3€ at the end of the experiment (irrespective of their decisions).[10] The questionnaire contains questions on socio-demographics, personal characteristics and risk attitudes (see also Dohmen et al., 2011).

In *Part 4,* payment takes place. Payments are determined through an individual draw of a price offer. Each participant draws (randomly) one out of k cards from a bag, each showing one amount from the BDM-sheet. The randomly drawn amount corresponds to the offer the participant receives. If a participant had indicated on the BDM-sheet that she is willing to accept sharing her personal data for the drawn offer, the participant signed a consent form for the data transmission, the data was shared and the amount was paid to the participant. If a participant had indicated on the BDM-sheet that she is not willing to share the data for the drawn offer, the participant did not sign the consent form for the data transmission, the data was not sent to the recipient(s), and the drawn amount was not paid to the participant.

---

[8] In Study 2 offers include only positive amounts starting from 0.50€ to 13€. As Preibusch et al. (2013) have documented over-disclosure of web users in online forms (without compensation), we included the "0.00" amount in the BDM-sheet in Study 1, 3 and 4, which were conducted after Study 2.

[9] Data was sent (and amounts were paid) only if participants gave informed written consent for sharing their data. Recipients are students from a university in the same or in a different city. Recipients signed a consent form agreeing to receive the data via email. For Studies 1, 3 and 4 (as well as for the *close* treatments in Study 2) recipients were recruited from the subject pool of the University of Erlangen-Nuremberg. In the *distant* treatments in Study 2, recipients were recruited from the experimental subject pool at the University of Konstanz.

[10] In Study 3 participants received 4€ for the questionnaire due to changes in the local laboratory's regulations.

	Treatment	Type of data	Recipients	Participants		
				Male	Female	all
Study 1	*Number low*	Address data (full name, street, postal code, city)	*1 close*	28	30	58[11]
	Number medium		*20 close*	29	30	59
	Number high		*50 close*	23	26	49
Study 2	*Close address*	Address data (full name, street, postal code, city)	*50 close*	16	14	30
	Distant address		*50 distant*	14	13	27[15]
	Close body	Body data (full name, height, weight)	*50 close*	17	18	35[15]
	Distant body		*50 distant*	19	21	40
Study 3	*No bundling*	Address data, date of birth and eye color	*60 close*	29	31	60
	Bundling		*60 close*	29	24	53
Study 4	*No verification*	Address data (full name, street, postal code, city)	*20 close*	29	30	59
	verification		*20 close*	29	30	59
			Total:	233	237	**470**

Table 1: Number of participants across treatments

In total 470 subjects participated in the four studies (see Table 1 for the number of participants for each treatment). To avoid potential experimenter demand effects all studies use a between-subject design, i.e. each participant participates in exactly one treatment. The questionnaire and parts of the instructions were presented using z-Tree (Fischbacher, 2007). The minimum WTA was elicited with pen and paper. Participants were informed about the procedures and were aware that they were allowed to abort the experiment at any time (without receiving payment) or to take part without participating in *Part 1* (the data collection stage). In the latter case participants were paid for the questionnaire but made unpaid, hypothetical decisions in *Part 2*. We do not include the hypothetical decisions of the 4 subjects who did not participate in the data collection in *Part 1* in the data analysis.[12] All experiments were conducted at the Laboratory for Experimental Research in Nuremberg (LERN), Germany. Participants were recruited using ORSEE (Greiner, 2004) from the LERN subject pool which consists of undergraduate and graduate students. Session lasted 45 minutes on average.

---

[11] In each of the treatments *Number low, No bundling* and *Bundling* one participant refused data collection. In *Distant address* two participants refused data collection.

[12] The procedure for participants who refused data collection was identical to the procedure for all other subjects (except for decisions in Part 2, which were hypothetical). To minimize social influence, we made sure that participants were not observed by other participants during their decision whether or not to agree to the data collection.

2.2 Structure of the data analysis

To compare behavior across treatments we use four different outcome measures. First, we compare the likelihood of participants refusing data sharing, i.e. the fraction of participants rejecting all offers. Second, we focus on the likelihood of participants accepting all positive offers. Third, we identify each participant's minimum willingness to accept (WTA), i.e. the lowest amount the participant accepts to share her personal data and compare the median WTAs across treatments.[13] Forth, we compare the cumulative distribution functions (cdfs) of minimum WTAs across treatments. As we are interested in identifying factors that affect the costs of sharing personal data (holding everything else constant) we only compare treatments within each study and refrain from interpreting absolute values of WTAs, as these values may depend on the range of amounts offered in the BDM-sheet.[14]

2.3 Study 1: Number of recipients and the willingness to share personal data

Experimental design and procedures

In Study 1 we elicit participants' willingness to accept (WTA) sharing their *address data* with a number of anonymous recipients. We contrast three treatments: in treatment *number low* (n=58) there is only 1 recipient, in treatment *number medium* (n=59) there are 20 recipients, in treatment *number high* (n=49) there are 50 recipients.[15] In Part 1 of Study 1, participants fill out an address form at their individual desk. Participants put the address form into an envelope, but do not seal it. Participants are informed that address data that is transferred will be verified at the end of the experiment by checking their ID card. In Part 2, participants fill in the BDM-sheet, which consists of 27 different amounts (0€ to 13€, in steps of 0.50). The questionnaire in Part 3 is conducted as described in the general experimental procedures. In Part 4, individual draws take

---

[13] We do not know whether participants never accepting an offer in our experiment, would have accepted any offer above 13 euros. In order not include but not to inflate these participants' WTAs in the regression analysis, we assume that those participants have a minimum WTA of 13.50€.

[14] Benndorf and Normann (2014) compare BDM measures with take-it-or-leave-it and find strong differences in the elicited valuations. Hence interpreting absolute valuations of personal data can be misleading.

[15] In all three treatments recipients are socially close (i.e. students from the same university).

place. If a participant accepts data sharing for the drawn amount, the participant hands over the envelope to the experimenter, the data is verified and the experimenter pays the drawn amount. In case a participant rejects data sharing for the drawn amount, no amount is paid for the data and the participant keeps the envelope (i.e. her data).

Behavioral Predictions

Spreading personal data comes along with risks. Data might fall into the hands of someone who uses the information against the will or at the expense of the person sharing the information. Such risks are likely increasing in the number of recipients. On the other hand, it has been put forward that as soon as personal information has been shared with others, individuals have, anyways, little control over the secondary use of their personal information (Varian, 1997). In turn, the willingness to share personal information may not be affected by the number of recipients. Accordingly, we formulate the following two hypotheses:

Hypothesis 1A: The willingness to share personal data increases with the number of recipients.

Hypothesis 1B: The number of recipients does not affect the willingness to share personal data.

Results

Figure 1 and Table 2 provide evidence that the number of recipients affects participants' willingness to share personal data. The number of participants rejecting all positive offers increases with the number of recipients (see Figure 1, Panel (A)). The median WTA in *number low* is significantly lower than the median WTA in *number high*. Also the cumulative distribution functions (cdfs) of WTAs in *number low* versus *high number* differ significantly (see Figure 1, Panel (C)). Only the number of participants willing to share their data for all positive amounts does not differ significantly between treatments (see Figure 1, Panel (B)). The regression analysis in Table 3 confirms that *number high* significantly increases the minimum WTA, also when

8

adding controls for individual characteristics of participants.[16] We conclude with Result 1 which is in line with Hypothesis 1A.

Result 1: The willingness to share personal data is decreasing in the number of recipients.

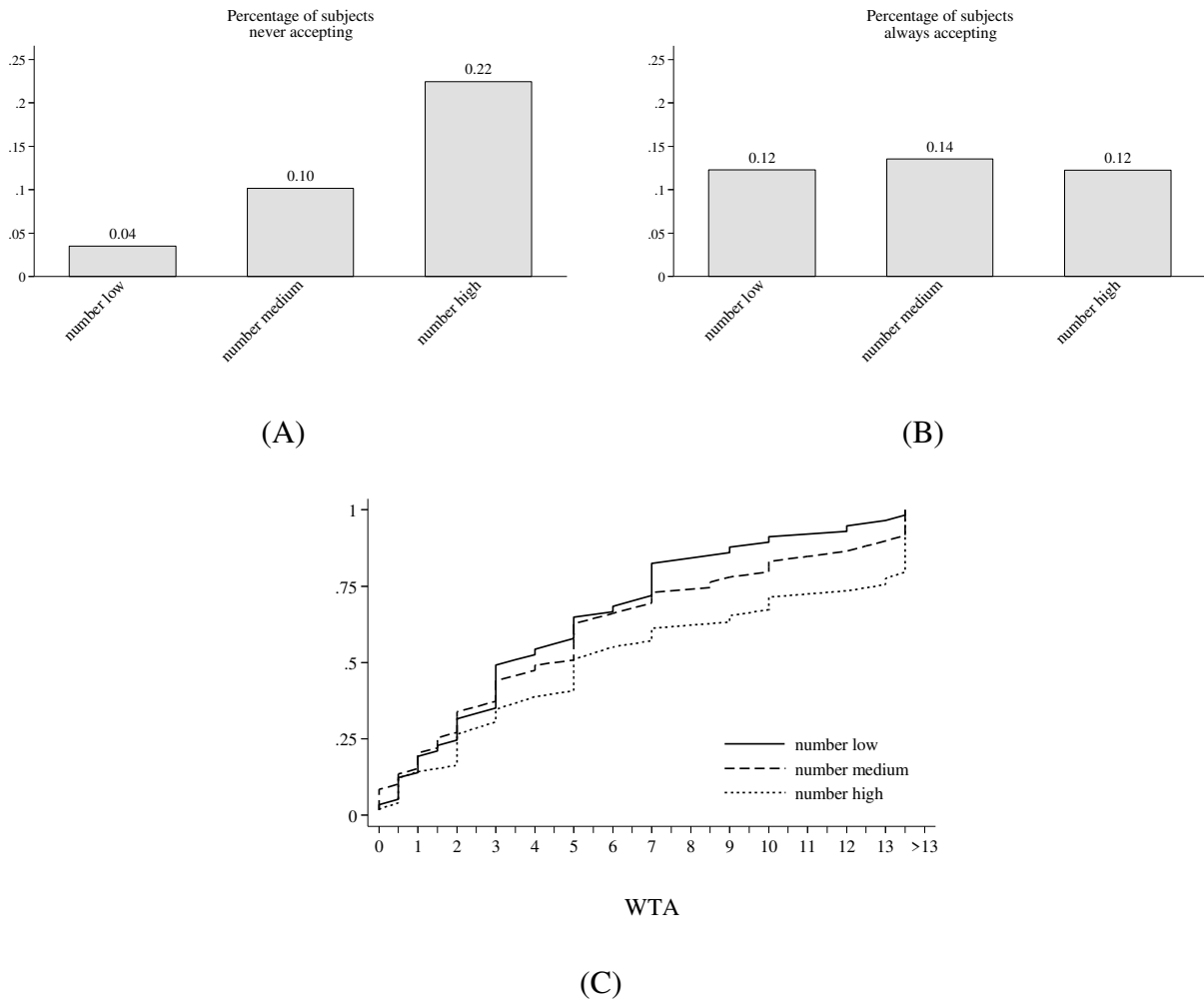(A)   (B)

WTA

(C)

Figure 1: Frequencies of never (A) or always accepting (B) and cdfs (C) of minimum WTAs in Study 1 for treatments *number low*, *number medium* and *number high* number

	Never accepted	Always accepted	Median WTA	cdf WTA
	p-value	p-value	p-value	p-value
Low vs. med	0.15	0.53	0.66	0.79
Low vs. high	0.003***	0.61	0.04**	0.10*
Med vs. high	0.07 *	0.54	0.12	0.52

Table 2: p-values for Fisher Exact Test (frequencies), Mann-Whitney-U-Test (Median WTA) and Kolmogorov-Smirnov-test (differences in WTA distributions), Study 1.

---

[16] Additional controls in Table 3 (as well as in Table 5, 7 and 9) refer to the field of study.

Dep. Variable	Minimum WTA Address Data	
	(1)	(2)
Number medium	0.621	0.339
	(0.753)	(0.777)
Number high	2.072**	1.756*
	(0.853)	(0.899)
Female		-0.638
		(0.710)
Belief on frequency of full name within Germany		0.935
		(1.122)
Age		-0.199
		(0.149)
Willingness to take risk when trusting in other people		-0.297*
		(0.176)
Constant	4.693***	10.773***
	(0.487)	(3.742)
Observations	165	165
R-squared	0.037	0.097
Additional Controls	No	Yes

Table 3: Regression analysis of Study 1. OLS, Dependent Variable.: Minimum WTA. Robust standard errors in parentheses, *** p<0.01, ** p<0.05, * p<0.1.

2.4 Study 2: Social distance and the willingness to share personal data

Experimental design and procedures

Study 2 employs a factorial 2x2 design. The first treatment dimension is social distance. We elicit participants' willingness to accept (WTA) sharing their data with 50 *close* or *distant* recipients. Our treatments reflect an understanding of social distance that focuses on the path length between trading partners in social networks (see e.g. by Binzel and Fehr, 2013 and Jackson, 2008), i.e. we vary the likelihood of knowing one or more recipients: *Close* recipients are students from the same university as the participants (University of Nuremberg). *Distant* recipients are students from the University of Konstanz (a city 400 km away from Nuremberg). The second treatment dimension is the type of data that is shared: *address data* or *body measures*. We chose to use two data types that differ in nature, as data types may be relevant for the importance of social distance. For instance, contact details such as address data may be more likely to be shared with close recipients (as close recipients are more likely to know the

participant and her contact details) whereas lifestyle profile information may be shared less frequently with close compared to distant recipients (as it may provide grounds for discrimination or feelings of unease or shame towards socially close recipients).[17]

In Part 1 of Study 2 a research assistant collected and verified participants' data.[18] The BDM-sheet in Part 2 consisted of 26 different amounts (0.50€ to 13€, in steps of 0.50). The questionnaire in Part 3 and payment in Part 4 are conducted as described in the general procedures.

Behavioral Predictions

For individualistic societies it has been shown that people trust more in others who are socially close (Buchan et al., 2006). As trust in the recipients of personal information may be crucial when sharing personal data, we suspect that privacy valuations also depend on social distance. If recipients come from a socially close group, following the literature of in-group-bias,[19] individuals will perceive socially close recipients as less likely to use information against their will or at their expense. Consequently we hypothesize:

Hypothesis 2: The willingness to share personal data decreases with the social distance of the recipients.

Results

We do not find evidence that the participants are more likely to share address data with socially close recipients (see Figure 2 and Table 4). The fraction of participants who are never willing to

---

[17] See also Huberman et al. (2007) who used a second-price auction experimental setup to study what amount individuals put on specific pieces of private information (such as their weight). They found that individuals requested more money to reveal information that was "abnormal" or "undesirable."

[18] To reduce social influence effects, the research assistant collected the personal information individually in the experimenter room before subjects made their decisions. To avoid that experimenter effects (e.g. mistrust in the specific research assistant) biases our treatment comparisons, the same research assistant elicits the data in all sessions of Study 2.

In the address data treatments the assistant verified and copied the participants' address (by ID participants' ID card) but not the participant's name. In the body data treatments the assistant measured body weight and height but not the participant's name. All forms were collected in order to receive body measures also from those participants who decided against data sharing. In case of data sharing we additionally verified the participant's name. Thus, collected data was only connected to the participants name in Part 2 and only when participant agreed to the data sharing.

[19] For an overview see, for instance, Tajfel and Turner (1986), Brown (2000), McDermott (2009) and Chen and Li (2009) .

share their data, the number of participants always willing to share and the median WTA do not significantly differ across treatments (see Figure 2 and Table 4). Likewise the cumulative distribution functions (cdfs) for *close address* and *distant address* do not differ significantly.
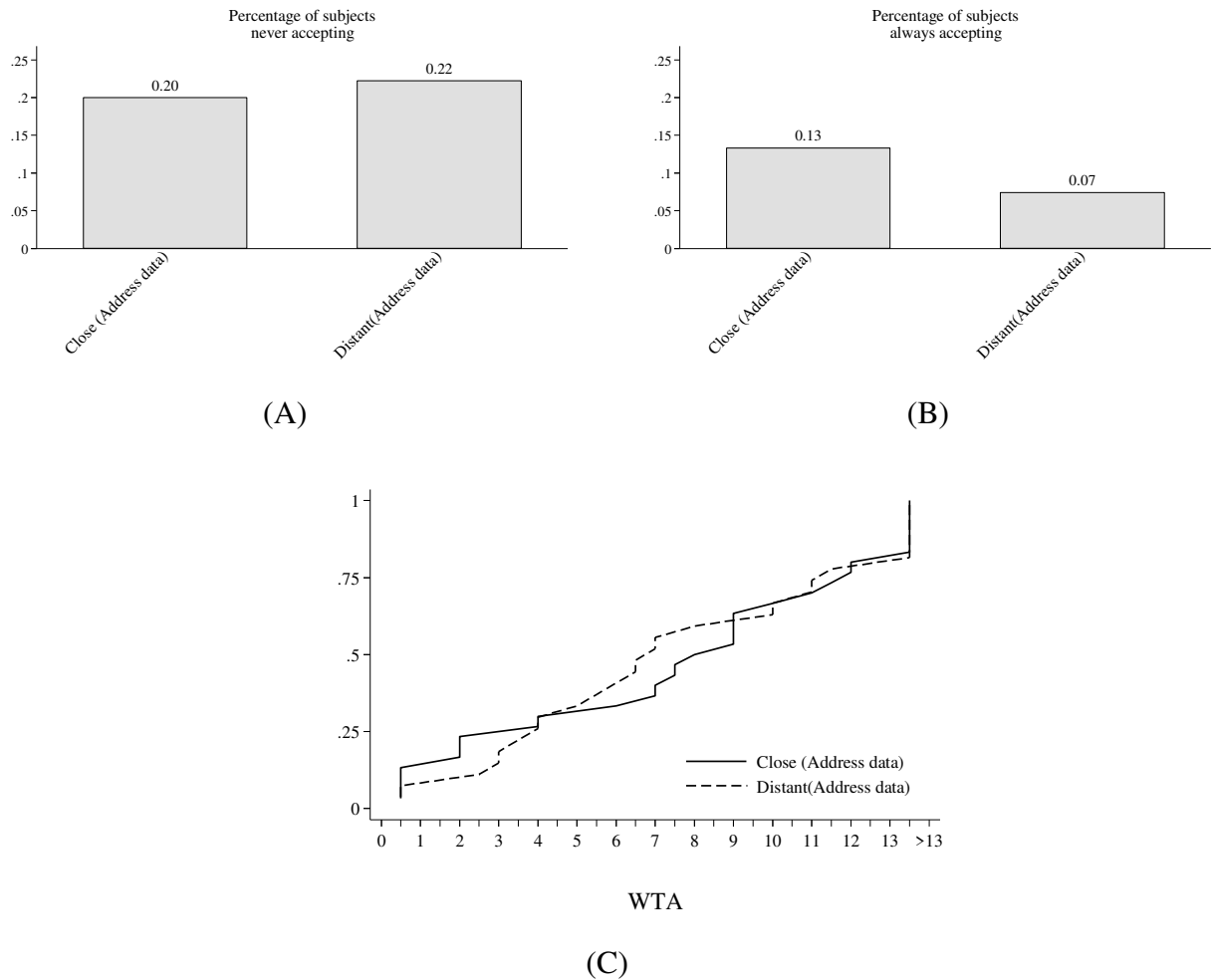
Percentage of subjects
never accepting

Percentage of subjects
always accepting

(A)

(B)

WTA

(C)

Figure 2: Frequencies of never (A) or always accepting (B) and cdfs (C) of minimum WTAs in Study 2 for treatments *close address* and *distant address*

	Never accepted	Always accepted	Median WTA	cdf WTA
	p-value	p-value	p-value	p-value
Close vs. *Distant*				
Address Data	0.49	0.43	0.57	0.56
Body measures	0.26	0.43	0.13	0.41

Table 4: p-values for Fisher Exact Test (frequencies), Mann-Whitney-U-Test (Median WTA) and Kolmogorov-Smirnov-test (differences in WTA distributions) in Study 2 (*close* vs. *distant*)

Percentage of subjects never accepting

Percentage of subjects always accepting

(A)   (B)

WTA

(C)
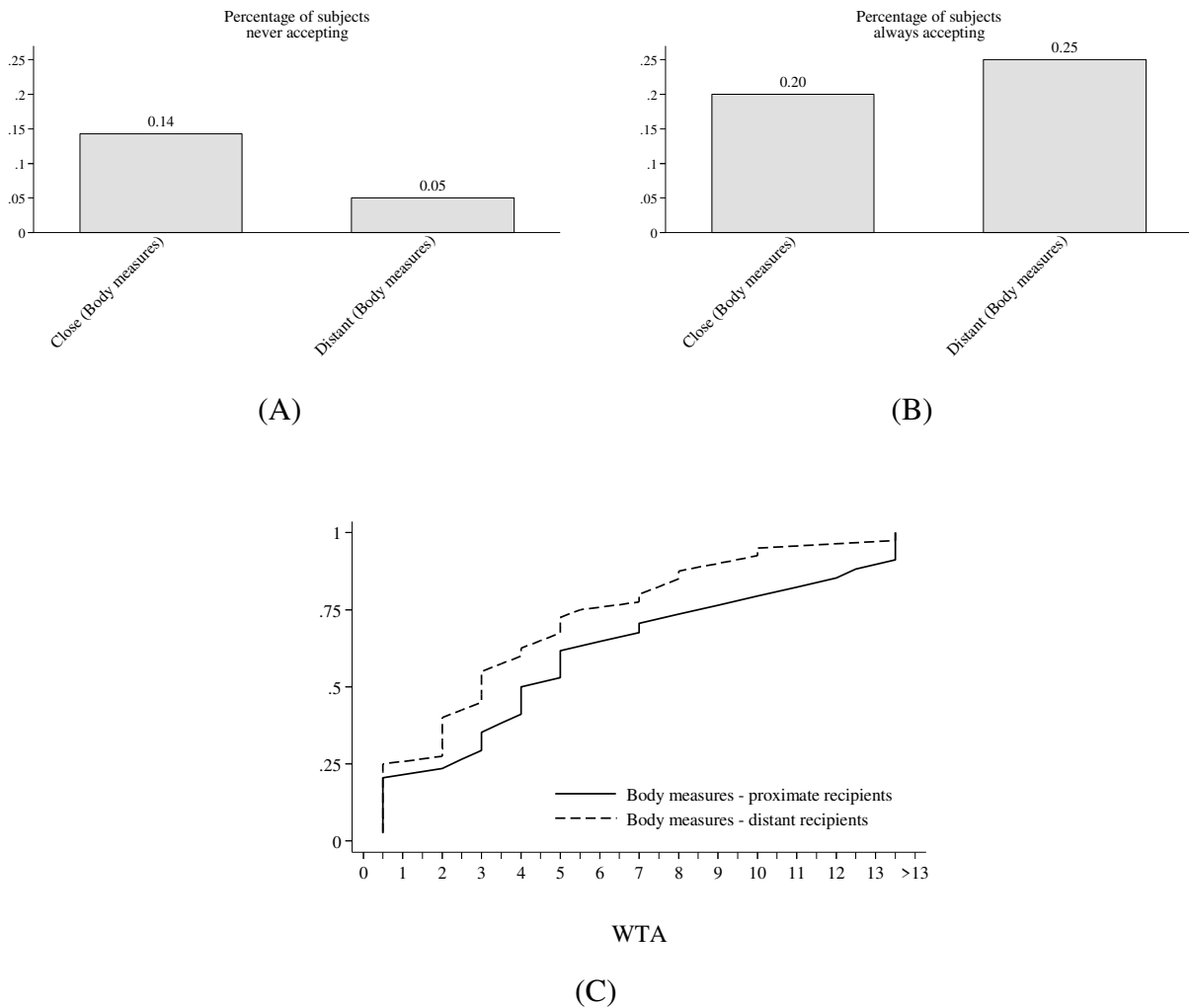
Figure 3: Frequencies of never (A) or always accepting (B) and cdfs (C) of minimum WTAs in Study 2 for treatments *close body* and *distant body*

Also, for body measures we do not find that people are more likely to share personal data with socially close recipients (see Figure 3). Instead, the data reveals a tendency that people are more willing to share their body data with distant rather than close recipients. The fraction of participants never sharing their data tends to be lower when sharing data with distant recipients and the number of participants always willing to share tends to be higher with distant recipients. Also the median WTA across treatments and the cdfs (see Figure 3, (C)) reflect this tendency.

13

Dep. Variable	Minimum WTA					
	Address Data			Body measures		
	(1)	(2)	(3)	(4)	(5)	(6)
Treatment Dummy (1= close, 0 = distant recipients)	0.550 (1.180)	0.799 (1.528)	1.117 (2.493)	1.564 (0.947)	1.687* (0.962)	-0.836 (1.156)
Female		2.810* (1.655)	2.605 (2.309)		2.259** (1.015)	-0.038 (1.267)
Treatment*Female			0.533 (3.157)			4.784** (1.902)
Belief on frequency of full name within Germany		1.095 (2.850)	1.055 (2.872)		-0.839 (1.597)	-1.190 (1.673)
Age		-0.105 (0.315)	-0.097 (0.329)		-0.181 (0.153)	-0.110 (0.146)
Willingness to take risk when trusting in other people		0.141 (0.267)	0.157 (0.286)		-0.333 (0.223)	-0.329 (0.210)
Constant	7.200*** (0.829)	6.758 (7.749)	6.328 (8.583)	4.113*** (0.566)	8.806* (4.757)	8.524* (4.501)
Observations	55	46	46	74	74	74
R-squared	0.004	0.185	0.185	0.038	0.234	0.310
Additional Controls	No	Yes	Yes	No	Yes	Yes

Table 5: Regression analysis of Study 2. OLS, Dependent Variable.: Minimum WTA. Robust standard errors in parentheses, *** p<0.01, ** p<0.05, * p<0.1.

The regression analysis in Table 5 shows that the treatment coefficient is small and insignificant for address data. Table 5 further shows that women request higher amounts, in particular when sharing body measures. This finding is in line with evidence by Manson et al. (1995) pointing out that women show a higher dissatisfaction with body shape regardless of ethnicity. Interestingly, this is in particular the case when body measures are to be shared with close recipients (see model (6)). We summarize the findings for address and weight data in Result 2 which does not confirm Hypothesis 2.

Result 2: People are not more willing to share personal information with close recipients.

Study 2 also provides evidence that participants care about what type of personal data is shared. Address data is considered more valuable than information on body measures, irrespective of whether the data is transferred to close or distant recipients. Pooling data for both,

close and *distant* recipients, the fraction of participants never willing to share amounts to 18% for address data and to 8% for body measures (Fisher exact test, two-sided, p=0.08). Vice-versa, the fraction of participants accepting all positive offers amounts to 11% for address data and to 23% for body measures (Fisher exact test, two-sided, p=0.06). The median of participants' request for address data is 7.50€ whereas it is 4€ for body measures (Wilcoxon rank-sum test, p-value= 0.0003). Also the cdfs of WTAs for address and body measures differ significantly (Kolmogorov Smirnov test, p=0.000).

2.5 Study 3: Combination of personal information

Experimental design and procedure
To study whether people care about how much combined information about them is revealed to a group of recipients, we employ two treatment conditions, in which we elicit participants' WTA for sharing personal data with two groups of recipients. The idea of the experimental design is to vary the amount of data that is transferred to each recipient group while holding the total amount of data and the number of recipients across treatments constant. In treatment *no bundling* participants decide on the BDM sheet whether or not they agree that three groups of 20 anonymous recipients each receive their personal data. If a participant agrees, the first group receives the participant's full name and address data, the second group receives the participant's full name and date of birth, and the third group receives the participant's full name and eye color. In treatment *bundling*, we instead elicit participants WTA for sharing their full name, address data, date of birth and eye color with the first group and sharing their full name with the second and third group. Thus, holding the number of recipients constant, treatment differences in WTAs will indicate whether participants prefer that many recipients will learn "little" about them or few recipients will learn "a lot" about them.

In Part 1 participants filled out an address form at their individual desk. Participants put the address form into an envelope, but did not seal it. Participants were informed that address data that is transferred will be verified at the end of the experiment by checking their ID card. The

BDM-sheet in Part 2 consisted of 27 different amounts (0.00€ to 13€, in steps of 0.50). The questionnaire in Part 3 and the payment procedure in Part 4 were conducted as described in the general procedures.

Behavioral Predictions

Westin (1970) described privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and *to what extent* information about them is communicated to others". Building on Westin's idea it seems natural to assume that people have a preference for controlling what extent of personal information about them is communicated to a single recipient or specific group of recipients. First, the more detailed information a recipient receives on an individual, the more useful is the information for the recipient. Second, the more information is received, the higher is the likelihood of misuse (such as selling, or using the data against the will of the data sharing individual). Holding the amount of transferred information and the number of recipients constant and varying the number of recipients receiving combinations of information, we therefore hypothesize:

Hypothesis 3: The willingness to share personal information decreases with the amount of information a single recipient receives.

Results

We find no evidence for Hypothesis 3. The fraction of participants who never accept sharing personal data is 0.17 in both treatments (see Figure 4, Panel(A)). The fraction of participants who are always willing to share is 0.12 in *bundling* and 0.13 in *no bundling* (see Figure 4, (B)). The median WTA is 4€ in *no bundling* and 5€ in bundling and all differences – also differences in cdfs - fail to be statistically significant (see Figure 4, (C) and Table 6). The regression analysis in Table 7 confirms these findings. Also when adding controls for individual characteristics of participants the bundling treatment has no significant effect on our participants' minimum WTA.

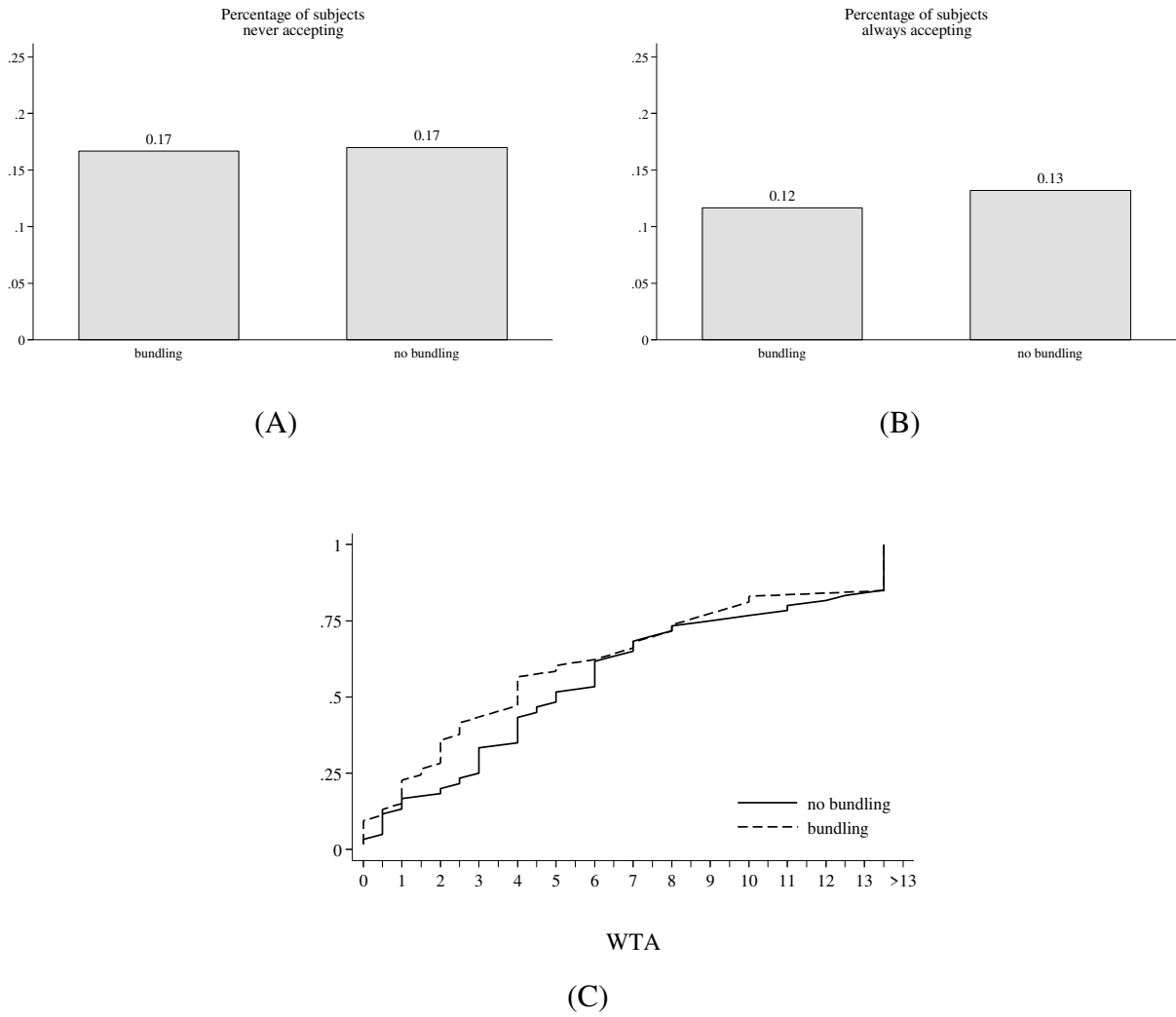**Result 3: Data bundling does not affect the WTA for sharing personal information.**

Figure 4: Frequencies of never (A) or always accepting (B) and cdfs (C) of minimum WTAs in Study 3 for treatments *no bundling* and *bundling*

	Never accepted	Always accepted	Median WTA	cdf WTA
	p-value	p-value	p-value	p-value
No bundling vs. *bundling*	0.58	0.51	0.28	0.27

Table 6: p-values for Fisher Exact Test (frequencies), Mann-Whitney-U-Test (Median WTA) and Kolmogorov-Smirnov-test (differences in WTA distributions), Study 3.

Dep. Variable	Minimum WTA	
	Address data, date of birth and eye color	
	(1)	(2)
Bundling	0.747	0.610
	(0.859)	(0.943)
Female		0.586
		(0.880)
Belief on frequency of full name within Germany		-0.392
		(1.575)
Age		-0.028
		(0.156)
Willingness to take risk when trusting in other people		-0.458**
		(0.190)
Constant	5.387***	8.363**
	(0.638)	(4.088)
Observations	113	113
R-squared	0.007	0.099
Additional Controls	No	Yes

Table 7: Regression analysis of Study 3. OLS, Dependent Variable.: Minimum WTA. Robust standard errors in parentheses, *** p<0.01, ** p<0.05, * p<0.1.

2.6 Study 4: The importance of data verification

Experimental design and procedure

Several studies have elicited incentivized measures of preferences for data privacy. In some of these studies the elicited data was verified (e.g. Huberman et al., 2005). In others, the willingness for sharing non-verified data was studied (e.g. Beresford et al., 2012) and in Benndorf and Normann (2014), both verified and non-verified data has been used to measure preferences for privacy. However, no study so far has investigated the direct impact of verification on the valuation of privacy. Study 4 focuses on this aspect and investigates the importance of verification of personal data when eliciting privacy preferences. We contrast the treatment *number medium* from Study 1 (from now on *verification*) in which personal data are verified with an otherwise identical treatment, in which personal data are not verified (*no verification*).

In *Part 1* of Study 4, participants fill out an address form at their individual desk. Participants put the address form into an envelope. In *verification* participants are instructed not to seal the envelope and informed that the data will be verified before payment. In *no verification*

participants are informed that the data will not be verified and instructed to seal the envelope. The BDM-sheet in *Part 2* consists of 27 different amounts (0.0€ to 13€, in steps of 0.50). The questionnaire in Part 3 is conducted as described in the general procedures. In *Part 4* if data sharing is agreed upon, the envelope is collected. In *verification* the experimenter opens the envelope, verifies the participant's name and address data using her ID card and pays the drawn amount in addition to the 3€ for answering the questionnaire. In *no verification* the experimenter does not verify the data and pays the drawn amount without opening the envelope. In both treatments, if the participant decides to reject data sharing for the drawn amount, the participant keeps the envelope, the ID card is not verified, and the drawn amount is not paid.

Behavioral Predictions
We suspect that the valuation of privacy depends on whether or not data is verified. In particular, participants who value their personal data may be inclined to misreport their data and request lower amounts for sharing that data when data is not verified. We therefore hypothesize:

Hypothesis 4: The willingness to share personal data increases when the personal information is not verified.

Results
Study 4 provides evidence for Hypothesis 4, i.e. data verification affects participants' willingness to share personal data. As Figure 5 and Table 8 show, the fraction of participants not sharing personal data is significantly higher when personal data is verified. The fraction of participants always sharing personal data tends to be lower (0.14) in *verification* than in *no verification* (0.22) but the difference fails to be statistically significant. Also the median WTA reflects the tendency that non-verified data is valued less (3€ in *no verification* and 5€ in *verification*) but the difference is not statistically significant. The cumulative distribution functions (cdfs) reflect the tendency of lower valuations if data is not verified as well but do not differ significantly (see Table 8). Is verification nevertheless an important issue? Misreporting of personal data involves

dishonesty and the impact of our verification treatment on WTAs may thus also depend on individual lying costs. As there is evidence that women tend to behave more honestly than men in a variety of experimental tasks (see e.g. Rosenbaum et al., 2014, p. 191) we further analyze the effects of verification separately for male and female participants. As suggested by the literature on dishonesty, we find that differences in valuations across treatments (*verification* versus *no verification*) are solely driven by male participants. The fraction of males not sharing personal data, median WTA and cdfs, differ significantly. Solely the fraction of male participants willing to share their data for all positive in verification (7 percent) compared to *no verification* (22 percent) fails to differ significantly (p-value = 0.12). For females, none of the measures differs significantly (see Table 8, last two columns).

all
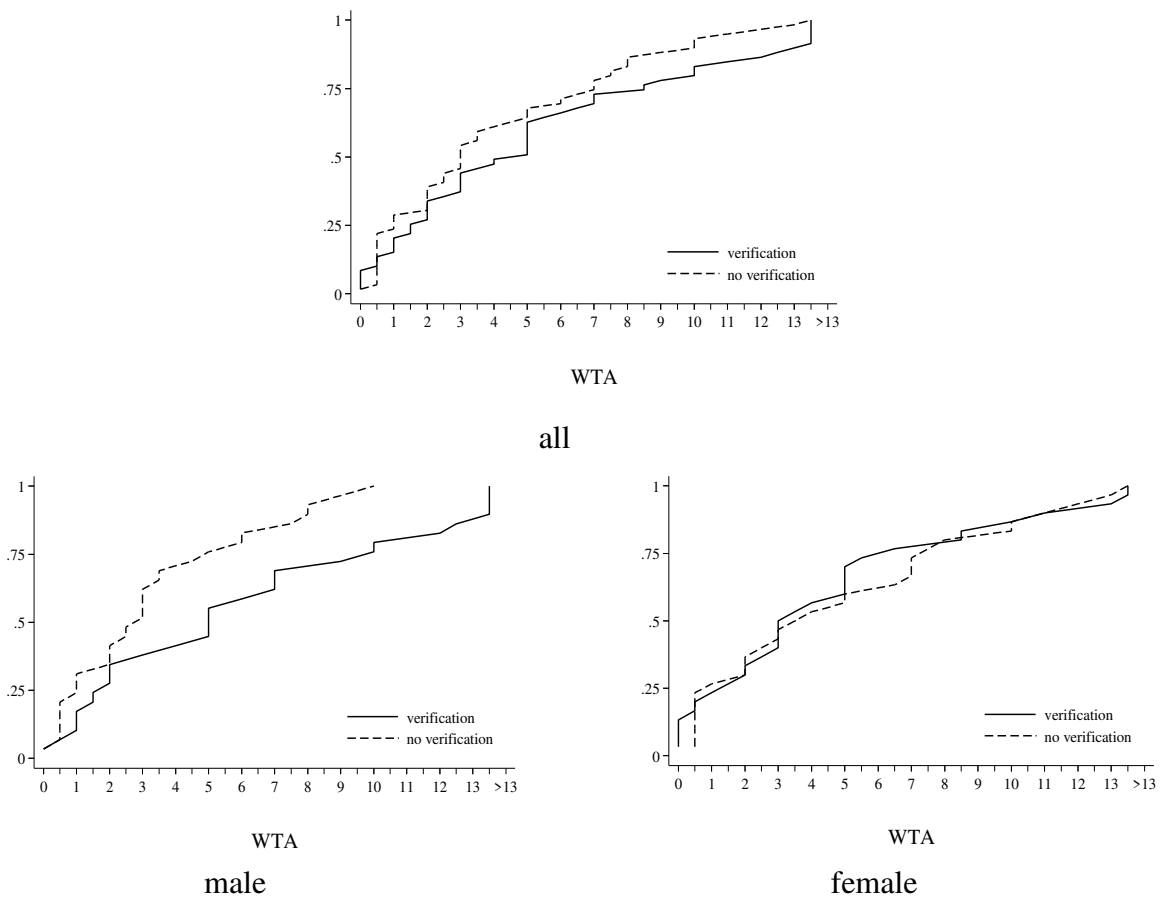
male

female

Figure 5: Cdfs of minimum WTAs in Study 4 for treatments *verification* and *no verification*, for all, male and female participants

	Participants					
	all		male		female	
Verification	yes	no	yes	no	yes	no
Fraction of participants never willing to share	0.10	0.02	0.14	0.02	0.07	0.02
Fisher Exact Test, p-value	0.06*		0.06*		0.50	
Fraction of participants willing to share for all positive amounts	0.14	0.20	0.07	0.22	0.20	0.22
Fisher Exact Test, p-value	(0.19)		(0.12)		0.50	
Median WTA	5.00	3.00	5.00	3.00	3.25	3.75
Mann-Whitney-U-Test, p-value	0.23		0.04**		0.73	
Kolmogorov-Smirnov-test, p-value	0.53		0.06*		0.85	

Table 8: Fractions of participants always/ never accepting and medians including p-values of non-parametric test results for treatments differences (*no verification* vs. *verification*) in Study 4.

Dep. Variable	Minimum WTA		
	Address Data		
	(1)	(2)	(3)
Verification	1.102	0.987	2.621**
	(0.744)	(0.790)	(1.069)
Verification*Female		-0.008	-3.242**
		(0.837)	(1.519)
Female			1.626
			(1.037)
Belief on frequency of full name		0.418	0.186
within Germany		(1.360)	(1.364)
Age		-0.108	-0.102
		(0.143)	(0.143)
Willingness to take risk when trusting in other people		-0.048	-0.103
		(0.178)	(0.176)
Constant	4.212***	6.716*	6.101
	(0.474)	(3.836)	(3.825)
Observations	118	118	118
R-squared	0.019	0.041	0.079
Additional Controls	No	Yes	Yes

Table 9: Regression analysis of Study 4. OLS, Dependent Variable: Minimum WTA. Robust standard errors in parentheses, *** p<0.01, ** p<0.05, * p<0.1.

The regression analysis in Table 9 confirms the non-parametric findings, also when adding controls for individual characteristics of participants. We conclude with Result 4.

Result 4: Verification of personal data increases the fraction of males not willing to share their data.

3 Discussion and Conclusion

Identifying factors that shape the valuation of personal information with unknown recipients is difficult using field data. First, the true benefits of sharing personal data in the field are usually unknown to the researcher. Second, people may not always be aware of the fact that their data is shared with unknown recipients in the field (Acquisti et al., 2015, , p. 509). To avoid these difficulties and elicit the valuation of privacy in an unbiased way, we conducted a series of controlled laboratory experiments, in which participants decided on whether or not to share (verified) personal data. The experiments made the benefits from sharing personal data explicit and the anonymity of recipients salient. The laboratory experiment allowed us to systematically vary factors that may change the costs of sharing information with unknown recipients while holding everything else, in particular the benefits from sharing the information, constant.

Our findings provide several insights into preferences for privacy: First, most of our participants make a tradeoff when being confronted with the opportunity to share their personal data, i.e. the share of people always accepting or never accepting to share personal data is low in most of the treatments. Also, we observe a large heterogeneity of valuations of personal data, which are affected by several factors that shape the willingness to share personal information with unknown recipients. We find that people care whether few or many others receive their personal information. Consequently, the disutility of sharing personal data is increasing in the number of recipients when it is salient how many others directly receive the personal data. This is interesting given that"[f]ew consumers actually take the time to read [information on firms' information practices], understand them, and make a conscious choice about whether to opt out of information sharing ..." (Beales and Muris, 2008, p.113).

Second, and contrary to the literature on in-group favoritism (see e.g. Brown, 2000; Chen and Li, 2009; McDermott, 2009 and Tajfel and Turner, 1986) people do not favor sharing data with closer recipients. For sharing contact details, the valuation of personal information does not

significantly differ. For sharing lifestyle information, females even discriminate against closer recipients, i.e. they dislike sharing information on their size and weight with close recipients much more than with distant recipients. Also, and in line with previous research (see e.g. Benndorf and Normann, 2014), Study 2 reveals that people value different types of data differently: our participants request on average higher amounts when sharing address data compared to body measures. This difference may for instance reflect the fear of data misuse people have in mind when sharing their personal data.

Third, and most astonishingly, our participants do not seem to care whether different pieces of their personal information are combined. Participants request similar amounts of money to share their personal data, irrespective of whether three recipient groups receive one piece of personal information each in addition to the full name of the participant or one group of recipients receives all pieces of information while the two other groups receive only their name. This finding is at odds with the intuition that people dislike giving away "too much" information to a single recipient group but fits well with the fact that many people are not reluctant to use only one search engine or buy all their products at the same online store, adding data every day to the profile the company may generate. While our aim was to test whether people dislike that their data is combined – even if such a combination is not necessarily informative to the recipient – it will be interesting to see, whether the intuition of sharing too much information only relates to sharing combined information for which the sum of information is indeed (and saliently) larger than its parts.

Our results are important for economists, politicians, businesses and researchers, From an economic perspective the results shed light on the costs of individuals when sharing data. Our evidence shows that costs are heterogeneous and that data privacy is not a sacred value. Many people are willing to trade off costs and benefits from sharing personal data and value different data types differently. Further, if people dislike sharing data the more the larger the number of

recipients is, our findings suggest that consumers outside the laboratory - who are frequently inattentive to firms' data sharing practices (e.g. with subsidiaries and business partners) - may not act in the best of their interest. Policies may thus focus on the clarity and salience of firms' information practices that may ease consumers behaving in the best of their interest. Also, businesses themselves, who are interested in better privacy practices, may benefit from sharing their costumers' data with a small number of recipients and from clarifying how few recipients potentially deal with their customers' data. Vice-versa businesses may also take this finding as a warning that data breaches may matter, in particular, if many recipients receive the data. Finally, speaking to researchers interested in a better understanding of the concept of privacy we provide three important insights. First, we find no evidence for both, the intuition that sharing data with closer recipients is preferred to sharing data with distant recipients and the intuition that people dislike giving away "too much" information to a single recipient group. Second, we see that many people are willing to give up substantial monetary amounts to avoid sharing their personal data. Third, we show that not verifying personal data that is to be shared may result in unpredictable biases in the measures for privacy preferences. Hence we strongly recommend data verification in future research on privacy preferences.

Acknowledgement

References

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.

Acquisti, A., Fong, C.M., 2013. An experiment in hiring discrimination via online social networks. *Available at SSRN 2031979*.

Acquisti, A., John, L.K., Loewenstein, G., 2013. What is privacy worth? *The Journal of Legal Studies*, 42(2), 249-274.

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

Akerlof, G.A., 1997. Social distance and social decisions. *Econometrica: Journal of the Econometric Society*, 1005-1027.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L., Agarwal, Y., 2014. Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging.

Altman, I., 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.

Beales, J.H., Muris, T.J., 2008. Choice or consequences: Protecting privacy in commercial information. *The University of Chicago Law Review*, 109-135.

Becker, G.M., Degroot, M.H., Marschak, J., 1964. Measuring Utility by a Single-Response Sequential Method. *Behavioral Science*, 9(3), 226-232.

Benndorf, V., Normann, H.-T., 2014. *The willingness to sell personal data*, DICE Discussion Paper No. 143.

Berendt, B., 2012. More than modelling and hiding: towards a comprehensive view of Web mining and privacy. *Data Mining and Knowledge Discovery*, 24(3), 697-737.

Beresford, A.R., Kübler, D., Preibusch, S., 2012. Unwillingness to Pay for Privacy: A Field Experiment. *Economics Letters*, 117, 25-27.

Binzel, C., Fehr, D., 2013. Social distance and trust: Experimental evidence from a slum in Cairo. *Journal of Development Economics*, 103(0), 99-106.

Brown, R., 2000. Social identity theory: Past achievements, current problems and future challenges. *European Journal of Social Psychology*, 30(6), 745-778.

Buchan, N.R., Johnson, E.J., Croson, R.T.A., 2006. Let's get personal: An international examination of the influence of communication, culture and social distance on other regarding preferences. *Journal of Economic Behavior & Organization*, 60(3), 373-398.

Bundesverfassungsgericht, 1983, Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 (Volkszählung). BVerfGE 65, 1. Bundesverfassungsgericht [Federal Constitutional Court of Germany].

Chen, Y., Li, S.X., 2009. Group identity and social preferences. *The American Economic Review*, 99(1), 431-457.

Dohmen, T., Falk, A., Huffman, D., Sunde, U., Schupp, J., Wagner, G.G., 2011. Individual risk attitudes: Measurement, determinants, and behavioral consequences. *Journal of the European Economic Association*, 9(3), 522-550.

Etang, A., Fielding, D., Knowles, S., 2011. Does trust extend beyond the village? Experimental trust and social distance in Cameroon. *Experimental Economics*, 14(1), 15-35.

Greiner, B., 2004, *An online recruitment system for economic experiments*. In: K. Kremer, V. Macho (Eds.). Forschung und wissenschaftliches Rechnen GWDG Bericht 63. Gesellschaft für Wissenschaftliche Datenverarbeitung, Göttingen, pp. 79-93.

Gross, R., Acquisti, A., 2005, Information revelation and privacy in online social networks. Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, pp. 71-80.

Hermstrüwer, Y., Dickert, S., 2013. Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten. *MPI Collective Goods Preprint*(2013/15).

Hoffman, E., McCabe, K., Smith, V.L., 1996. Social Distance and Other-Regarding Behavior in Dictator Games. *American Economic Review*, 86(3), 653-660.

Huberman, B., Adar, E., Fine, L.R., 2005. Valuating privacy. *Security & Privacy, IEEE*, 3(5), 22-25.

Jackson, M.O., 2008, *Social and economic networks*, vol. 3. Princeton University Press Princeton.

Manson, J.E., Willett, W.C., Stampfer, M.J., Colditz, G.A., Hunter, D.J., Hankinson, S.E., Hennekens, C.H., Speizer, F.E., 1995. Body weight and mortality among women. *New England Journal of Medicine*, 333(11), 677-685.

McDermott, R., 2009. Psychological approaches to identity: Definitions, measurement and experimentation. *Measuring Identity: A Guide for Social Science Research, Cambridge, UK: Cambridge University Press, forthcoming*.

Netzer, R.J., Sutter, M., 2009. *Intercultural trust. An experiment in Austria and Japan*, Working Papers in Economics and Statistics.

Odlyzko, A., 2003, Privacy, economics, and price discrimination on the Internet. Proceedings of the 5th international conference on Electronic commerce. ACM, pp. 355-366.

Preibusch, S., 2013. Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, 71(12), 1133-1143.

Preibusch, S., Krol, K., Beresford, A.R., 2013, *The privacy economics of voluntary over-disclosure in Web forms*. The Economics of Information Security and Privacy. Springer, pp. 183-209.

Rosenbaum, S.M., Billinger, S., Stieglitz, N., 2014. Let's be honest: A review of experimental evidence of honesty and truth-telling. *Journal of Economic Psychology*, 45, 181-196.

Steinfield, C., Ellison, N.B., Lampe, C., 2008. Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology*, 29(6), 434-445.

Stone, E.F., Gueutal, H.G., Gardner, D.G., McClure, S., 1983. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology*, 68(3), 459.

Stutzman, F., Gross, R., Acquisti, A., 2013. Silent listeners: The evolution of privacy and disclosure on facebook. *Journal of privacy and confidentiality*, 4(2), 2.

Tajfel, H., Turner, J., 1986, *The Social Identity Theory of Intergroup Behavior*, In *The Psychology of Intergroup Relations,* ed. Stephen Worchel and William Austin. 7-24. Chicago: Nelson-Hall.

Tavani, H.T., 2007. Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, 38(1), 1-22.

Toma, C.L., Hancock, J.T., 2013. Self-affirmation underlies Facebook use. *Personality and Social Psychology Bulletin*, 39(3), 321-331.

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

Varian, H.R., 1997, *Economic aspects of personal privacy*. in: Privacy and Self-Regulation in the Information Age. NTIA, United States Department of Commerce.

Warren, J., 2008, *Self-imposed violations of privacy in virtual communities*. UTSA, College of Business.

Westin, A.F., 1970, *Privacy and freedom*. Atheneum, New York.

Appendix

The appendix contains all material from the treatment number medium of Study 1 (translated from German).

A1 On screen instructions

Welcome!

Thank you for participating in today's experiment.

As in every experiment you can decide against participation at any point in time without stating any reasons. However, if you decide to leave the experiment, you will not receive any payment.

What can you expect in today's experiment?

Today's experiment consists of two parts. You can find the instructions for the first part right in front of you on your desk. The second part contains a questionnaire and will start right after part 1.

You will receive 3 Euro for your participation.

A2 Written instructions

Instructions

In the following you will decide if you agree to transfer your address data together with your full name. You decide yourself, for which monetary amount you are willing to agree to transfer the data.

If you agree to the transfer 20 FAU (Nuremberg) students will receive an email with your address data (street name with house number, postal code with city) together with your full name. This email will be sent within the next six month, together with the other participants' data, who agreed to transfer their data (the figure below gives an example for such an email).

As previously announced, you receive this email informing you that the following participants have agreed to transfer their data to you. You will receive this email only once, no further emails will follow.

Name	Street name and house number	Postal code	City
Marie Mustermann	...	...	...
Max Mustermann	...	...	...
...	...	...	...
...	...	...	...

Kind regards,
your experimental team

Procedures

When you have finished reading these instructions and answered the comprehension questions correctly, you will receive a data form and an envelope. Please fill in the form. Afterwards put the form into the envelope. Do not close the envelope yet. When you agree to the transfer of your data afterwards, you will give us the envelope for the transfer. We will verify the data with the help of your ID card and forward the data via email within the next six months. If you decide not to pass on your data, you keep the envelope, and the data will not be transferred.

Your decision

You decide by filling in a decision table. You receive this table from us once you have read the instructions and answered the comprehension questions correctly. In the table, there are 27 amounts (between 0.00 euros and 13.00 Euro), each accompanied by a "yes"- and "no"-column. For every amount in the table, you decide whether you accept ("yes") or refuse ("no") to transfer the data, given you receive this amount. Please tick "yes" or "no" for each single amount

If you have filled in the table, raise your hand. The experimenter will come to your seat and collect your decision table. Afterwards, we ask you to answer a questionnaire on the computer.

Payment

After answering questionnaire, the payment procedure takes place. You will draw one out of the 27 amounts listed on the table randomly (You will pick one of the 27 amounts out of the bag by yourself and you can verify that every amount is available exactly once).

If you ticked "yes" in your decision table for the drawn amount (i.e. you agreed to transfer the data for this amount) the data will be transferred. In this case, you receive the drawn amount (in addition to the 3 euros you receive for filling in the questionnaire) and you sign a consent form for data dissemination and the acknowledgment for the received amount. If you ticked "no" for the drawn amount, (i.e. you did <u>not</u> agree to transfer the data for the respective amount), the data will not be transferred. In this case, you will <u>not</u> receive the drawn amount. In both cases, you will receive the 3 euros for showing up on time and filling in the questionnaire.

In the following we give three examples in order to clarify the procedure.

Example 1

Assume a participant agrees to transfer the data for an amount larger or equal to 3 euros. In this case, she ticks "no" for rows one to six (0.00€ to 2.50€) and "yes" in the left column from row 7 (i.e. from 3.00€) onwards. The table below illustrates this example.

At the end of the experiment, you draw one of 27 lots. Each of the 27 lots is labeled with one of the 27 amounts. This way, every amount of money has the same likelihood to be drawn. After you have drawn one lot, we compare the number written on the lot with your decisions in your table.

Yes	Amount	No
□	0,00 €	X
□	0,50 €	X
□	1,00 €	X
□	1,50 €	X
□	2,00 €	X
□	2,50 €	X
X	3,00 €	□
X	3,50 €	□
X	4,00 €	□
X	4,50 €	□
X	5,00 €	□
X	5,50 €	□
X	6,00 €	□
X	6,50 €	□
X	7,00 €	□
X	7,50 €	□
X	8,00 €	□
X	8,50 €	□
X	9,00 €	□
X	9,50 €	□
X	10,00 €	□
X	10,50 €	□
X	11,00 €	□
X	11,50 €	□
X	12,00 €	□
X	12,50 €	□
X	13,00 €	□

Case 1: The drawn lot shows 7.- €.

7.- €
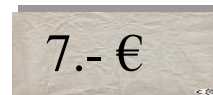
In this case, (see illustration on the left), "yes" has been ticked for 7.-€. This means the participant in the example receives 7.-€ and the data will be transferred including her first and last name.

Case 2: The drawn lot shows 0.50€.

0.50 €

In this case (see illustration on the left), "no" has been ticked for 0.50€. This means the participant does not receive the amount and the data will not be transferred.

Example 2

Let us assume, the participant does not agree with a data transfer for any offered amount. In this case, the participant ticks "no" for every amount. The table below illustrates this example.

Yes	Amount	No
☐	0,00 €	X
☐	0,50 €	X
☐	1,00 €	X
☐	1,50 €	X
☐	2,00 €	X
☐	2,50 €	X
☐	3,00 €	X
☐	3,50 €	X
☐	4,00 €	X
☐	4,50 €	X
☐	5,00 €	X
☐	5,50 €	X
☐	6,00 €	X
☐	6,50 €	X
☐	7,00 €	X
☐	7,50 €	X
☐	8,00 €	X
☐	8,50 €	X
☐	9,00 €	X
☐	9,50 €	X
☐	10,00 €	X
☐	10,50 €	X
☐	11,00 €	X
☐	11,50 €	X
☐	12,00 €	X
☐	12,50 €	X
☐	13,00 €	X

Assume that the drawn lot shows 13€.   13.- €
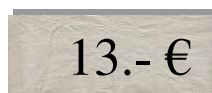
In this example the participant ticked "no" for the amount of 13.- € (see figure above). Thus, the participant does not receive an additional amount of money and the data will not be transmitted. Note, in this example, this would be the case for any amount drawn.

Example 3

Let us assume, the participant does agree with a data transfer for any offered amount. In this case, the participant ticks "yes" for every amount. The table below illustrates this example.

Yes	Amount	No
X	0,00 €	☐
X	0,50 €	☐
X	1,00 €	☐
X	1,50 €	☐
X	2,00 €	☐
X	2,50 €	☐
X	3,00 €	☐
X	3,50 €	☐
X	4,00 €	☐
X	4,50 €	☐
X	5,00 €	☐
X	5,50 €	☐
X	6,00 €	☐
X	6,50 €	☐
X	7,00 €	☐
X	7,50 €	☐
X	8,00 €	☐
X	8,50 €	☐
X	9,00 €	☐
X	9,50 €	☐
X	10,00 €	☐
X	10,50 €	☐
X	11,00 €	☐
X	11,50 €	☐
X	12,00 €	☐
X	12,50 €	☐
X	13,00 €	☐

Assume that the drawn lot shows 10€.

10.- €
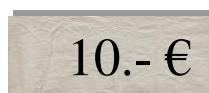
In this example, "yes" has been ticked for 10.- € (see illustration above). This means the participant in the example receives 10.- € and the data will be transferred including her first and last name.

A3 Decision Table

Please fill in the following table. You may take as much time as you need. Decide for each amount, this means tick a box ("Yes" or "No") for each amount. If you tick "Yes", you indicate that you are agree that your address data (street name, house number and postal code with city) together with your full name will be sent to 20 FAU (Nuremberg) students via email. If you tick "No", you indicate that you do not agree that your data is sent when being offered the respective amount. After you filled in the table an experimenter will collect the form and start the questionnaire on your computer.

Yes	Amount	No
☐	0,00 €	☐
☐	0,50 €	☐
☐	1,00 €	☐
☐	1,50 €	☐
☐	2,00 €	☐
☐	2,50 €	☐
☐	3,00 €	☐
☐	3,50 €	☐
☐	4,00 €	☐
☐	4,50 €	☐
☐	5,00 €	☐
☐	5,50 €	☐
☐	6,00 €	☐
☐	6,50 €	☐
☐	7,00 €	☐
☐	7,50 €	☐
☐	8,00 €	☐
☐	8,50 €	☐
☐	9,00 €	☐
☐	9,50 €	☐
☐	10,00 €	☐
☐	10,50 €	☐
☐	11,00 €	☐
☐	11,50 €	☐
☐	12,00 €	☐
☐	12,50 €	☐
☐	13,00 €	☐

You made a decision for each amount?

Please raise your hand. We will come to your cubicle and continue the experiment.

Seat number: _____

A4 Data Form

Please fill in

First name   _____

Surname   _____

Street, house number   _____

Postal code, city   _____

Please fold the paper and put in to the provided envelope.

Please do not close the envelope yet.

If you agree to transfer your data, you will hand us over the envelope at the end of the experiment. We will then verify your data by checking your ID card and forward your data via email within the next six months.

If you do not agree to transfer your data, you will keep the envelope and the data will not be transferred.

A5 Consent Form

This form was filled out after the random draw, in case the participant had indicated on the BDM-sheet that she is willing to accept sharing her personal data for the drawn offer.

Consent for data transfer

I hereby confirm that I have voluntarily participated in the experiment today and that I have been fully informed about the experimental procedures and the consequences of my decision. At the beginning of the experiment the following data was collected: First name und surname, address data (street, house number, postal code, and city).

I decided to pass on the data to the LERN for a unique transfer to 20 FAU students.

I know that I can refuse data collection or data transfer. In this case no data will be transferred to other students.

I give my consent to transfer my data (street, house number, postal code, and city) together with my name to the LERN for a unique transfer to 20 FAU students and receive _____ Euros.

Name	_____
Signature	_____