Keep Them out of It! How Information Externalities Affect the Willingness to Sell Personal Data Online*

Tim Friehe† Leonie Gerhards‡ Franziska Weber§

October 17, 2022

Abstract

Many individuals act rather naively when providing personal data online. When individuals share their personal data, this can allow third parties to learn more about others, too. Our large-scale online experiment reveals that individuals are less willing to sell personal data when sharing can compromise others' privacy. Compared to a benchmark without data compromise, individuals' willingness to sell personal data decreases in scenarios in which others' data is compromised with 50% and 100% probability, respectively. By applying two well-studied interventions – peer effects and a social norm focus – we explore ways to mitigate excessive data sharing, laying the ground for the design of effective policies. While peer effects seem to increase individuals' willingness to share personal data on average, making people reflect on the appropriate behavior appears a promising policy approach.
Keywords: Privacy; Information Externality; Social Norms; Peer Effects; Experiment.
JEL Codes: C91, D30, D91.

*This study was pre-registered on AsPredicted.org before we began data collection; registration number #51902 (link to document). We obtained ethical approval from the German Association for Experimental Economic Research on November 11, 2020; Institutional Review Board Certificate No. f1xrtJmW (link to document).

†Public Economics Group, University of Marburg; Am Plan 2, 35037 Marburg, Germany. CESifo, Munich, Germany. EconomiX, Paris, France. Email: tim.friehe@uni-marburg.de.

‡King's Business School, King's College London, Bush House, 30 Aldwych, London, WC2B 4BG, UK. Email: leonie.gerhards@kcl.ac.uk.

§Rotterdam Institute of Law and Economics/Erasmus School of Law, Erasmus University Rotterdam; Burg. Oudlaan 50, 3062 PA Rotterdam. Email: weber@law.eur.nl.

1 Introduction

Radical advancements in information technology have led to fascinating opportunities to collect, store, and utilize vast amounts of (personal) data. These innovations transformed individuals from consumers of information to producers thereof via, for example, social media activities, online searches, online shopping, and other uses of the internet. However, many individuals act either naively or myopically when they produce or provide personal information in their everyday transactions, even despite the fact that they care about privacy (e.g., Acquisti et al., 2020). They accept cookies without checking them closely, upload files such as photos and videos (e.g., via social platforms), and share personal data about their preferences and attitudes (e.g., via their purchasing histories at large retailers) without understanding how service providers may use the data provided. Importantly, individuals often ignore that "information about one person is also information about others" (Fairfield and Engel, 2015, p. 389). Informed consent is the main legal tool to exercise control over one's data (see Arts. 6 (1) a and 7 General Data Protection Regulation), an instrument that has only questionable effectiveness and neglects data externalities. The relationships of individual pieces of data often determine the value of personal data to the buyers and the connectivity of data is pervasive in the digital economy nowadays (e.g., Barocas and Levy, 2020, MacCarthy, 2010).[1] For instance, one important element of the Cambridge Analytica scandal, in which personal data of millions of Facebook users were collected without their consent to be used for political advertising, was the fact that the company not only harvested the data of users who had deliberately downloaded their app but simultaneously that of their Facebook friends.[2]

If data interdependencies are not internalized by the data-disclosing individual, an information externality and excessive data sharing (i.e., at a level above the socially desirable level) will likely result. The few existing theoretical analyses of information externalities assume that individuals ignore the repercussions of their own disclosure for others (Acemoglu et al., forthcoming, Bergemann et al., 2022, Choi et al., 2019, Ichihashi, 2021). We put this assumption to the test.

The controlled environment of our online experiment uniquely enables us to single out whether individuals' willingness to sell (WTS) personal data decreases when own data dis-

[1] For example, Richards (2012, p. 1939) states that "Big Data is fundamentally networked. Its value comes from the patterns that can be derived by making connections between pieces of data, about an individual, about individuals in relation to others, about groups of people, or simply about the structure of information itself."

[2] See theguardian.com (last accessed June 21, 2022).

closure can compromise others' privacy. In our design, compromised privacy means lower consumer surplus in the ambit of personalized price discrimination, which is empirically one of the most important manifestations of harm from compromised privacy according to, for instance, Calo (2011). Similarly, Hidir and Vellodi (2021) state that "price discrimination is of first-order concern in online settings".[3] Hannak et al. (2014) find evidence for price discrimination being widespread, using a novel way to measure it on e-commerce sites such as Amazon. In the context of consumers' willingness to pay, there are different ways to imagine information externalities. For example, in the spirit of Bergemann et al. (2022), the measured individual willingness to pay may either (i) be composed of a common type and some random noise so that more observations via others' information disclosure help the firm to identify the common type or (ii) consist of an idiosyncratic type and common noise where more observations via others' disclosure improve the firm's understanding of the common noise, thereby allowing for a better inference of the idiosyncratic type.

We focus on information externalities affecting others close to the individual. Applying a group enhancement protocol, our experiment is designed to mimic relationships of colleagues, friends, or other close contacts. Across treatment variants Prob0, Prob50, and Prob100, we exogenously vary the level of the probability (either 0%, 50% or 100%) with which their data sale compromises another subject's data and thereby (potentially) lowers the other subject's expected payoffs. Finding that individuals do not moderate their data disclosure even when adverse effects are made transparent would call for wide-ranging policy interventions to avoid social harm from privacy breaches.

Our experiment reveals that subjects' WTS reflects the possibly adverse effect of own data disclosure on others' payoffs. Compared to a benchmark without data compromise (i.e., treatment variant Prob0), subjects' WTS is significantly lower when others' privacy can be compromised (i.e., in information externality scenarios Prob50 and Prob100).

In addition to exploring how a positive compromise probability shapes subjects' WTS, we investigate how two well-studied interventions influence data-disclosing behavior: information about peers' behaviour and the focus on socially appropriate behavior (e.g., Agerström et al., 2016; Bartke et al., 2017; Croson and Shang, 2008; Cialdini et al., 2006; Keizer et al., 2008). In treatment Info, subjects may revise their initial WTS after observing a peer's WTS. Findings

[3]Clearly, other important manifestations of harm exist. For example, in an interesting recent study, Acquisti and Fong (2020) explore how personal information posted by job candidates on social media sites influences hiring decisions. Lin (forthcoming) provides an empirical analysis that separates the instrumental value of privacy, which is our focus in the present study, from the intrinsic value of privacy.

from this treatment provide evidence for peer effects in the domain of data disclosure: a sizable share of subjects (about 27% on average across treatment variants) revise their initial WTS in the information externality scenarios, whereby their WTS personal data increases in their peers' WTS, leading to an *even higher* WTS. In treatment NORM, we apply an injunctive norm focus (Krupka and Weber, 2009) to let subjects reflect on socially appropriate behavior before eliciting their WTS. We find that subjects who are asked to think carefully about the socially appropriate data-disclosure behavior state a lower willingness to sell personal data. Our findings thus provide evidence that social norms can shape behavior in the domain of data disclosure. In summary, we present new insights into the conditions under which the two interventions, peer effects and social norms, can be effective policy instruments against excessive data sharing.

The rest of the paper is structured as follows: We survey the related literature next and describe our experimental design in Section 3. We discuss our key behavioral predictions in Section 4, and present our empirical findings in Section 5. Section 6 concludes.

2 Related Literature

The numerous trade-offs involved in the personal-data context increasingly attract scholarly attention. This is well deserved because "if this is the age of information, then privacy is the issue of our times" (Acquisti et al., 2015, p. 509). Indeed, the privacy literature is by now vast and extensive.

Many studies have established that an individual's disclosure of personal data can be detrimental for others (e.g., Acemoglu et al., forthcoming). First, an individual disclosing personal data may pressure others into sharing their personal data, for example, when competing for resources and attention (e.g., Acquisti et al., 2012). Second, an individual's data disclosure often compromises others' privacy. This can result from a *direct link*, examples being a photo that shows people besides the individual sharing it or an individual providing household-level information, thereby giving away information about the spouse or partner. Moreover, a privacy compromise can result from *inferences* enabled by data sharing. For example, a consumer who accepts data tracking can compromise the privacy of similar consumers when artificial intelligence algorithms match consumers (e.g., Choi et al., 2019), and an individual expressing their own political attitudes allows observers to learn about the political attitudes of others in the individual's social network using homophily (e.g., Jernigan and Mistree, 2009).[4]

[4]Barocas and Levy (2020), for example, elaborate on the many ways in which own privacy depends on others'

Acquisti et al. (2016) provide a survey of the theoretical and empirical work on the economics of privacy. In the following, we review the part of the behavioral and experimental literature that is most related to our approach. One strand of the literature on information externalities models individuals as interdependent and analyzes how they react strategically to this interdependence. Fairfield and Engel (2015) explain that privacy can fundamentally be considered a public good and, against this background, refer to the large public-good literature for insights about privacy policy. Ackfeld and Güth (2019) consider a setup in which two subjects may use *more* data disclosure as a means to persuade another party to select them as allocator in a subsequent distribution task, where being selected means a significant monetary benefit. The authors find that this strategic concern induces more data revelation. In Benndorf et al. (2015), participants may reveal personal productivity information in a labor-market experiment, the motivation being that observers do not draw negative inferences about them. The authors find that unraveling occurs frequently, but less often than theory predicts. Whereas Benndorf et al. (2015) show that information revelation by some individuals induces others to reveal information, Goh et al. (2015) show that the decision not to share information can also be contagious. They find that individuals who barred telemarketers from contacting them later induced other individuals to follow suit because they were targeted to a greater extent after some individuals were no longer viable contacts for telemarketing.

Our paper is closely related to experiments focusing on the general willingness to share personal data.[5] Benndorf and Normann (2018) measure the willingness to sell personal data (preferences, contact data, *Facebook Timeline*, *Facebook About*) to a firm for marketing purposes. They find that roughly one sixth of the participants refuse to sell their personal data, while another sixth ask for 2.50 Euro or less. On average, those willing to sell demand about 15 (19) Euro in exchange for their contact details (Facebook data).[6] Collis et al. (2021) also consider the willingness to sell Facebook data. Their focus is on the effects of an information treatment. After a statement of subjects' initial willingness to sell, they are provided a reference value, and then invited to adjust their willingness to sell. The authors find that the dispersion of the valuation decreases as a result of the intervention but persists. One cause of such a dispersion may lie in the heterogeneity in terms of the intrinsic preference for privacy which are isolated in

disclosure choices.

[5] Lee and Weber (2022) indicate that monetary equivalents can discriminate between the underlying privacy attitudes of different types of individuals and that experimental privacy choices exhibit a degree of rationality that is similar to experimental choices in other domains.

[6] Benndorf and Normann's (2018) study includes *Facebook Timeline* data that may compromise others' privacy, but this is not the focus of their study.

Lin (forthcoming). Schudy and Utikal (2017) report results from four experiments, seeking to explore the effects of (i) how many recipients obtain personal data after disclosure, (ii) the social distance to the recipient, (iii) the comprehensiveness of the disclosed personal data, and (iv) how data verification influences the willingness to sell personal data about contact details and their own physical characteristics. However, different to our study, no third-party consequences results from a sale of these data. Hermstrüwer and Dickert (2017) elicit the willingness to sell information about their own allocation choices in a dictator game, studying the consequences of having the disclosure choice before or after the dictator game for (i) the willingness to sell and (ii) dictator-game giving. All of these studies use the Becker-DeGroot-Marschak mechanism (BDM; Becker et al., 1964), which we also apply to elicit subjects' willingness to sell data.

Besides shedding light on data disclosing behavior in information externality scenarios, our paper analyzes two specific behavioral interventions in this domain. In treatment INFO, we test for peer effects. Building on Cialdini et al.'s (1990) ideas and the subsequent literature, we provide individuals with information about another subject's choice and allow them to adjust their WTS. In contrast to other papers on peer effects (e.g., Thöni and Gächter, 2015), subjects interact in a previous stage and have interdependent payoffs, making us expect sizable peer effects.[7] In treatment NORM, we apply an injunctive norm focus, following Krupka and Weber (2009), who showed that making subjects think about socially appropriate behavior induces more norm-compliant, prosocial choices.

3 Design and Procedures

3.1 Design

The online experiment consists of four stages that we summarize in Table 1 and explain below. Treatments differ only in Stage 3, where we implement a 2×3 factorial design (see Table 2 for the number of subjects per treatment). Stage-specific instructions are displayed on subjects' computer screens at the beginning of each stage. The experiment ends with a final questionnaire in which we elicit a range of personal characteristics.[8]

Stage 1: Personal Data Creation Subjects receive an endowment of 12 Euro which they can use to buy a lottery ticket in a BDM mechanism (Becker et al., 1964). The lottery ticket

[7] Lindström et al. (2018), for example, argue that people consider observed behavior as more moral, and we hypothesize that such considerations will be important for peer effects in our information externality scenarios.

[8] See the Supplementary Material for translated and original versions of the instructions and questionnaire.

Table 1: Experiment Design

Stage 1: *Personal Data Creation*	Subjects state their willingness to pay (WTP) for a lottery ticket (WTP represents personal data in Stages 3 & 4).
Stage 2: *Social Proximity*	Subjects are randomly matched in pairs and participate in an activity to increase social proximity.
Stage 3: Willingness to Sell	0) Only in NORM: Subjects are incentivized to think about the socially appropriate willingness to sell (WTS) personal data to a firm. 1) In NORM and INFO: Subjects state their personal WTS in a multiple price list format. 2) Only in INFO: Subjects see their peer's WTS and may revise their WTS. 3) In NORM and INFO: In case of sale, peer's personal data is disclosed to firm with treatment-variant-specific compromise probability, either 0%, 50% or 100%.
Stage 4: *Effect of Data Sale*	Firms make a take-it-or-leave-it offer for lottery ticket equal to the subjects' WTP from Stage 1, if that information is available to the firm. Otherwise, the lottery ticket price is a random number.

has an expected value of 4 Euro. It returns 11 Euro with probability 30% and 1 Euro with probability 70%. The BDM mechanism first asks subjects to state the maximum amount they would be willing to pay for the lottery ticket, B, and then compares B to the realization of a random number, R, that is uniformly distributed over $[0.00, 12.00]$. Subjects buy the lottery ticket at price R when $R \leq B$ and do not buy otherwise. Thus, stating $B = 12.00$ Euro would imply that subjects buy the ticket with certainty. Subjects' willingness to pay (WTP) for the lottery ticket reveals information about their preferences. Subjects learn only in Stage 3 that their WTP may be sold as personal data and will potentially be disclosed to a firm.

Stage 2: Social Proximity Two subjects are paired to form a color-coded group. The group color is either green, blue, yellow, orange or red and shows on all subsequent decision screens. Group formation using the subjects' association to a color-coded group is common practice in the minimal group literature (e.g., Chen and Chen, 2011, Chen and Li, 2009). In addition, we follow evidence indicating that group enhancement through some joint activity (e.g., Eckel and Grossman, 2005) strengthens subjects' identification with the group. We use the procedure successfully employed by Hett et al. (2020), by engaging subjects in three (unincentivized) group

quizzes about the appropriate umbrella term for a set of four pictures.[9] For each quiz, subjects have 60 seconds to discuss potential solutions with their fellow group member, henceforth called the "peer", via a chat program before they enter their answers individually. This stage is intended to increase social proximity between subjects in order to ultimately increase their caring about their peer.

Stage 3: Willingness to Sell Personal Data We elicit our main outcome variable, subjects' willingness to sell personal data to a firm (an automaton, further details follow below) as the minimum acceptable price at which they are willing to disclose personal data. Specifically, in a BDM mechanism, subjects state the minimum acceptable price at which they are willing to disclose their own WTP for the lottery ticket from Stage 1 as well as possibly also their peer's WTP. The higher (lower) a subject's minimum acceptable price, the lower (higher) their WTS.

Subjects submit their minimum acceptable price in a multiple price list format (e.g., Schudy and Utikal, 2017).[10] For each Euro amount between 0.00 and 6.00 (in steps of 20 Cents), subjects indicate whether they are willing to sell personal data in case that amount is randomly drawn as the payoff relevant one. Formally, we define:

$$\text{WTS} = 6.00 - \text{the minimum acceptable price.}$$

To provide greatest possible clarity about the available options, the instructions present examples of multiple price lists of (i) an individual who is not willing to sell personal data at any of the available prices, (ii) an individual who is willing to sell personal data at each of the available prices, and (iii) an individual with an "interior" WTS.

Importantly, we are not interested in the level of subjects' WTS per se. Our main aim is to study how the presence and the extent of information externalities impinge on their WTS. Across treatment variants, we vary the probability with which the own sale of personal data signifies revealing the peer's personal data as a byproduct. In treatment variants Prob0, Prob50, and Prob100, selling personal data compromises the peer's privacy with probability 0%, 50% and 100%, respectively.

Compromising the peer's privacy can materially harm the peer. In Stage 4, the firm makes a

[9] See the Supplementary Material for instructions and screen shots.

[10] Presenting the BDM elicitation procedure in a different format than in Stage 1 comes with the advantage that subjects are less prone to confuse Stages 1 and 3 when we refer back to them later in the experiment. We implemented the multiple price list such that the statement of the minimum acceptable price led to the consistent filling of the remaining price lines (with the possibility to change the minimum acceptable price before finalization), so as to avoid the problem of multiple switching points.

take-it-or-leave-it offer to the peer. In case the firm has learned the peer's WTP through the sale of personal data, the take-it-or-leave-it offer is equal to the peer's WTP. Conversely, if the peer's WTP is not known to the firm, the take-it-or-leave-it offer is randomly drawn from a uniform distribution on the interval $[0.00, 4.00]$. Given that the lottery ticket's expected value amounts to 4.00 Euro, and, empirically, subjects' average willingness to pay amounts to 3.91 Euro[11], the outlook of a random lottery ticket price with an average value of 2.00 Euro means significant expected consumer surplus. This signifies that compromising the peer's privacy reduces the peer's consumer surplus quite substantially with a probability close to one. A subject who is selling personal data does thereby not influence their own consumer surplus. The potentially substantial decrease of consumer surplus can only stem from the peer's sale of data.[12]

Besides the variation with respect to the compromise probability (PROB0, PROB50 and PROB100), we implement two treatments in Stage 3 of the experiment.

In treatment INFO, we consider peer effects regarding the willingness to sell personal data. Subjects first state their WTS. Next and without previous announcement, they learn their peer's WTS and may subsequently adjust their own WTS.[13] In this treatment, we hence elicit both subjects' *unconditional* and *conditional* WTS (i.e., the minimum acceptable price *before* and *after* observing their peer's minimum acceptable price).[14]

In treatment NORM, we implement an injunctive norm focus (Krupka and Weber, 2009). *Before* subjects indicate their WTS, we ask them to state (i) "What is the socially appropriate minimum price regarding the sale of personal data in your situation?" and to guess (ii) the respective norm statement of another randomly selected participant. If a subject's guess is in

[11] A Kruskal Wallis test does not reveal significant differences in subjects' WTP across the six treatment variants, $p = 0.31$.

[12] Our design captures a trade-off between a personal material gain and lower payoffs of the peer, which seemingly makes it similar to social dilemma situations. However, note that there are some aspects that contrast with typical allocation games and reflect relevant aspects from the privacy domain. The harm imposed on the peer consists not only of the material component but also from potential harm resulting from the intrinsic value of privacy (Lin, forthcoming). The WTS in our PROB0 treatment variant will give an indication of this intrinsic value. In addition, in contrast to standard dictator games, for example, the data disclosing party cannot know the precise material harm because the peer's actual WTP for the lottery ticket remains unknown to her (similar to the fact that the marketing value of personal data is often not known for peers).

[13] In treatment INFO, subjects know that only one group member's change of one group member will eventually be implemented. This ensures that subjects can optimize against the other individual's announcement without having to anticipate a further round of changes.

[14] Since we did not pre-announce the later revelation of their stated WTS to their peer, we elicited subjects' opinion on this design feature in our questionnaire. Answer options for this item ranged from (1) "very bad" to (5) "very helpful" with a middle response option (3) "neutral". In all three treatment variants, subjects' median answer is 3, with means of 3.29 (s.d. 0.69), 3.37 (s.d. 0.76) and 3.34 (s.d. 0.88) in PROB0, PROB50 and PROB100, respectively. In PROB 0, 9% of subjects state they experienced the unannounced revelation of WTS as "bad" (no one experienced it as "very bad"), while 34% experienced it as "helpful" or even "very helpful". In PROB 50, 10% of subjects state that they experienced this revelation as "very bad" or "bad", while 43% experienced it as "helpful" or even "very helpful". In PROB 100, the respective percentages amount to 12% and 37%.

the range of $+/-0.20$ Euro of the other's norm statement, the subject receives an additional 2.00 Euro.

Stage 4: Effect of Data Sale The firm (role assumed by the computer) offers the lottery ticket exactly at the subject's WTP if this information is known from the sale of personal data by the subject's peer in Stage 3. Otherwise, the take-it-or-leave-it offer is the realization of a random variable that is uniformly distributed on the interval $[0.00, 4.00]$. After the firm states the price, subjects can either *accept* or *reject* the firm's offer.

Questionnaire After Stages 1-4, we inquire about subjects' age and gender, which turned out to be important control variables in some of the studies reviewed in Section 2. To account for the fact that the privacy breach was creating probabilistic harm in PROB50, we elicit subjects' general risk attitude in an unincentivized survey item (e.g., Dohmen et al., 2010). Moreover, we want to include a measure for their privacy concerns outside the specific context studied here. For this reason, we collect subjects' privacy concerns based on Westin's privacy index (e.g., Ackfeld and Güth, 2019, Westin, 2001). In addition, we collect attitudes towards various forms of norm violations to construct an individual measure of (social) norm obedience. For this, we ask subjects about their agreements with six statements regarding socially inappropriate behavior (on skiving off, drunk driving, tax evasion, fare dodging, hazardous waste disposal in household waste and speeding) that were previously used by Traxler and Winter (2012). Lastly, we conduct an SVO test (Murphy et al., 2011).[15] Since the extent to which subjects care about others' payoffs and norms are important channels in our design, we considered these personal characteristics potentially relevant control variables.

3.2 Procedures

The WISO laboratory at the University of Hamburg ran the online experiment in Winter 2020/2021, using h-root (Bock et al., 2014) for recruitment and oTree (Chen et al., 2016) to code the experiment. Stage-specific instructions were presented at the beginning of the respective stages. Realized random variables and payoffs were shown only at the end of the experiment.

In total, 596 subjects, recruited from the laboratory's usual student subject pool (covering various fields of study) successfully participated in the experiment up to Stage 3, 591 completed

[15] We implemented an SVO with hypothetical choices. According to, inter alia, Mentzakis and Mestelman (2013), this does not imply biased choices.

all parts of the final questionnaire.[16] Each of the initially invited subjects participated in only one of our six treatment variants (see Table 2).

Table 2: Number of Subjects per Treatment

	Prob0	Prob50	Prob100	Total
Norm	99	100	97	296
Info	100	100	100	300
Total	199	200	197	596

In each session, treatment variants were randomized at the individual level. The experiment was relatively gender-balanced (overall 57% female, 42.1% male subjects). Subjects were made aware that payoffs from Stage 3 were always payoff relevant. In addition, either Stage 1 or Stage 4 (i.e., one of the two stages involving the lottery ticket) became payoff relevant. Average earnings for the 60 minutes sessions amounted to 15.35 Euro (with a standard deviation of 4.52).[17]

4 Predictions

Our experiment is designed to test whether individuals' willingness to sell personal data is influenced by the degree to which sharing own data implies compromising others' privacy. In our design, compromising others' privacy is associated with personalized price discrimination and hence a loss of consumer surplus, which is also one of the most important ways compromised privacy results in harm in reality (e.g., Calo, 2011).

As a baseline for our predictions, we consider the stylized *homo oeconomicus* portrayal. Our design ensures that disclosing personal data entails only beneficial payoff consequences for the individual selling the personal data (as the information about the selling individual is irrelevant for the firm). Thus, an economic agent who is solely self-interested and focuses on monetary outcomes alone would be willing to sell personal data at all prices and independent of treatment.

[16] In total, 606 subjects started the experiment. However, 14 subjects dropped out of the experiment. Two of these had to be excluded before they began reading any instructions since we required even numbers of participants per session. One subject did not correctly solve the first set of control questions, so he/she and his/her matching partner could not proceed with the experiment. Another five subjects did not solve correctly the second set of control questions. They, as well as three of their matching partners, had to leave the experiment after Stage 3. One subject dropped out when being confronted with the injunctive norm focus question, meaning that his/her matching partner also had to leave the experiment after Stage 3. Finally, for the sake of completeness, one subject did not answer the social value orientation part of the questionnaire. This leaves us with 591 subject observations.

[17] We preregistered our design, hypotheses, and the respective empirical tests on aspredicted.org and obtained IRB approval from the German Association for Experimental Economic Research.

We do not expect that our subjects focus on monetary outcomes alone. In our experiment, we purposefully included a group formation activity to increase social proximity between randomly matched subjects (the peers) in order to mimic relationships outside the lab, where the decision to disclose one's personal data may concern that person's friends, colleagues or other close contacts. Prosocial preferences for the peer predict that the WTS stated in Stage 3 will be decreasing in the compromise probability. The same prediction results from models in which individuals care about norm compliance (e.g., Krupka and Weber, 2013, Kimbrough and Vostroknutov, 2016). In Kimbrough and Vostroknutov (2016), for example, utility depends on monetary payoffs and a possible cost from noncompliance with a social norm regarding the behavior at hand. When applied to our context, the basic idea is that while selling personal data increases own expected monetary payoffs for all positive prices, it can simultaneously create expected norm noncompliance costs. If the social norm dictates that personal data may only be sold at a sufficiently high price, an individual's norm noncompliance costs will be lower the lower the stated WTS. We suppose that the norm about the "sufficiently high price" is increasing in the compromise probability. The underlying idea is that larger social consequences increase subjects' caring about norm compliance.

Hypothesis 1: *Subjects' WTS decreases in the compromise probability:* $WTS(\textsc{Prob0}) > WTS(\textsc{Prob50}) > WTS(\textsc{Prob100})$.

In light of the potential for information externalities, we implement treatments to analyze how two well-known social factors – peer effects and a focus on injunctive norms – influence subjects' WTS. For this analysis, we focus on treatment variants Prob50 and Prob100, since compromising the peer's personal data is ruled out by design in Prob0.

In treatment Info, the observation of the peer's WTS provides information about how similar others behave. Previous evidence suggests that individuals tend to prefer conformity in circumstances with social relevance (e.g., Carlsson et al., 2010). In our design, there exists an additional effect stemming from reciprocity. After all, the higher the peer's WTS, the greater the likelihood that a subject's own consumer surplus is harmed. On the basis of conformity and reciprocity, we hypothesize that subjects' WTS will increase with the peer's WTS.

Moreover, we expect that individuals are more receptive to their peer's influence, the larger the social consequences of their own behavior. The underlying idea is that larger social consequences increase subjects' reflecting upon and caring about socially appropriate behavior,

which is associated with a stronger reaction towards observing a peer behaving relatively more (or less) appropriately.

Hypothesis 2.1: *In treatments with a positive compromise probability, subjects' conditional WTS correlates positively with their peers' unconditional WTS.*

Hypothesis 2.2: *The influence of the peer effect on subjects' conditional WTS increases in the compromise probability.*

In treatment NORM, we apply an injunctive norm focus (Krupka and Weber, 2009) by asking subjects to reflect on the minimum acceptable price they deem socially appropriate before letting them indicate their own minimum acceptable price. The higher the social norm, the lower the willingness to sell personal data should be. Against the background of the results obtained by Krupka and Weber (2009), for example, we expect that any norm compliance concern weighs more heavily in treatment NORM. Therefore, subjects' WTS in NORM should be lower than the unconditional WTS in treatment INFO. Moreover, we hypothesize that the norm focus effect will increase in the compromise probability, as larger social consequences increase subjects' caring about socially appropriate behavior.

Hypothesis 3.1: *Comparing data from* INFO *and* NORM *treatments for the cases with a positive compromise probability, the injunctive norm focus decreases subjects' WTS, that is,*
$WTS_{\text{Norm}}(\text{PROB50 \& PROB100}) < WTS_{\text{Info,uncond}}(\text{PROB50 \& PROB100})$.

Hypothesis 3.2: *The effect of the injunctive norm focus on subjects' WTS increases in the compromise probability, that is,*
$WTS_{\text{Norm}}(\text{PROB50}) - WTS_{\text{Info,uncond}}(\text{PROB50}) < WTS_{\text{Norm}}(\text{PROB100}) - WTS_{\text{Info,uncond}}(\text{PROB100})$.

5 Results

Following our pre-registration, our empirical analysis first tests whether subjects' WTS is influenced by the probability with which own data sale implies that the peer's privacy is compromised. Next, we consider how peer information and providing an injunctive norm focus affects subjects' WTS. Moreover, we test how the effects depend on the level of the compromise probability.[18]

[18] Partly diverging from our pre-registered research plan, we stated directed hypotheses throughout Section 4. This was done for the ease of the reader. In the analysis, we only report two-sided test results, as initially pre-registered.

Table 3 summarizes subjects' WTS and reports how many subjects stated a WTS in the range of the eligible Euro amounts $[0.00, 6.00]$ and how many were not willing to sell personal data for any amount up to 6.00 Euro. We find that subjects' WTS vary substantially across treatments.[19]

Table 3: The Willingness to Sell Personal Data: Summary Statistics

	Mean	Std. dev.	Min	Max	#WTS $\in [0, 6]$	#Unwilling to sell for ≤ 6
Info, Prob0						
Unconditional WTS	3.88	1.71	0.00	6.00	96	4
Conditional WTS	3.92	1.73	0.00	6.00	96	4
Info, Prob50						
Unconditional WTS	3.52	1.63	0.00	6.00	93	7
Conditional WTS	3.54	1.58	0.00	6.00	97	3
Info, Prob100						
Unconditional WTS	3.52	1.70	0.00	6.00	97	3
Conditional WTS	3.77	1.67	0.80	6.00	97	3
Norm, Prob0						
WTS	3.97	1.63	0.00	6.00	97	2
Norm, Prob50						
WTS	3.17	1.58	0.00	6.00	93	7
Norm, Prob100						
WTS	3.08	1.50	0.00	6.00	88	9

Notes: A subject's WTS is quantified as "6 – minimum acceptable price", where 6 is the maximum amount offered for personal data in the experiment.

5.1 Willingness to Sell Personal Data: The Influence of the Compromise Probability

When we compare behavior across treatment variants in Table 3, we note that the Prob0 treatment variants stand out. In both treatments, Info and Norm, we observe the highest average WTS in Prob0.[20] Figure 1 shows the distributions of WTS across treatment variants, pooling data from treatments Norm and Info. In the latter treatment, we rely on subjects' unconditional WTS (i.e. the one stated before they receive information about the peer's choice).

[19]The treatment specific average minimum acceptable prices can be derived as 6 Euro – average WTS. While we are interested in differences across treatments and not subjects' WTS per se, it is interesting to contextualize the figures from Table 3. Schudy and Utikal (2017) observe a median minimum price of 3.50 Euro for sharing address data (full name, address) with a randomly selected anonymous student from the same university. Benndorf and Normann (2018) report an average minimum price of 8.32 Euro (median 5.00 Euro) for the disclosure of (knowingly unverifiable) personal data on preferences and demographic information to a telecommunications company.

[20]Note that the following data analysis abstracts from subjects unwilling to sell personal data for prices up to 6.00 Euro since we did not elicit their exact WTS and do not know whether they are willing to sell personal data for any price at all.

Non-parametric tests, as well as regressions, which allow us to control for potential NORM treatment fixed effects and subjects' personal characteristics, reveal that subjects' WTS in treatment variant PROB0 is significantly higher than in both information externality scenarios.

According to a Jonckheere-Terpstra test, distributions differ significantly across treatment variants ($p < 0.001$). Subjects' WTS in treatment variant PROB0 is significantly higher than in PROB50 and PROB100 (Mann Whitney ranksum tests, $p < 0.001$ for PROB0 vs. PROB50, for PROB0 vs. PROB100, and for PROB0 vs. (PROB50 and PROB100)). However, the distribution of subjects' WTS in PROB50 is not significantly different from that in PROB100 (Mann Whitney ranksum test, $p = 0.87$).

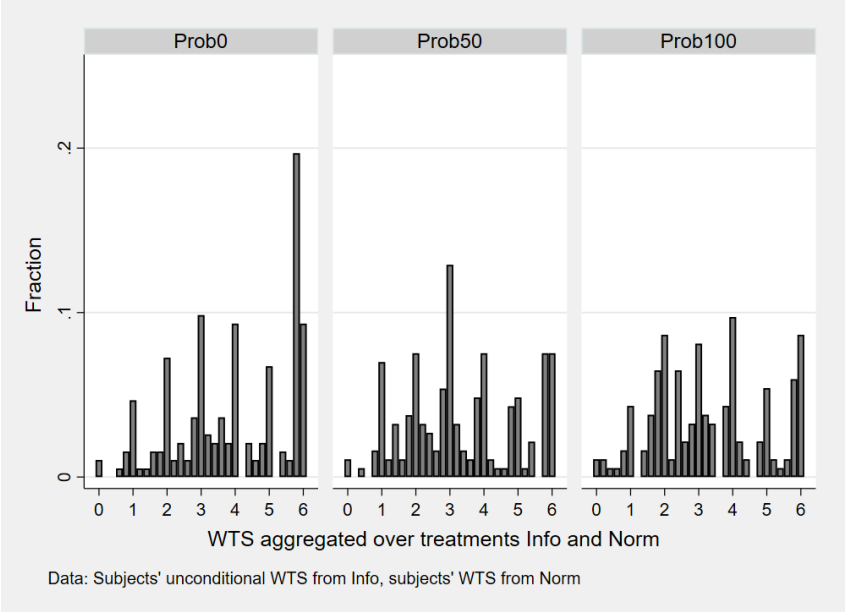

Figure 1: Willingness to Sell Personal Data Across Treatment Variants

Ordinary-least-squares regressions confirm the above results. Subjects' WTS is significantly higher in the treatment variant without data compromise (PROB0) compared to the information externality scenarios, see Column (1) of Table 4. Considering treatment variants PROB50 and PROB100 separately in Column (2), subjects demand on average 58 Cents (62 Cents) more in exchange for the disclosure of personal data in PROB50 (PROB100) than in PROB0. The insignificant Wald test result reported in the lower part of the table reveals that the WTS does not differ significantly between treatment variants PROB50 and PROB100. All treatment effects are robust to the inclusion of subjects' personal characteristics (see Columns (3) and (4)).[21] As further robustness checks, we rerun the entire analysis using Tobit regressions, see Table A.2 in

[21] Table A.1 in the appendix presents summary statistics for these control variables. Note that our regression specifications do not include type dummies for SVO: Altruistic type, SVO: Competitive type, and Westin: Privacy unconcerned as control variables because these types are very infrequent in our data.

the appendix. They corroborate the above results.

Taken together, the findings confirm Hypothesis H1 and we conclude:

Result 1: *Comparing* PROB50 *and* PROB100 *to* PROB0*, subjects' WTS is lower when there is a positive compromise probability. Subjects' WTS in treatment variant* PROB50 *is not different from subjects' WTS in treatment variant* PROB100*.*

Table 4: Willingness to Sell Personal Data: Impact of Compromise Probability

	(1)	(2)	(3)	(4)
PROB0	0.60***		0.64***	
	(0.00)		(0.00)	
PROB50		-0.58***		-0.60***
		(0.00)		(0.00)
PROB100		-0.62***		-0.68***
		(0.00)		(0.00)
NORM	-0.23	-0.23	-0.28*	-0.28*
	(0.11)	(0.11)	(0.05)	(0.05)
Age			-0.01	-0.01
			(0.70)	(0.69)
Gender: Female			-0.17	-0.17
			(0.24)	(0.23)
Risk proneness			-0.05	-0.05
			(0.18)	(0.17)
SVO: Prosocial type			-0.60***	-0.61***
			(0.00)	(0.00)
Westin: Privacy fundamentalist			-0.19	-0.19
			(0.17)	(0.18)
Norm obedience			0.00	0.00
			(0.70)	(0.71)
Constant	3.44***	4.04***	4.42***	5.08***
	(0.00)	(0.00)	(0.00)	(0.00)
Observations	564	564	559	559
R^2	0.03	0.03	0.07	0.07
Prob50 vs. Prob100 (p-value)		0.81		0.63

Notes: We present results from OLS regressions. Dependent variable: WTS in treatments INFO and NORM (in INFO: subjects' unconditional WTS). In Columns (3) and (4) we include a battery of control variables, comprising subjects' age and gender, their risk proneness (elicited unincentivized), their social value orientation type (from an SVO test, Murphy et al., 2011), their privacy concerns (classified in the form of Westin's privacy index types, Westin, 2001) and their degree of norm obedience (reversely elicited as agreement to various statements of social norm violations, taken from Traxler and Winter, 2012). Standard errors clustered at the pair level, p-values given in parentheses *** p<0.01, ** p<0.05, * p<0.1.

5.2 Willingness to Sell Personal Data: The Influence of Peer Information

Next, we turn to the analysis of peer effects in the INFO treatment. We hypothesized that subjects' conditional WTS increases with their peer's unconditional WTS, and that such peer effects are more prevalent in PROB100 than in PROB50.

We find that 23 percent of subjects in PROB50 and 30 percent in PROB100 change their WTS (not significantly different across treatment variants, $p = 0.26$ according to a χ^2 test). For the following ordinary-least-squares regressions, presented in Table 5, we focus on subjects' WTS in the PROB50 and PROB100 treatment variants. We regress subjects' conditional WTS on their unconditional WTS, their peer's WTS, a PROB100 treatment dummy and a dummy variable *Amends WTS* that captures whether the subject's conditional WTS differs from the unconditional one.

Column (1) of Table 5 reveals a significant average peer effect of 0.17. That means, subjects increase their own WTS by almost an entire 20-cents step for every Euro-unit increase in the peer's WTS, controlling for the level of subjects' unconditional WTS, their general tendency to amend their WTS, and any general treatment variant effects. The found peer effect remains virtually unchanged if we control for a range of subjects' characteristics, see Column (2).

The regression presented in Column (3) extends the one from Column (1) by adding an interaction term between the peer's WTS and the treatment variant dummy. It reveals that while the peer's WTS has a significant and positive effect on subjects' conditional WTS in the order of magnitude of 0.12 in PROB50, its effect is significantly more pronounced in PROB100 (0.12+0.11). Again, the findings are robust to the inclusion of further control variables, see Column (4). Likewise, results are robust to excluding the dummy variable *Amends WTS* from the covariate vector.[22]

As a final robustness check, we repeat the regression analysis from Table 5, using Tobit specifications. The results remain qualitatively and quantitatively the same, see Table A.3 in the appendix.

Overall, we confirm Hypotheses 2.1 and 2.2 and conclude that:

Result 2: *Considering data from treatment variants* PROB50 *and* PROB100 *in treatment* INFO*, subject's conditional WTS increases with the peer's WTS. This peer effect is relatively stronger if personal data is compromised with certainty.*

[22]Results available upon request from the authors.

Table 5: Determinants of Conditional WTS in Info Treatment Variants

	(1)	(2)	(3)	(4)
Unconditional WTS	0.85***	0.84***	0.85***	0.84***
	(0.00)	(0.00)	(0.00)	(0.00)
Peer's WTS	0.17***	0.17***	0.12***	0.12***
	(0.00)	(0.00)	(0.00)	(0.00)
Amends WTS	0.42**	0.41**	0.40**	0.39**
	(0.01)	(0.01)	(0.02)	(0.01)
Prob100	0.20*	0.19*	-0.19	-0.17
	(0.06)	(0.05)	(0.38)	(0.42)
Peer's WTS × Prob100			0.11*	0.10*
			(0.07)	(0.10)
Age		-0.00		0.00
		(0.96)		(0.98)
Gender: Female		0.17		0.16
		(0.11)		(0.12)
Risk proneness		-0.06*		-0.06**
		(0.05)		(0.04)
SVO: Prosocial type		-0.01		-0.02
		(0.93)		(0.85)
Westin: Privacy fundamentalist		-0.12		-0.10
		(0.23)		(0.26)
Norm obedience		0.00		0.00
		(0.50)		(0.48)
Constant	-0.19*	-0.05	0.02	0.10
	(0.09)	(0.93)	(0.93)	(0.85)
Observations	190	190	190	190
R^2	0.81	0.82	0.82	0.83

Notes: We present results from OLS regressions. Dependent variable: Conditional WTS in treatment variants Prob50 and Prob100 in treatment Info. In Columns (2) and (4) we include a battery of control variables, comprising subjects' age and gender, their risk proneness (elicited unincentivized), their social value orientation type (from an SVO test, Murphy et al., 2011), their privacy concerns (classified in the form of Westin's privacy index types, Westin, 2001) and their degree of norm obedience (reversely elicited as agreement to various statements of social norm violations, taken from Traxler and Winter, 2012). Standard errors clustered at the pair level, p-values given in parentheses *** p<0.01, ** p<0.05, * p<0.1.

The summary statistics presented in Table 3 indicate that, on average, subjects revise their WTS upward. In a further, not pre-registered analysis, we examine the question of whether being matched to a peer whose WTS is larger than one's own WTS has a stronger effect on subjects than being matched to a peer with a comparably lower WTS. We conjecture that conforming to the peer's choice may be more tempting when the peer is more willing to sell than otherwise – be it out of a desire for revenge or because being matched to a peer with a relatively higher WTS would give subjects an additional excuse for selling private data themselves. We report the results from this additional regression analysis in Table A.4 in the appendix. We split the sample into two similarly sized groups of subjects matched to a peer with a strictly higher unconditional WTS and subjects matched to a peer with a similar or lower unconditional WTS. In line with our expectations, the coefficient of the peer's WTS is relatively larger for subjects whose peer's WTS exceeds their own WTS (0.19* vs. 0.01). A Wald test finds the coefficients to be marginally significantly different at the 10-percent level ($p = 0.0968$). As our experiment was not explicitly designed to test for these different forms of peer effects, we can only take these findings as suggestive evidence that negative peer effects prevail.

5.3 Willingness to Sell Personal Data: The Influence of a Social Norm Focus

Next, we analyze if and how an injunctive norms focus influences individuals' WTS in the treatment variants of Prob50 and Prob100 in Norms.

Table A.5 in the Appendix provides evidence that our injunctive norm focus manipulations indeed work as intended. Subjects in Prob100 state a significantly lower socially appropriate WTS than those in Prob50, see Columns (1) and (2). Moreover, the actually chosen WTS is positively and significantly correlated with the stated social norms, see Columns (3) and (4). Subjects' behavior thus traces the stated social norms.[23]

To test Hypotheses 3.1 and 3.2, we compare reported WTS from the Norm treatment to the unconditional WTS from the Info treatment. Consider the respective mean WTS reported in Table 3 as well as Figure 2, which displays the distributions of subjects' WTS in treatment Norm (row 1) and treatment Info (row 2).

Mann-Whitney ranksum tests confirm the visual impression that the distribution of WTS is significantly shifted to the left in treatment Norm ($p = 0.03$ when considering Prob50 and Prob100 jointly).[24] The finding is confirmed in an additional regression analysis. In Column

[23] Our pre-registration did not include these analyses.

[24] Further Mann-Whitney ranksum test results produce $p = 0.17$ when considering Prob50 only and $p = 0.08$

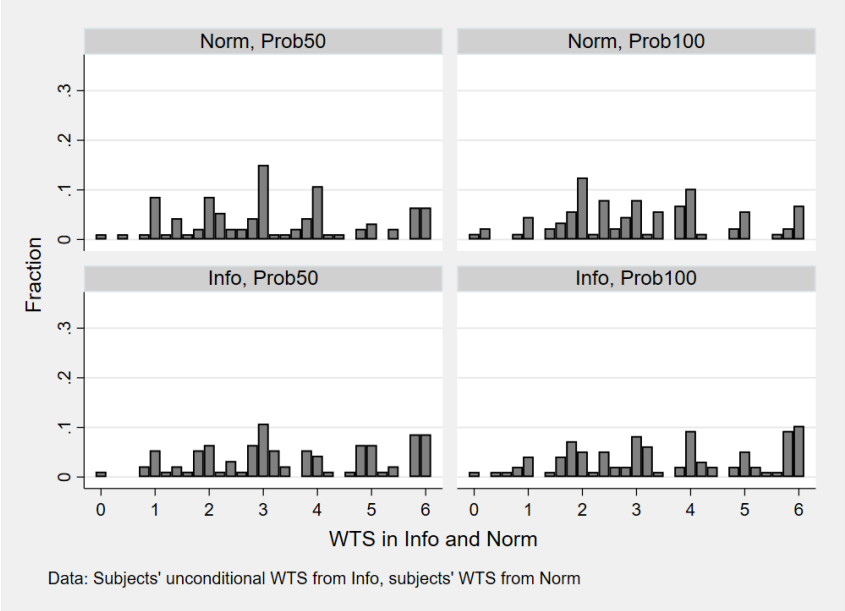

Figure 2: Willingness To Sell Personal Data Across INFO and NORM Treatment Variants

(1) of Table 6, we present a statistically and economically significant negative NORM treatment effect on subjects' WTS. Averaging over PROB50 and PROB100, subjects state a 39 Cent lower WTS in NORM than in INFO to protect their peer's expected surplus of about 2 Euro in Stage 4.[25] The result is robust to the inclusion of treatment variant fixed effects and the battery of individual control variables that were also included in Tables 4 and 5, (see Column (2) of Table 6). This confirms Hypothesis 3.1

To test Hypothesis 3.2, Columns (3) and (4) of Table 6 include the interaction term NORM × PROB100, which turns out insignificant. The injunctive norm focus seems to be comparable in the two treatment variants.[26] These findings are essentially unchanged if we repeat the regression analysis from Table 6, using Tobit specifications, see Table A.6 in the appendix. We hence summarize:

Result 3: *Comparing subjects' WTS in treatments* INFO *and* NORM*, we find that an injunctive norm focus decreases subjects' WTS. The level of the compromise probability does not significantly alter this effect.*

when considering PROB100 only.

[25]The expected value of the lottery ticket is 4 Euro. In view of the relatively small stakes, it seems reasonable to assume that subjects expect an average risk attitude close to neutrality. In fact, data from Stage 1 shows that subjects' average WTP for the lottery ticket is 3.91 Euro. The WTP for the lottery ticket is similar for all six treatment and treatment variant combinations ($p = 0.31$ in a Kruskal-Wallis test). Remember that, if the firm does not know a subject's WTP, subjects can buy the lottery ticket at an expected price of 2 Euro in Stage 4. This implies that disclosing the peer's personal data is associated with a loss in the peer's expected consumer surplus of about 2 Euro. This may thus be considered a rough quantification of the negative externality.

[26]Accordingly, treatment variant PROB100 induces a significantly lower social norm, but does not differently affect behavior.

Table 6: Willingness to Sell Personal Data: Impact of a Social Norm Focus

	(1)	(2)	(3)	(4)
Norm	-0.39**	-0.41**	-0.35	-0.37
	(0.03)	(0.02)	(0.17)	(0.13)
Prob100		-0.09	-0.00	-0.05
		(0.62)	(1.00)	(0.83)
Norm × Prob100			-0.09	-0.07
			(0.80)	(0.84)
Age		-0.00		-0.00
		(0.92)		(0.91)
Gender: Female		-0.21		-0.21
		(0.23)		(0.24)
Risk proneness		-0.06		-0.06
		(0.21)		(0.21)
SVO: Prosocial type		-0.57***		-0.57***
		(0.00)		(0.00)
Westin: Privacy fundamentalist		-0.19		-0.19
		(0.26)		(0.26)
Norm obedience		0.00		0.00
		(0.68)		(0.70)
Constant	3.52***	4.35***	3.52***	4.35***
	(0.00)	(0.00)	(0.00)	(0.00)
Observations	371	368	371	368
R^2	0.02	0.05	0.02	0.05

Notes: We report results from OLS regressions. Dependent variable: WTS in treatment variants Prob50 and Prob100 in treatments Info and Norm (in Info: subjects' unconditional WTS). In Columns (3) and (4) we include a battery of control variables, comprising subjects' age and gender, their risk proneness (elicited unincentivized), their social value orientation type (from an SVO test, Murphy et al., 2011), their privacy concerns (classified in the form of Westin's privacy index types, Westin, 2001) and their degree of norm obedience (reversely elicited as agreement to various statements of social norm violations, taken from Traxler and Winter, 2012). Standard errors clustered at the pair level, p-values given in parentheses *** p<0.01, ** p<0.05, * p<0.1.

6 Conclusion

Personal data is widely shared by individuals and often used by firms for personalized advertising and price discrimination, for example. Undoubtedly, this will intensify in the coming years. This may bring potential benefits in the form of better customization, better information, and the like. However, a wide-ranging usage of personal data can also have adverse consequences such as a redistribution of rents from consumers to firms. Besides, some individuals simply prefer to secure their privacy, irrespective of any material considerations. Yet, in many situations individuals cannot perfectly control data flows and depend on others to protect their privacy.

Our experiment is designed to study data disclosure in situations involving information externalities. Using a controlled experiment allows us to measure the value of personal data in an internally consistent way. We test whether individuals' willingness to sell personal data is affected by the degree to which their own data disclosure harms others' privacy, and possibly others' payoff prospects. We find that, on average, subjects are less willing to sell personal data in information externality scenarios, when sharing can compromise others' privacy and thereby imply harm on others. This finding is good news for data protection. Interestingly, however, subjects do not distinguish between the case in which others' privacy is harmed for certain and the case where it results only with 50% probability, a result that is more indicative of deontological than utilitarian reasoning. Compared to the PROB0 treatment variant, subjects in PROB50 and PROB100 demand on average 0.60 Euro more for data disclosure to increase the probability of an expected surplus of 2 Euro for their peer.

The context of our controlled experiment allowed us to additionally study the effects of two well-studied behavioral interventions: (i) providing information about a comparable subject's behavior, which potentially gives rise to peer effects as well as (ii) the application of a social norm focus. As regards the first intervention, we observe that 27% of subjects do react to the peer information and, on average, increase their willingness to sell data as a result. While the average WTS remains largely unchanged in PROB50, it increases by about 7% (0.25 Euro) in PROB100, see Table 3. From these observations we conclude that an intervention that draws on peer effects alone will potentially not reach many people – and if it does, it will likely only worsen the situation in information externality scenarios. Hence, transparency about peer behavior would not lead to more care for the data of others, quite the opposite.

In contrast, the results from our NORM treatment speak for the effectiveness of a social norms awareness campaign. Introducing an injunctive norm focus, that is, encouraging individuals to reflect on a widely shared social norm in the context of data disclosure can effectively decrease excessive data disclosure. We observe an average decrease in WTS of about 10% (0.25 Euro) when comparing the NORM and the INFO treatment (unconditional WTS) in the PROB50 treatment variant and an even larger decrease of about 12.5% (0.44 Euro) in the PROB100 variant, see Table 3. Against the backdrop of our results, we therefore consider policies and interventions which raise awareness for the potential side effects of data disclosure particularly promising.

Still, a number of important questions remain for future research. First, one may argue

that our design makes transparent that disclosing own personal data can compromise another individual's privacy, while such relationships are oftentimes difficult to detect in reality. Arguably, this salience may increase awareness for data privacy issues (e.g., John et al., 2011). In addition, the disclosure of the peer's data was embedded in an explicit market-exchange relationship between the firm and the individual in terms of data for money. In reality, individuals are often compensated with products and services that do not have an obvious monetary value (e.g., a free mail account). This alters the framing of and thus potentially the behavior in decision-making situation. Second, our experiment has focused on information externalities affecting others close to the individual. While one could argue that individuals are potentially even more concerned about the well-being of real-life peers than about 'experiment peers', how the social proximity of the affected party shapes individuals' willingness to disclose personal data remains an open question. It is up to future research to explore these effects of salience and social proximity as well as their potential interrelations in greater detail. In this context, it would be interesting to study how social norms and behavior evolve over time. Furthermore, our experiment was conducted with subjects from Germany, and there exists evidence that privacy is particularly important in this country (e.g., Prince and Wallsten, forthcoming). This calls for further cross-cultural comparisons. Moreover, our present design features relatively high data compromise probabilities ($\geq 50\%$), which are, moreover, openly communicated to subjects. It would be interesting to see how individuals' propensity to share their own and others' data might differ in settings with lower compromise probabilities or in settings with ambiguity. This would also help identify whether individuals are indeed largely reasoning deontologically, such that their willingness to disclose personal data is independent of the compromise probabilities (as currently suggested by the insignificant treatment difference between Prob50 and Prob100 discussed in section 5.1). We regard the proposed studies as the logical next steps to further explore and get a better understanding of the determinants of data sharing in information externality scenarios.

Appendix

Table A.1: Summary Statistics on Control Variables

	Mean	Std. dev.	Min	Max	N
Age	23.75	2.80	7.00	37.00	592
Gender: Female	0.58	–	0	1	592
Risk proneness	4.75	2.10	0.00	10.00	592
SVO: Altruistic type	0.00	–	0	1	591
SVO: Competitive type	0.00	–	0	1	591
SVO: Individualistic type	0.26	–	0	1	591
SVO: Prosocial type	0.73	–	0	1	591
Westin: Privacy fundamentalist	0.54	–	0	1	592
Westin: Privacy pragmatist	0.44	–	0	1	592
Westin: Privacy unconcerned	0.02	–	0	1	592
Norm obedience	46.35	9.24	8.00	60.00	592

Standard deviations omitted for dummy variables. Westin's privacy index types generated as in Westin (2001). Social value orientation (SVO) types generated as in Murphy et al. (2011). Norm obedience elicited in the style of Traxler and Winter (2012). Note that only 591 participants answered the SVO part of the questionnaire.

Table A.2: Robustness checks: Tobit Regressions. Willingness to Sell Personal Data: Impact of Compromise Probability

	(1)	(2)	(3)	(4)
Prob0	0.62***		0.67***	
	(0.00)		(0.00)	
Prob50		-0.60***		-0.63***
		(0.00)		(0.00)
Prob100		-0.63***		-0.71***
		(0.00)		(0.00)
Norm	-0.25	-0.25	-0.31**	-0.31**
	(0.12)	(0.12)	(0.05)	(0.05)
Age			-0.02	-0.02
			(0.54)	(0.53)
Gender: Female			-0.18	-0.18
			(0.24)	(0.24)
Risk proneness			-0.06	-0.06
			(0.15)	(0.15)
SVO: Prosocial type			-0.69***	-0.70***
			(0.00)	(0.00)
Westin: Privacy fundamentalist			-0.23	-0.23
			(0.13)	(0.14)
Norm obedience			0.00	0.00
			(0.60)	(0.61)
Constant	3.51***	4.13***	4.76***	5.45***
	(0.00)	(0.00)	(0.00)	(0.00)
Observations	564	564	558	558
Pseudo R^2	0.01	0.01	0.02	0.02
Prob50 vs. Prob100 (p-value)		0.86		0.68

Notes: We present results from Tobit regressions. Dependent variable: WTS in treatments Info and Norm (in Info: subjects' unconditional WTS). In Columns (3) and (4) we include a battery of control variables, comprising subjects' age and gender, their risk proneness (elicited unincentivized), their social value orientation type (from an SVO test, Murphy et al., 2011), their privacy concerns (classified in the form of Westin's privacy index types, Westin, 2001) and their degree of norm obedience (reversely elicited as agreement to various statements of social norm violations, taken from Traxler and Winter, 2012). Standard errors clustered at the pair level, p-values given in parentheses *** p<0.01, ** p<0.05, * p<0.1.

Table A.3: Robustness checks: Tobit Regressions. Determinants of Conditional WTS in Info Treatment Variants

	(1)	(2)	(3)	(4)
Unconditional WTS	0.89***	0.88***	0.89***	0.88***
	(0.00)	(0.00)	(0.00)	(0.00)
Peer's WTS	0.20***	0.20***	0.14***	0.14***
	(0.00)	(0.00)	(0.00)	(0.00)
Amends WTS	0.39**	0.39**	0.37**	0.37**
	(0.02)	(0.02)	(0.03)	(0.02)
Prob100	0.25**	0.24**	-0.18	-0.17
	(0.04)	(0.03)	(0.43)	(0.45)
Peer's WTS × Prob100			0.12*	0.12*
			(0.07)	(0.08)
Age		-0.00		-0.00
		(0.88)		(0.93)
Gender: Female		0.17		0.16
		(0.11)		(0.12)
Risk proneness		-0.06**		-0.06**
		(0.05)		(0.04)
SVO: Prosocial type		-0.04		-0.06
		(0.73)		(0.64)
Westin: Privacy fundamentalist		-0.13		-0.12
		(0.20)		(0.25)
Norm obedience		0.01		0.01
		(0.45)		(0.42)
Constant	-0.40**	-0.17	-0.17	-0.01
	(0.01)	(0.77)	(0.44)	(0.99)
Observations	190	190	190	190
R^2	0.41	0.43	0.42	0.43

Notes: We present results from Tobit regressions. Dependent variable: Conditional WTS in treatment variants Prob50 and Prob100 in treatment Info. In Columns (2) and (4) we include a battery of control variables, comprising subjects' age and gender, their risk proneness (elicited unincentivized), their social value orientation type (from an SVO test, Murphy et al., 2011), their privacy concerns (classified in the form of Westin's privacy index types, Westin, 2001) and their degree of norm obedience (reversely elicited as agreement to various statements of social norm violations, taken from Traxler and Winter, 2012). *Amends WTS* is a dummy variable equal to one if the subject's conditional WTS differs from the unconditional one. Standard errors clustered at the pair level, p-values given in parentheses *** p<0.01, ** p<0.05, * p<0.1.

Table A.4: Additional Tests: Determinants of Conditional WTS in Info Treatment Variants

	(1) Peer's WTS > own WTS	(2) Peer's WTS ≤ own WTS
Unconditional WTS	0.78***	0.98***
	(0.00)	(0.00)
Peer's WTS	0.19*	0.01
	(0.06)	(0.86)
Amends WTS	1.37***	-0.94***
	(0.00)	(0.00)
Prob100	0.17	0.09
	(0.14)	(0.21)
Age	0.01	-0.01
	(0.73)	(0.34)
Gender: Female	0.16	-0.08
	(0.20)	(0.33)
Risk proneness	-0.07**	-0.02
	(0.03)	(0.33)
SVO: Prosocial type	-0.18	0.08
	(0.22)	(0.37)
Westin: Privacy fundamentalist	-0.08	0.01
	(0.50)	(0.84)
Norm obedience	0.01	-0.00
	(0.11)	(0.87)
Constant	-0.55	0.44
	(0.47)	(0.20)
Observations	94	96
R^2	0.87	0.95
Peer's WTS in (1) vs. Peer's WTS in (2) (p-value)	0.10	

Notes: We present results from OLS regressions. Dependent variable: Conditional WTS in treatment variants Prob50 and Prob100 in treatment Info. We include a battery of control variables, comprising subjects' age and gender, their risk proneness (elicited unincentivized), their social value orientation type (from an SVO test, Murphy et al., 2011), their privacy concerns (classified in the form of Westin's privacy index types, Westin, 2001) and their degree of norm obedience (reversely elicited as agreement to various statements of social norm violations, taken from Traxler and Winter, 2012). *Amends WTS* is a dummy variable equal to one if the subject's conditional WTS differs from the unconditional one. Standard errors clustered at the pair level, p-values given in parentheses *** p<0.01, ** p<0.05, * p<0.1.

Table A.5: Additional Tests: Impact of a Social Norm Focus on Reported Appropriateness and WTS

	(1) Social Norm WTS	(2) Social Norm WTS	(3) Actual WTS	(4) Actual WTS
Prob100	-0.44**	-0.47**	0.11	0.04
	(0.04)	(0.03)	(0.63)	(0.87)
Social norm WTS			0.42***	0.41***
			(0.00)	(0.00)
Age		0.02		-0.04
		(0.48)		(0.41)
Gender: Female		-0.39*		-0.39
		(0.09)		(0.10)
Risk proneness		-0.04		-0.05
		(0.49)		(0.37)
SVO: Prosocial type		0.03		-0.53**
		(0.91)		(0.02)
Westin: Privacy fundamentalist		-0.23		0.02
		(0.31)		(0.92)
Norm obedience		-0.01		0.00
		(0.17)		(0.88)
Constant	2.83***	3.55***	1.94***	3.66***
	(0.00)	(0.00)	(0.00)	(0.01)
Observations	197	194	181	178
R^2	0.02	0.05	0.15	0.20

Notes: We present results from OLS regressions using observations from treatment variants Prob50 and Prob100 in treatment Norm. The dependent variable *Social Norm WTS* is defined as subjects' stated socially appropriate WTS. In Columns (2) and (4), we include a battery of control variables, comprising subjects' age and gender, their risk proneness (elicited unincentivized), their social value orientation type (from an SVO test, Murphy et al., 2011), their privacy concerns (classified in the form of Westin's privacy index types, Westin, 2001) and their degree of norm obedience (reversely elicited as agreement to various statements of social norm violations, taken from Traxler and Winter, 2012). Standard errors clustered at the pair level, p-values given in parentheses *** p<0.01, ** p<0.05, * p<0.1.

Table A.6: Robustness checks: Tobit Regressions. Willingness to Sell Personal Data: Impact of a Social Norm Focus

	(1)	(2)	(3)	(4)
Norm	-0.42**	-0.44**	-0.37	-0.40
	(0.03)	(0.02)	(0.18)	(0.14)
Prob100		-0.08	0.01	-0.03
		(0.67)	(0.96)	(0.89)
Norm × Prob100		-0.10	-0.09	
			(0.79)	(0.81)
Age		-0.01		-0.01
		(0.81)		(0.80)
Gender: Female		-0.21		-0.21
		(0.26)		(0.26)
Risk proneness		-0.07		-0.07
		(0.21)		(0.21)
SVO: Prosocial type		-0.65***		-0.65***
		(0.00)		(0.00)
Westin: Privacy fundamentalist		-0.22		-0.22
		(0.24)		(0.24)
Norm obedience		0.01		0.01
		(0.61)		(0.62)
Constant	3.59***	4.61***	3.59***	4.60***
	(0.00)	(0.00)	(0.00)	(0.00)
Observations	371	368	371	368
Pseudo R^2	0.00	0.01	0.00	0.01

Notes: We report results from Tobit regressions. Dependent variable: WTS in Prob50 and Prob100 treatment variants in treatments Info and Norm (in Info: subjects' unconditional WTS). In Columns (3) and (4) we include a battery of control variables, comprising subjects' age and gender, their risk proneness (elicited unincentivized), their social value orientation type (from an SVO test, Murphy et al., 2011), their privacy concerns (classified in the form of Westin's privacy index types, Westin, 2001) and their degree of norm obedience (reversely elicited as agreement to various statements of social norm violations, taken from Traxler and Winter, 2012). Standard errors clustered at the pair level, p-values given in parentheses *** p<0.01, ** p<0.05, * p<0.1.

References

Acemoglu, Daron, Ali Makhdoumi, Azarakhsh Malekian, and Asuman Ozdaglar, "Too much data: Prices and inefficiencies in data markets," *American Economic Journal: Microeconomics*, forthcoming.

Ackfeld, Viola and Werner Güth, "Personal information disclosure under competition for benefits: Is sharing caring?," *MPI Collective Goods Discussion Paper*, 2019, (2019/4).

Acquisti, Alessandro and Christina Fong, "An experiment in hiring discrimination via online social networks," *Management Science*, 2020, *66* (3), 1005–1024.

_ , Curtis Taylor, and Liad Wagman, "The economics of privacy," *Journal of Economic Literature*, 2016, *54* (2), 442–492.

_ , Laura Brandimarte, and George Loewenstein, "Privacy and human behavior in the age of information," *Science*, 2015, *347* (6221), 509–514.

_ , _ , and _ , "Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age," *Journal of Consumer Psychology*, 2020, *30* (4), 736–758.

_ , Leslie K John, and George Loewenstein, "The impact of relative standards on the propensity to disclose," *Journal of Marketing Research*, 2012, *49* (2), 160–174.

Agerström, Jens, Rickard Carlsson, Linda Nicklasson, and Linda Guntell, "Using descriptive social norms to increase charitable giving: The power of local norms," *Journal of Economic Psychology*, 2016, *52*, 147–153.

Barocas, Solon and Karen Levy, "Privacy dependencies," *Washington Law Review*, 2020, *95*, 555–616.

Bartke, Simon, Andreas Friedl, Felix Gelhaar, and Laura Reh, "Social comparison nudges – Guessing the norm increases charitable giving," *Economics Letters*, 2017, *152*, 73–75.

Becker, Gordon M., Morris H. Degroot, and Jacob Marschak, "Measuring utility by a single-response sequential method," *Behavioral Science*, 1964, *9* (3), 226–232.

Benndorf, Volker and Hans-Theo Normann, "The willingness to sell personal data," *The Scandinavian Journal of Economics*, 2018, *120* (4), 1260–1278.

_ , **Dorothea Kübler, and Hans-Theo Normann**, "Privacy concerns, voluntary disclosure of information, and unraveling: An experiment," *European Economic Review*, 2015, *75*, 43–59.

Bergemann, Dirk, Alessandro Bonatti, and Tan Gan, "The economics of social data," *RAND Journal of Economics*, 2022, *53* (2), 263–296.

Bock, Olaf, Ingmar Baetge, and Andreas Nicklisch, "hroot: Hamburg registration and organization online tool," *European Economic Review*, 2014, *71*, 117–120.

Calo, Ryan, "The boundaries of privacy harm," *Indiana Law Journal*, 2011, *86*, 1131.

Carlsson, Fredrik, Jorge H. García, and Åsa Löfgren, "Conformity and the demand for environmental goods," *Environmental and Resource Economics*, 2010, *47* (3), 407–421.

Chen, Daniel L., Martin Schonger, and Chris Wickens, "oTree – An open-source platform for laboratory, online, and field experiments," *Journal of Behavioral and Experimental Finance*, 2016, *9*, 88–97.

Chen, Roy and Yan Chen, "The potential of social identity for equilibrium selection," *American Economic Review*, 2011, *101* (6), 2562–2589.

Chen, Yan and Sherry Xin Li, "Group identity and social preferences," *American Economic Review*, 2009, *99* (1), 431–457.

Choi, Jay Pil, Doh-Shin Jeon, and Byung-Cheol Kim, "Privacy and personal data collection with information externalities," *Journal of Public Economics*, 2019, *173*, 113–124.

Cialdini, Robert B, Linda J Demaine, Brad J Sagarin, Daniel W Barrett, Kelton Rhoads, and Patricia L Winter, "Managing social norms for persuasive impact," *Social influence*, 2006, *1* (1), 3–15.

Cialdini, Robert B., Raymond R. Reno, and Carl A. Kallgren, "A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places," *Journal of Personality and Social Psychology*, 1990, *58* (6), 1015–1026.

Collis, Avinash, Alex Moehring, Ananya Sen, and Alessandro Acquisti, "Information Frictions and Heterogeneity in Valuations of Personal Data," *Mimeo*, 2021.

Croson, Rachel and Jen Yue Shang, "The impact of downward social information on contribution decisions," *Experimental Economics*, 2008, *11* (3), 221–233.

Dohmen, Thomas, Armin Falk, David Huffman, and Uwe Sunde, "Are risk aversion and impatience related to cognitive ability?," *American Economic Review*, 2010, *100* (3), 1238–1260.

Eckel, Catherine C. and Philip J. Grossman, "Managing diversity by creating team identity," *Journal of Economic Behavior & Organization*, 2005, *58* (3), 371–392.

Fairfield, Joshua A. T. and Christoph Engel, "Privacy as a public good," *Duke Law Journal*, 2015, *65*, 385.

Goh, Khim-Yong, Kai-Lung Hui, and Ivan Png, "Privacy and marketing externalities: Evidence from Do Not Call," *Management Science*, 2015, *61* (12), 2982–3000.

Hannak, Aniko, Gary Soeller, David Lazer, Alan Mislove, and Christo Wilson, "Measuring price discrimination and steering on E-commerce web sites," *Proceedings of the 2014 Conference on Internet Measurement Conference*, 2014, pp. 305–318.

Hermstrüwer, Yoan and Stephan Dickert, "Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge," *International Review of Law and Economics*, 2017, *51*, 38–49.

Hett, Florian, Mario Mechtel, and Markus Kröll, "The structure and behavioral effects of revealed social identity preferences," *The Economic Journal*, 2020, *130* (632), 2569–2595.

Hidir, Sinem and Nikhil Vellodi, "Privacy, personalization, and price discrimination," *Journal of the European Economic Association*, 2021, *19* (2), 1342–1363.

Ichihashi, Shota, "The economics of data externalities," *Journal of Economic Theory*, 2021, *196*, 105316.

Jernigan, Carter and Behram F. T. Mistree, "Gaydar: Facebook friendships expose sexual orientation," *First Monday*, 2009.

John, Leslie, Alessandro Acquisti, and George Loewenstein, "Strangers on a plane: Context-dependent willingness to divulge sensitive information," *Journal of Consumer Research*, 2011, *37*, 858–873.

Keizer, Kees, Siegwart Lindenberg, and Linda Steg, "The spreading of disorder," *Science*, 2008, *322* (5908), 1681–1685.

Kimbrough, Erik O. and Alexander Vostroknutov, "Norms make preferences social," *Journal of the European Economic Association*, 2016, *14* (3), 608–638.

Krupka, Erin and Roberto A. Weber, "The focusing and informational effects of norms on pro-social behavior," *Journal of Economic Psychology*, 2009, *30* (3), 307–320.

Krupka, Erin L. and Roberto A. Weber, "Identifying social norms using coordination games: Why does dictator game sharing vary?," *Journal of the European Economic Association*, 2013, *11* (3), 495–524.

Lee, Yi-Shan and Roberto Weber, "Revealed Privacy Preferences: Are Privacy Choices Rational?," 2022. Working paper.

Lin, Tesary, "Valuing Intrinsic and Instrumental Preferences for Privacy," *Marketing Science*, forthcoming.

Lindström, Björn, Simon Jangard, Ida Selbing, and Andreas Olsson, "The role of a common is moral heuristic in the stability and change of moral norms," *Journal of Experimental Psychology: General*, 2018, *147* (2), 228.

MacCarthy, Mark, "New directions in privacy: Disclosure, unfairness and externalities," *Journal of Law and Policy for the Information Society*, 2010, *6*, 425.

Mentzakis, Emmanouil and Stuart Mestelman, "Hypothetical bias in value orientations ring games," *Economics Letters*, 2013, *120* (3), 562–565.

Murphy, Ryan O., Kurt A. Ackermann, and Michel Handgraaf, "Measuring social value orientation," *Judgment and Decision Making*, 2011, *6* (8), 771–781.

Prince, Jeffrey and Scott Wallsten, "How Much is Privacy Worth Around the World and Across Platforms?," *Journal of Economics and Management Strategy*, forthcoming.

Richards, Neil M., "The dangers of surveillance," *Harvard Law Review*, 2012, *126*, 1934.

Schudy, Simeon and Verena Utikal, "You must not know about me – On the willingness to share personal data," *Journal of Economic Behavior & Organization*, 2017, *141*, 1–13.

Thöni, Christian and Simon Gächter, "Peer effects and social preferences in voluntary cooperation: A theoretical and experimental analysis," *Journal of Economic Psychology*, 2015, *48*, 72–88.

Traxler, Christian and Joachim Winter, "Survey evidence on conditional norm enforcement," *European Journal of Political Economy*, 2012, *28* (3), 390–398.

Westin, A., "Privacy on & off the Internet: What consumers want," *Hackensack, NJ: Privacy & American Business*, 2001.