Hermstrüwer, Yoan; Dickert, Stephan

**Working Paper**

# Tearing the veil of privacy law: An experiment on chilling effects and the right to be forgotten

Preprints of the Max Planck Institute for Research on Collective Goods, No. 2013/15

**Provided in Cooperation with:**
Max Planck Institute for Research on Collective Goods

*Suggested Citation:* Hermstrüwer, Yoan; Dickert, Stephan (2013) : Tearing the veil of privacy law: An experiment on chilling effects and the right to be forgotten, Preprints of the Max Planck Institute for Research on Collective Goods, No. 2013/15, Max Planck Institute for Research on Collective Goods, Bonn

This Version is available at:
https://hdl.handle.net/10419/84983

**Preprints of the
Max Planck Institute for
Research on Collective Goods
Bonn 2013/15**

# Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten

Yoan Hermstrüwer
Stephan Dickert

Preprints of the
Max Planck Institute
for Research on Collective Goods

Bonn 2013/15

# Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten

Yoan Hermstrüwer / Stephan Dickert

August 2013

Max Planck Institute for Research on Collective Goods, Kurt-Schumacher-Str. 10, D-53113 Bonn
http://www.coll.mpg.de

# Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten

**Yoan Hermstrüwer and Stephan Dickert***

## Abstract

Privacy law relies on the argument that consent does not entail any relevant impediments for the liberty of the consenting individual. Challenging this argument, we experimentally investigate whether consent to the publication of personal information in cyberspace entails self-coercion on a social norm level. Our results suggest that the monetary benefits from consent constitute a price that people are willing to accept for increased compliance with social norms. Providing people with a prior consent option is sufficient to generate chilling effects (i.e., a reduction of norm-deviant behavior). However, nudging people towards potential publicity does not increase the value they place on privacy. We also test how the default design of the right to deletion of personal information (right to be forgotten) affects chilling effects and privacy valuations. Surprisingly, the right to be forgotten does not reduce chilling effects. Moreover, individuals tend to stick with the status quo of permanent information storage.

*JEL:* A13, C91, C93, D03, K29

*Keywords:* Behavioral Law and Economics of Privacy, Consent, Right to Be Forgotten, Dictator Games, Social Norms, Nudges

---

* YOAN HERMSTRÜWER is Research Fellow at the Max Planck Institute for Research and Collective Goods and PhD student at the University of Bonn, School of Law. STEPHAN DICKERT is Assistant Professor at the Vienna University of Economics and Business, Institute for Marketing and Consumer Research. This paper was awarded the Göran Skogh Award for the most promising paper presented at the 30th Annual Conference of the European Association of Law and Economics in Warsaw (EALE 2013). We would like to thank Jonathan Baron, Stefan Bechtold, Daniel Chen, Christoph Engel, Joshua Fairfield, Susann Fiedler, Christine Jolls, Adrian Künzler, Pascal Langenbach, Stefanie Ostheimer, and seminar participants at Yale Law School, the Max Planck Institute for Research on Collective Goods, the Law and Economics Seminar at the ETH Zürich, and EALE 2013 for valuable comments and discussions. We also thank Rafael Aigner and Tobias Salz for their insights on modeling, Lukas Kießling for helpful assistance in programming, and the Cologne Laboratory of Economic Research. For questions and comments, please contact >hermstruewer@coll.mpg.de<.

*"…the very minute a thought is threatened with publicity it seems to shrink toward mediocrity."*

*Oliver Wendell Holmes (1872, p. 403)*

## 1. Introduction

Consenting to the collection and storage of personal information has become a risky activity. Today every internet user has to brace herself for the risk that personal information collected by internet companies like Facebook or Google might sooner or later be subject to an unwanted gaze (Rosen 2001). It may inadvertently end in the hands of the National Security Agency (NSA); or it may unexpectedly become public. Consider the case of a young mother whose personal information was collected by Netflix. Based on an anonymized dataset about film preferences, she was identified as being homosexual. She claimed that public knowledge about her sexual orientation would hinder her and her children's ability to live peaceful lives within her rural community (*Doe v. Netflix, Inc.* [N.D. Cal. 2009]). Watching certain films caused her tremendous reputational harm. Had she known that her film preferences may become public, would she have avoided watching her preferred films in the first place? In this article, we shed light on the behavioral effects of private-sector surveillance and present the first behavioral analysis of the right to be forgotten as a tool to recover privacy losses.

A major problem of privacy law is that we lack a compelling account of how exactly a privacy loss might corrode our liberties or welfare. While the benefits of a privacy loss are usually very palpable – discounts, personalized services, or convenience -, its costs are rather ill-defined. It is therefore relatively easy to refute the diffuse fears and the sense of "creepiness" associated with the free flow and permanent storage of personal information (Posner 2008; Bull 2011); it stands to reason that privacy law helps the suppression of „discrediting facts", thereby catalyzing adverse selection and inefficient transactions (Posner 1978; Stigler 1980; Posner 1981). It is much more difficult, however, to defend privacy with arguments which nobody would reasonably object to on empirical grounds. Coping with this problem, scholars have argued that privacy losses generate similar normalizing power as Bentham's *panopticon* (Foucault 1977; Lyon 2006). They have repeatedly claimed that a watchful gaze resulting from a privacy loss produces compliance with the law or the normative expectations of their community (Sunstein 2003). When being watched, people will be deterred from making choices that do not conform to mainstream expectations (Mitrou 2010). Tying in with First Amendment doctrine, philosophers and lawyers have defined this as a chilling effect on civil liberties (White and Zimbardo 1975; Goodin and Jackson 2007; Richards 2013).

The common assumption underlying the chilling effects hypothesis is that people cannot choose whether they want personal information registered. This typically holds for government surveillance; people do not give their consent to government surveillance. It is therefore very difficult to autonomously sidestep the subtle kind of coercion that potential publicity im-

poses on them. The U.S. Supreme Court has been reluctant to recognize chilling effects as a sufficient ground for a violation of constitutional rights. In *Clapper v. Amnesty International USA*, for instance, the court rejected an infringement of liberty, arguing that threatened injury resulting from the interception of private communications must be "certainly impending" (568 U.S.___[2013]). The German Constitutional Court, on the other hand, has repeatedly ascertained violations of the right to privacy on the grounds that uncertainty about the collection and storage of personal information might lead to conforming behavior (BVerfGE 65, 1 [1983]; Bull 2011).

A more complex behavioral problem – one that has received much less attention in the existing literature – arises in case of private-sector surveillance. Private-sector surveillance is often legitimized on the basis of an express agreement; it leaves room for different trade-offs than government surveillance which is typically based on coerced privacy losses. Under European privacy law, for instance, personal information may not be processed without consent. Despite their general sensitivity to diffuse fears, privacy lawyers have largely ignored the psychological intertwining between consent and chilling effects in case of private-sector surveillance. Even German courts have been reluctant to rely on the chilling effects argument when people had the opportunity to avoid surveillance by refusing consent (Britz 2010). The reasons are threefold. First, even though it is rather obvious that consent is seducing because of palpable incentives to disclose personal information (Haggerty and Ericson 2000), it is usually not seen as a tool used to receive monetary benefits. Second, consent is rarely seen as an expression of normative preferences. Third, consent is never seen as the potential resolution of a conflict between normative preferences and preferences for money. Imagine an Internet service provider offering you a discount if you consent to the disclosure of information about your book taste. Would you prefer a discount over your ability to be unobserved when reading Mao's *Little Red Book* or Milne's *Winnie-the-Pooh*? In case of consent, would you stop reading books that others would regard as deviant from their normative expectations?

As we will show in our experimental investigation, there is a risk that people will experience a chilling effect when consenting to the disclosure of personal information. This chilling effect is conceptualized as an increased propensity to comply with social norms. For the purposes of this article, we define social norms as jointly recognized understandings or expectations about types of behavior that are pro- or prescribed (Elster 1989; Bicchieri 2006). Our findings suggest that providing people with an incentivized ex ante consent option will lure them into surveillance and induce them to forego the benefits from norm deviations – the benefits from exercising their civil liberties.

The chilling effects hypothesis ties in with another pressing legal policy problem. In an age of permanent information storage, there is an increasing risk that people become entrenched in their past. People who once deviated from a legal or social norm are likely to be remembered as norm violators a long time after the fact. They incur the risk of having their reputations stained for a lifetime (Zittrain 2008). Consider the case of a Canadian who was denied entry to the U.S. in 2006 because according to an article stored online he had taken LSD in the 1960s

(Mayer-Schönberger 2009); or consider the case of a Spaniard who fears social repercussions because of a 15-year-old online notice mentioning his failure to repay taxes (European Court of Justice, *Google Spain, S.L., Google Inc. v AEPD, Mario Costeja González*, Case C-131/12 [2012]). These phenomena are exacerbated by the fact that truthful gossip is harder to sustain in large societies than in the context-rich environment of close-knit communities (Tönnies 1887; Ellickson 1991; Strandburg 2006).[1] In cyberspace, people incur an increasing risk of being (mis-)judged on the basis of bits and pieces of outdated information taken out of context (Rosen 2001; Nissenbaum 2010). Permanent storage of digital information, it appears, has considerably increased the expected cost of deviating from normative expectations and exercising civil liberties.

One way to cushion this behavioral pressure may be to provide people with a right to delete personal information, a right to be forgotten (Mayer-Schönberger 2009; Rosen 2011; Rosen 2012). If people anticipate that there is an option to escape the watchful gaze, this might allay their privacy fears. However, we lack a coherent account of the potential behavioral effects of privacy fears. While a reduction of privacy fears might dampen chilling effects on liberty (Bannon 2006; Mayer-Schönberger 2009), it may instead lower the inhibition threshold to disclose personal information, thereby reducing privacy and bolstering chilling effects. Moreover, chilling effects and privacy valuations might be influenced by such subtle factors as the default design of the right to be forgotten. People who anticipate that personal information will be automatically deleted (deletion default) might have a lower perception of risk than people who have to claim deletion actively (retention default). A plausible explanation is that most people will have a tendency to stick with the status quo (Samuelson and Zeckhauser 1988) and anticipate that the privacy risks incurred in case of a retention default will be higher. Our results indicate that a deletion default does not affect privacy valuations and does not dampen chilling effects. Furthermore, we find that only about 25 % of our sample used their right to be forgotten.

The remainder of this article is organized as follows. In Section 2, we elaborate on the incomplete nature of autonomy, chilling effects, and deletion as arguments in privacy law, and discuss empirical evidence on the factors driving privacy fears and privacy valuations. In Section 3, we address the methodological challenges of our experiment and present our experimental design. Section 4 provides an overview of our behavioral predictions. Section 5 presents an analysis of our experimental results. We conclude with a discussion of the implications for privacy law and legal policy in Section 6.

1 While social sanctions are immediately targeted at the person deviating from a social norm, gossip consists in spreading reputational information about a person who has engaged in deviant behavior, but is not present (Feinberg et al. 2012).

# 2. Legal and Behavioral Foundations

## 2.1. Autonomy, Chilling Effects, and Deletion Within the Bounds of Privacy Law

European privacy law implicitly assumes that consent to the disclosure of personal information is the ultimate expression of autonomous choice, irrespective of the consequences that this choice entails.[2] In this sense, the concept of autonomy and consent is deeply "agnostic about substance" (Solove 2013). The right to consent is purely procedural. In accordance with procedural conceptions of rights (see Nozick 1974; Sen 2010), it is specified only as a choice of actions or strategies. The strategies chosen by the recipients of personal information and the outcomes emanating from their choice is irrelevant under this account. In recognizing this, privacy law bows to autonomy.

We argue that this approach to privacy is incomplete, because it implicitly assumes that the outcome resulting from consent is unlikely to impose legally relevant constraints on the consenting person. Through the lens of constitutional law, coercion resulting from a privacy loss cannot be clearly qualified as an impediment to liberty if the very reason for this privacy loss is an autonomous decision itself.[3] This line of reasoning rests on the strong assumption that autonomy is the expression of an individual's preferences as revealed through the observable choice of consent. Exclusively looking at the autonomous exercise of the right to consent may short-circuit the chilling effects argument with its very *raison d'être*, that is, autonomy. If one of the objectives of privacy law is to forestall chilling effects (Sunstein 2003; Zittrain 2008), the law cannot ignore the chill of legal but socially non-conforming behaviors, just because an individual has given her consent.

It is important to note, however, that consent will only cause a behavioral change if the consenting individual is driven by her beliefs regarding society's beliefs about her behavior, i.e., her second-order beliefs (McAdams and Rasmusen 2007). For chilling effects to occur, people must be driven by the desire to please or by fear of the consequences resulting from the violation of normative expectations (see Sugden 1986; Bernheim 1994; Posner 2000; Young 2008; Krupka and Weber 2013). Under these assumptions, privacy law reduces the expected reputational cost associated with norm-deviations because it deprives society of the information necessary for social sanctions (McAdams 1997). Compliance resulting from a privacy loss and chilling effects can be seen as a costly investment to avoid such sanctions. Monetary

2 According to EU law, personal information may not be processed without consent. This principle is enshrined in Art. 8 II of the Charter of Fundamental Rights of the European Union and Art. 8 of the European Convention on Human Rights. It is also laid down in Art. 7 of the European Data Protection Directive 95/46/EC and § 4 I of the German Federal Data Protection Act (BDSG).

3 The German Constitutional Court acknowledges that data storage and opaque data processing may cause a "diffuse threat" justifying constitutional protection (BVerfGE 125, 260). The European Court of Human Rights seems to be hesitant with regard to the behavioral objectives of privacy law (*Odièvre v France*, ECHR, February 13, 2003). The European Court of Justice, to our knowledge, has not addressed the issue so far.

rewards received in exchange for one's consent to a privacy loss should therefore compensate the costs incurred by experiencing a chilling effect.

Against this backdrop, it is all the more surprising that most arguments brought forward in favor of the right to be forgotten have not elucidated the behavioral implications of control over information storage (see Mayer-Schönberger 2009). Based on rather general arguments, the European Commission has proposed to introduce a right to be forgotten (Rosen 2011; Rosen 2012).[4] Without allowing expungement of information from every cache file on the Internet, the right to have personal information deleted helps to reduce traceability (Lessig 2007; Cohen 2013). One of the unresolved problems is how to design the right to be forgotten. Some lawyers have claimed that chilling effects may best be cushioned in case of automatic deletion (deletion default). They have therefore advocated the use of automated deletion technologies like *X-Pire!* (Backes et al. 2011) or *Vanish* (Geambasu et al. 2009). Tying in with these claims, the European Data Protection Supervisor has proposed that the right to be forgotten shall ensure the automatic deletion of personal information (European Data Protection Supervisor 2011; de Terwangne 2012).[5] The recent Regulation proposal formulated by the European Commission, however, leaves room for two default designs of the right to be forgotten, a retention default and a deletion default. Art. 17 I b) of the EU Data Protection Regulation Draft provides that users shall have a right to be forgotten when they have withdrawn their consent or when the storage period consented to has expired.[6] From a behavioral perspective, the debate about deletion defaults is not only important because people may experience less conformity pressures if they anticipate that stored information will be deleted automatically. If people have to claim deletion actively, they might be afraid that their deletion request could be interpreted as a signal about the sensitivity of stored information. In case of a retention default, status quo bias may thus be bolstered by high rather than low privacy concerns. Automatic deletion is privacy-enhancing in that it does not allow any inferences about the motives of deletion.

## 2.2. Consent Beyond the Bounds of Rationality

While rational choice theorists have posited that individuals engage in consistent and utility-maximizing trade-offs between privacy and other concerns (Stigler 1980; Posner 1981), the emerging field of behavioral economics of privacy has demonstrated that privacy decision making is a domain in which preference uncertainty is particularly strong (Acquisti 2004;

4 In his opinion on the case *Google Spain, S.L., Google Inc. v AEPD, Mario Costeja González*, European Court of Justice, Case C-131/12 [2012], the Advocate-General concluded that the Data Protection Directive "does not provide for a general right to be forgotten in the sense that a data subject is entitled to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests" (June 25, 2013).

5 U.S. law already, yet sectorally, implements an automatic right to be forgotten. The Fair Credit Reporting Act (15 USC §§ 1681c(a)(2)-(5)) provides that information about the involvement in landlord-tenant litigation shall be automatically deleted from credit records after seven years (Strahilevitz 2008).

6 Commission Proposal for a Regulation with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), COM (2012) 11 final (Jan 25, 2012).

John et al. 2011). Privacy preferences are highly malleable and often emerge endogenously as a product of the elicitation methods and the framing used in decision situations. Since the probability of the possible outcomes of a certain type of information usage is generally unknown when consenting to the disclosure of personal information (Acquisti and Grossklags 2005b; Acquisti and Grossklags 2007; Grimmelmann 2009), individuals tend to rely on contextual cues and heuristics to assess the risks associated with disclosure (Hui et al. 2007). Unprofessional-looking websites, for instance, may induce people to disclose more information about socially undesirable behaviors, even though they are associated with higher risks for privacy than professional-looking websites (John et al. 2011). Experimental evidence also suggests that directing people's attention to the level of control over information release may distract their attention from the lack of control over information usage and increase their propensity to disclose sensitive information (Brandimarte et al. 2012).

A generic explanation for these findings is that privacy valuations and thus the propensity to give consent are often influenced by the perceived immediacy of risk, the strategic nature of uncertainty or the intangible nature of privacy harms (e.g., psychological unease). More specifically, these findings indicate that people tend to overestimate the importance of their own actions in comparison to others' privacy intruding actions. Facing rather impalpable privacy risks, people are likely to suffer from optimism bias when making their privacy choices (Jolls 2010). Experimental evidence suggests that people are more inclined to disclose personal information and accept confidentiality losses when having to rate the ethicality of their behavior than when being directly asked whether they have engaged in unethical behavior (John et al. 2011). Further evidence indicates that privacy valuations are lower when information about one's behavior in a public goods game is indirectly (vs. directly) sold to a person endowed with power to sanction antisocial behavior (Rivenbark 2012). Similar reductions of privacy fears can be observed when privacy choices are made in social interactions with strangers instead of acquaintances or friends (stranger phenomenon). People tend to feel more secure when revealing information about their non-conforming social preferences to strangers (Posner 1981; John et al. 2011), i.e., in situations that are not construed as a repeated social interaction. All these findings indicate that people have cognitive difficulties to anticipate potential secondary uses of personal information and imagine how information disclosed in a harmless context may be reused in a less benign fashion in a different context.

# 3. Experimental Design

## 3.1. Methodological Challenges

Most privacy experiments have investigated the willingness to accept money (*WTA*) in exchange for their disclosure of personal information (Chellapa and Sin 2005; Huberman et al. 2006; Wathieu and Friedman 2007), the willingness to pay money (*WTP*) for privacy protection (Acquisti and Grossklags 2005a; Tsai et al. 2011), or the discrepancy between *WTA* and *WTP*, indicating the existence of an endowment effect in privacy (Hui and Png 2006; Acquisti

et al., forthcoming). The common feature of these experiments is that they only investigate the effect of exogenous treatment variations on a single dependent variable, be it the propensity to disclose information (John et al. 2011; Brandimarte et al. 2012) or privacy valuations (Acquisti et al., forthcoming). Since the risk-benefit trade-offs are made relatively to an exogenous variable manipulating the riskiness of information disclosure, the only possibility to adjust to these risks is to disclose less information or increase privacy valuations. By contrast, we investigate the effect of exogenous treatment variations on social norm compliance (using a standard dictator game), privacy valuations, and consent, a design feature that allows for more complex and more realistic trade-offs. This design feature also enables us to test whether people are systematically biased in favor of consent and whether this tendency induces them to forego the benefits resulting from deviant or antisocial behavior.

A closely related problem is that many studies have used incentive-incompatible surveys to elicit privacy valuations of non-verifiable personal information. In surveys, individuals may express privacy preferences that reflect their privacy attitudes, but do not predict their actual privacy choices or the truthfulness of their responses (Kahneman and Ritov 1994; Hui et al. 2007; John et al. 2011; Brandimarte et al. 2012). In settings where the truthfulness of information cannot be verified, the dominant strategy for utility maximizing individuals who value their privacy is to disclose false information (Jentzsch et al. 2012). As recent research shows, privacy trade-offs tend to be made in favor of information disclosure when consent is only slightly incentivized. For example, most individuals seem to prefer data-intensive consumption options for a discount of 1 € over less intrusive consumption options without such a discount (Beresford et al. 2012).

One possible explanation is provided by models of bounded willpower (Loewenstein 1992; Strandburg 2006; Jolls 2010), which indicate that individuals are likely to hyperbolically discount the (often intangible) costs associated with privacy losses, and opt for the immediate gratification associated with consent (Laibson 1997; Acquisti 2004; Acquisti and Grossklags 2004). High discount rates over short-time horizons and low discount rates over long-time horizons may even cause preference reversals (O'Donoghue and Rabin 2001), inducing individuals to give their consent that they might not have given if the time lag between their consent and the dissemination of personal information had been shorter or if the risk of social disapproval had been salient.[7] Finally, even though it is true that privacy choice sets are dichotomous (take-it-or-leave-it) at present (Jentzsch et al. 2012), one of the possible changes in networked technologies may be the creation of bargaining markets where users will be able to assign specific values to their personal information. A sound analysis of privacy valuations should therefore allow for more granular measures. To cope with potential threats to external

7 In December 2012, giving in to a Netflix lobbying campaign, Congress amended the Video Privacy Protection Act (Section 2710(b)(2) 18 USC), relaxing the conditions for consent to the sharing of rental records (e.g., with Facebook). Under the new bill, consent can be given in advance for a period of time, not to exceed 2 years, and does not have to be confirmed each time video rental information is shared. The introduction of in-advance consent opens the door to the exploitation of time-inconsistent preferences. Privacy risks will be discounted more strongly when the time lag between consent and information usage is very long.

validity, we use real and verifiable information, and make the decision context as realistic as possible (a publicly accessible Google website) without giving up control over the experimental setting.

### 3.2. Treatments

Our experiment was designed to investigate whether consent under conditions of uncertain publicity crowds out selfish preferences (conceptualized as deviant preferences), and whether the default design of the right to be forgotten affects privacy valuations and social preferences. It was implemented using a 2x2 factorial design (Table 1) and consisted of three stages. In the first stage, we created a temptation to act selfishly. In the second stage, we offered to pay participants for publishing information about how selfishly they behaved. In the third stage, we gave participants the right to have this information "forgotten". Our experiment involves two types of novel manipulations. On the one hand, we vary the conditions under which participants may give their consent to the publication of personal information. More specifically, we test how the prospect of being subject to networked scrutiny affects social preferences in a standard dictator game (used as a tool for measuring compliance with social norms), the propensity to consent to the publication of information, and privacy valuations. On the other hand, we implement different designs of the right to be forgotten and test whether privacy valuations are affected by default rules of deletion, whether a default of automatic deletion dampens chilling effects, and how sticky the default of non-automatic deletion is. It is important to note that for the chilling effects hypothesis to be tested it is irrelevant whether the deviation from the social norm ought to be qualified as “good” or “bad”.

In the first stage, participants took part in a one-shot standard dictator game (Forsythe et al. 1994; Camerer 2003). At the beginning of this stage, each player was endowed with an initial endowment $e_i$ of 100 tokens. The conversion rate for one token was .09 €. Each player then had to decide how much of her endowment $e_i$ she was willing to share with the recipient. The recipient earned the amount $s_j \in [0,100]$ shared by the dictator. The dictator received the initial endowment minus the amount shared, i.e., $\pi_i = e_i - s_j$ . Economists have used the dictator game to show that the standard economic assumption of money-maximizing behavior is not well founded (Engel 2011) and that behavior in the dictator game cannot only be explained by social preferences, but also by situational properties (List 2007). However, it is also a robust result that most dictators keep higher amounts than they share with recipients. We exploit the latter effect and use the game as a technique to induce behavior that deviates from the fairness norm of equal split. Unlike in other neutrally framed experiments, our instructions explicitly referred to the concept of “sharing” in order to verbally illustrate that the dictators’ decision may indicate the level of compliance with the fairness norm of sharing.

In the second stage, participants could give their consent to the publication of personal information on a publicly accessible Google website. More specifically, participants had to decide whether to agree with the publication of their real name and the amount shared in the role of

dictator. In order to prevent inferences regarding the identity of non-consenting participants, valid consent would entail publication only with a probability $p = .80$. With the complementary probability $1 - p = .20$, valid consent would not be followed by publication. Participants were informed about these probabilities and instructed that payoffs would be cashed-out for any valid consent, irrespective of the (non-)publication of personal information. In addition, we used an incentive-compatible Becker-DeGroot-Marschak (BDM) mechanism to elicit participants' reservation prices for privacy (Becker et al. 1964). Each participant was instructed to state the minimal amount between 0.00 and 9.00 € (in increments of 0.01 €) that she would be willing to accept in exchange for her consent to the publication *(WTA)*.[8] The participant's *WTA* was then compared with a randomly determined bid price *b*, all bid prices *b* being equally probable in the interval [0.00, 9.00]. If the subject's *WTA* was less than or equal the bid price *b*, her consent was considered to be valid and information would be published with probability $p = .80$. In this instance, she received the randomly determined bid price *b*. Given a random bid *b*, her payoff was $b - WTA \geq 0$ if $WTA \leq b$. If $WTA > b$, her consent was considered to be invalid and she obtained 0. Participants who wanted to refuse consent could do so by expressing a $WTA > 9.00$ €. Reporting the truthful *WTA* is the optimal choice (Rivenbark 2012). Before making their decisions in the consent stage, participants were provided with a screenshot of the Google website on which their full name and their decision in the role of dictator would be published in case of valid consent (Fig. 1).[9]

8 We only measure the *WTA*, the reason being that, under European privacy law, personal information may not be processed without consent (cf. Section 2).

9 The website *Kölner Internet-Experimente 2012* can be accessed under the following URL: https://sites.google.com/site/koelnerinternetexperimente2012/. The headline states: "Amounts that participants shared with player B". The paragraph below contains a succinct description of the experiment: "On this website you are being presented the results of an experiment. In the experiment, player A was endowed with 100 tokens. Every token was worth real money which was cashed out to the participants at the end of the experiment. Player A had the opportunity to share any amount of his endowment with player B. The participants listed below have consented to the publication of their name and the amount shared with player B."

**Figure 1. Screenshot of the Google website (in German) with anonymized names of participants**


The first treatment variation consisted in changing the order of the first two stages. In the baseline treatment, participants made their decisions in the dictator game before deciding whether to give their consent (dictator game before consent). Before playing the dictator game, participants knew that another stage would follow without being informed about the specifics. In the chilling effects treatment, participants had to decide about their consent and state their *WTA* before deciding over the split in the dictator game (consent before dictator game). Decisions over the split in the dictator game had thus to be made in light of the decision made in the consent stage. This manipulation permits us to test whether the uncertain prospect of being subject to networked publicity enhances giving in the dictator game and thus generates a chilling effect. It is important to note that participants had to make their decision under a veil of uncertainty in both stages. Only after having made their decisions in both stages were they informed about the (in-)validity of their consent.

The second treatment variation consisted in changing the default of the right to be forgotten. Participants were informed about the default prior to making their choice in the consent stage. The actual deletion was implemented in the third stage outside the lab. In the non-automatic deletion treatment, participants were instructed that they would have the opportunity to have their personal information deleted by addressing an informal deletion request to the administrator of the Google website. They were told that their personal information would remain

public for at least four weeks starting from the date of publication and that they would be able to request deletion via Email afterwards. It was made clear that without actively claiming deletion their information would remain on the Google website for an indeterminate period. In the automatic deletion treatment, participants were informed that the information published on the website would automatically be deleted from the website after a period of four weeks. All participants were informed about the exact date of publication. Finally, we provided all participants with a concise summary of the privacy policy of the Cologne Laboratory of Economic Research and an extract of the Google privacy policy in effect at that time.

To observe the sharing decisions and elicit the privacy valuations of each participant, we implemented the strategy vector method (Selten 1967; Brandts and Charness 2011). Unlike under a sequential decision protocol, participants had to provide a strategy profile for the first two stages prior to being randomly assigned the role of "dictator" or the role of "recipient". More specifically, participants had to make their decisions in the role of "dictator" in both the dictator game stage and the consent stage before the random assignment of roles.

At the end of the experiment, we elicited participants' risk preferences using an incentive-compatible measure of risk aversion to test whether risk preferences might be driving privacy valuations (Holt and Laury 2002). In addition, we conducted a survey measuring participants' privacy attitudes and personality traits, including the Westin Privacy Index (Kumaraguru and Cranor 2005).[10]

**Table 1. Treatments**

| *Variation* | DG before consent | Consent before DG |
|---|---|---|
| Default of non-deletion | *Baseline / Non-automatic* | *Chilling effects / Non-automatic* |
| Default of deletion | *Baseline / Automatic* | *Chilling effects / Automatic* |

## 3.3. Procedure

The experiment was conducted in November 2012 at the Cologne Laboratory of Economic Research at the University of Cologne. We used the experimental software z-Tree (Fischbacher 2007) and invited participants from a subject pool of approximately 4500 individuals using ORSEE (Greiner 2004). Recruited participants were randomly assigned to one of four treatments (between-subjects design). We ran four sessions with a total of $n = 122$ participants[11] (55 male, 67 female). Upon arriving at the lab and before every stage of the experiment, participants received paper instructions that were also read aloud. Each session lasted approximately one and a half hours. To guarantee the confidentiality of our experimental procedure and protect the reputation of the lab, participants could not disclose their names during

10 The instructions and the survey questions used in this article are attached in Appendix B.

11 28 in the baseline/non-automatic treatment, 32 in the baseline/automatic treatment, 30 in the chilling effects/non-automatic treatment, and 32 in the chilling effects/automatic treatment.

the experiment. Instead, they were asked to assign themselves a personal identifier number (PIN) at the beginning of the experiment. After the experiment each participant was individually invited to fetch her payoff. To avoid the feeling of surveillance and social pressure within the lab, during the payment procedure neither participants nor the experimenter monitoring the sessions could learn about the decisions that (other) participants had made. Participants who validly consented had to present their PIN and an ID card in order to obtain their payoff. All participants received a show-up fee of 4.00 €. Across all treatments, participants earned 13.80 € on average. Those who gave their consent (*WTA ≤ 9.00 €*) earned 14.57 € on average,[12] while those who refused their consent (*WTA > 9.00 €*) earned 9.64 € on average.

## 4. Behavioral Predictions

In our experiment, participants have to engage in a trade-off between the benefits from not complying with the fairness norm of sharing in the dictator game and the reputational costs associated with their consent. More precisely, we assume that people experience disutility from inequitable outcomes and that people experience disutility from being publicly perceived as favoring inequitable outcomes. Building on the standard model of inequality aversion proposed by Fehr and Schmidt (1999) and only including the utility losses from advantageous inequality, under the veil of privacy dictators should maximize their utility according to a function

$$U(\pi_{ip}) = \pi_i - \beta_{ip} \max\{\pi_i - s_j, 0\}, \qquad i \neq j, \tag{1}$$

where $\pi_i$ captures the dictators' monetary payoff, $s_j$ denotes the recipients' payoff, and $\beta_{ip}$ measures the disutility from advantageous inequality ($\pi_i > s_j$) under the veil of privacy. The value of $\beta$ determines whether dictators opt for the egalitarian or the selfish solution. We assume that dictators will behave less selfishly in case of consent than if they decide under a veil of privacy, i.e., $\beta_{ic} \geq \beta_{ip}$, and that dictators giving their consent will require compensation for their loss of privacy. Building on these assumptions, we extend the model to predict amounts shared and privacy valuations in case of consent. Given that $\pi_i = e_i - s_j$, dictators' utility is captured by

$$U(\pi_i) = \begin{cases} e_i - s_j - \beta_{ip} \max\{e_i - 2s_j, 0\} & if\ privacy \\ e_i - s_j - \beta_{ic} \max\{e_i - 2s_j, 0\} + c & if\ consent, \end{cases} \tag{2}$$

where $c$ denotes the compensation for consenting (participants' $WTA$).[13] If $\beta_i > 0.5$, the model predicts that dictators will share $s_j = \frac{1}{2}e$. If $\beta_i < 0.5$, dictators should share $s_j = 0$

12 This includes participants whose *WTA* was smaller (valid consent) and larger (invalid consent) than the random bid price *b*.

13 An equivalent model explicitly capturing reputation is:
$U(\pi_{ic}) = e_i - s_j - \gamma_{ic} \max\{e_i - 2s_j, 0\} - \delta_{ic} \max\{e_i - 2s_j, 0\} + c$, where the $\delta$-term captures the disutility from having one's choices in the dictator game published. The model is equivalent, since

(Fehr and Schmidt 1999). Theoretically, we should thus only observe egalitarian (conforming) or selfish (non-conforming) choices. Building on the two corner solutions, we predict that consenting participants will ask for a compensation $c \geq 0$ if ($\beta_{ic} \geq \frac{1}{2}, \beta_{ip} \geq \frac{1}{2}$) or ($\beta_{ic} \leq \frac{1}{2}, \beta_{ip} \leq \frac{1}{2}$). In these cases, dictators' inequality aversion does not strongly vary with the degree of privacy under which their normative or social preferences are elicited. Privacy-insensitive dictators will therefore always choose either the egalitarian or the selfish option irrespective of their consent. Being indifferent with respect to their reputation, they should express relatively low privacy valuations. The more interesting case occurs if dictators are sensitive to privacy losses, i.e., if ($\beta_{ic} \geq \frac{1}{2}, \beta_{ip} \leq \frac{1}{2}$). In this case, dictators should ask for $c \geq \frac{1}{2} e_i$, which should entirely compensate for the loss incurred by making the egalitarian choice.[14] In stylized fashion, this simple model shows that dictators' $WTA$ can be thought of as a compensation for an experienced chilling effect (the cost that they have incurred to avoid a loss of reputation or a loss from social sanction). Even under these assumptions, however, the chilling effects treatment should not lead to differences in the amounts shared in the dictator game. Dictators should know their degree of inequality aversion, anticipate their behavior in the dictator game accordingly, and base their $WTA$ on this expectation.

However, as recent privacy studies suggest, contextual cues signaling that personal information may be published can lead to a significant increase in privacy concerns (Acquisti et al., forthcoming; John et al. 2011). Building on these findings, we assume that simply giving participants a previous consent option and nudging their attention towards potential publicity is sufficient to reduce social distance. While a related strand of economic experiments illustrates that double-blind protocols lead to a significant increase of self-regarding behavior (Hoffman et al. 1994; Hoffman et al. 1996; Levitt and List 2007), reducing social distance by giving recipients the opportunity to visually identify dictators (Bohnet and Frey 1999), by showing a pair of eyes (Haley and Fessler 2005), or by learning the names of the respective counterparts (Charness and Gneezy 2008) can significantly enhance other-regarding behavior in the dictator game. In the chilling effects treatment, we thus expect dictators to have a stronger feeling of uncertainty about publicity. This should activate their disposition to comply with the social norm of sharing. The social norm for sharing in the dictator game is assumed to be an equal split of the endowment for the very reason that it is customary (Levitt and List 2007; Young 2008; Andreoni and Bernheim 2009) and most "norm-compliant" (Krupka and Weber 2013).[15] In addition, we expect the chilling effect to be particularly strong for consenting individuals, since they are not only aware of the consent option but also make use of this option. Against this backdrop, we posit:

---

$-\gamma_{ic} \max\{e_i - 2s_j, 0\} - \delta_{ic} \max\{e_i - 2s_j, 0\} = -(\gamma_{ic} + \delta_{ic}) \max\{e_i - 2s_j, 0\} = -\beta_{ic} \max\{e_i - 2s_j, 0\}$, where $\beta_{ic} \equiv \gamma_{ic} + \delta_{ic}$.

14 In the unlikely case of ($\beta_{ic} \leq \frac{1}{2}, \beta_{ip} \geq \frac{1}{2}$), participants should even have a willingness to pay for giving up their privacy, i.e., $c \geq -\frac{1}{2} e_i$. A proof of all possible solutions is included in Appendix A.

15 Whether the 50-50 norm bears upon what one ought to do (injunctive norm) or whether it refers to a regularity of actions (descriptive norm; Bicchieri 2006), is irrelevant with respect to the chilling effects hypothesis, because deviations from both norm types can be seen as the product of unconstrained choice.

*Hypothesis 1:* Dictators share higher amounts (closer to the norm of equal split) when consenting before the dictator game (chilling effects treatment) than when consenting afterwards (baseline treatment).[16]

With respect to the intertwining of privacy valuations and behavior in the dictator game, we build on earlier findings showing that "undesirable traits" lead to an increase of the reservation price for personal information (Huberman et al. 2005). A closely related argument posits that the concealment of personal information may be regarded as a form of costly insurance against the consequences of social misconduct (Posner 1978; Posner 1981). Since individuals deviating from the 50-50 norm in the dictator game may be perceived as antisocial or defectors, they will refuse consent if the expected reputational costs associated with networked publicity exceed the payoff from the satisfaction of their normative or social preferences under the veil of privacy. Participants' *WTA* or refusal of consent should reflect their inclination to deviate from the norm of sharing. Hence we propose:

*Hypothesis 2a:* Amounts shared in the dictator game and participants' *WTA* are negatively correlated.

*Hypothesis 2b:* Non-consenting individuals will share or have shared lower amounts in the dictator game than consenting individuals.

As regards the default rule of deletion, we consider it to be a tool enhancing control over the *lifetime* of information. An increase of perceived control over the *release* of personal information has been shown to mitigate the effect of reactance and enhance the propensity to disclose personal information (Tucker 2011; Brandimarte et al. 2012). This finding confirms earlier studies showing that perceived control is positively correlated with risky behavior (Slovic 2000). Since automatic deletion should reduce the perceived risk of being detected as a norm violator, we hypothesize:

*Hypothesis 3a:* In the baseline treatment, automatic deletion reduces privacy valuations.

*Hypothesis 3b:* In the chilling effects treatment, automatic deletion either facilitates self-regarding behavior, thereby increasing privacy valuations, or reduces privacy valuations, thereby pressurizing individuals to engage in other-regarding behavior.

Additionally, we test for personality factors which should allow us to disentangle between unfair types and privacy unconcerned individuals. We also predict that individuals with strong control claims and high privacy concerns should have higher privacy valuations than individuals who, according to their own statements, are not concerned about a lack of control or privacy. Finally, we hypothesize that a large fraction of participants will suffer from status quo bias (Samuelson and Zeckhauser 1988; Kahneman et al. 1991; Johnson et al. 2002) and will not claim deletion in the non-automatic deletion treatment.

16 More concretely, in the chilling effects treatment, the average amount shared should be closer to 28.35 % while the mode should shift from 0 to .5.

# 5. Results

## 5.1. Effects of a Privacy Loss

### *5.1.1. Chilling Effects*

We first examined the impact of the chilling effects treatment (vs. the baseline treatment) on participants' decisions in the dictator game. A Wilcoxon-Mann-Whitney test revealed that participants shared slightly larger amounts in the chilling effects treatment (consent before dictator game; $n = 62$, $M = 25.48$, SD = 19.21) than in the baseline condition (dictator game before consent; $n = 60$, $M = 19.61$, SD = 20.98, $z = 1.74$, $p = .08$).[17] Moreover, a two-part regression model[18] showed that almost twice as many participants ($n = 24$, 38.7 %) shared nothing of their endowment in the baseline condition as compared to the chilling effects treatment ($n = 13$, 21.7 %) (Table 2, column 1). However, the chilling effects treatment did not have a significant impact on the amounts shared in the dictator game once participants who kept the entire endowment for themselves are excluded (Table 2, column 2). The chilling effect therefore seems to be driven mainly by the different proportions of participants reluctant to share anything. The difference in participants' behavior in the dictator game is also visible in Fig. 2, which shows the distributions of amounts shared in the baseline and the chilling effects treatment. An Epps-Singleton test for equality of variances was not significant ($p = .13$). This suggests that the chilling effect does not reduce the scope of different behaviors.

*Result 1:* The fraction of individuals sharing some portion of their endowment is higher when they are previously given an option to consent to the disclosure of their information.

**Table 2. Regression results (columns 1-4)**

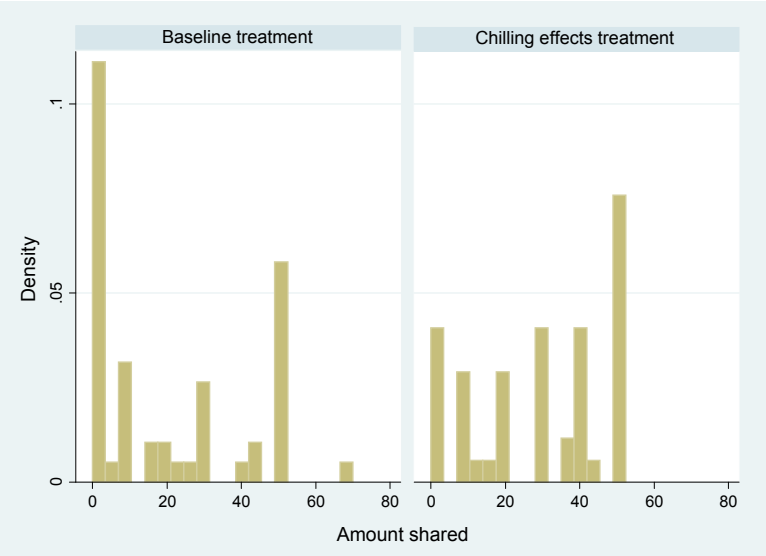
| | (1) Give something (yes = 1 / no = 0) | (2) Amount shared | (3) Give something (yes = 1 / no = 0) | (4) Amount shared |
|---|---|---|---|---|
| Chilling effect | 0.826* | 0.650 | -1.070 | -4.168 |
| (1 = consent before DG) | (2.02) | (0.15) | (-1.11) | (-0.29) |
| Consent | | | -0.059 | 7.991 |
| (1 = gave consent) | | | (-0.08) | (0.80) |
| Chilling effect x Consent | | | 2.588* | 4.800 |
| | | | (2.37) | (0.32) |
| Constant | 0.460+ | 30.10** | 0.511 | 23.22* |
| | (1.76) | (8.89) | (0.70) | (2.44) |
| Sigma Constant | | 18.09** | | 17.85** |
| | | (9.74) | | (9.82) |
| N | 122 | 85 | 122 | 85 |

**Note.** + $p < 0.10$, * $p < 0.05$, ** $p < 0.01$. *t*- and *z*-values in parentheses. Columns 2 and 4 report the results of a truncated regression which excludes participants who kept the entire endowment for themselves.

17 All the results presented in this section are those of a two-sided Wilcoxon-Mann-Whitney test, unless reported otherwise.

18 First part: logistic regression to predict a dummy variable for giving in the dictator game. Second part: truncated regression to predict giving after excluding those who kept the entire amount for themselves.

**Figure 2. Distribution of amounts shared in the baseline and chilling effects treatment (Note. Only participants who gave their consent are included in the figure.)**




We further analyzed the treatment effects for participants who consented (vs. did not consent). Out of 122 participants, only 19 (15.6 %) had a valuation of privacy that exceeded 9.00 € and, thus, did not give their consent.[19] As expected, those who refused consent shared lower amounts ($M$ = 12, SD = 17.82) than those who gave their consent ($M$ = 24.44, SD = 20.17, $z$ = 2.48, $p$ = .01). In line with the chilling effects hypothesis, consenting participants shared lower amounts in the baseline treatment ($M$ = 20.06, SD = 21.22) than in the chilling effects treatment ($M$ = 29.27, SD = 17.93, $z$ = 2.46, $p$ = .01). Conversely, participants who refused consent did not share significantly different amounts across treatments ($z$ = 1.16, $p$ = .25). A two-part regression model that first tests for the propensity to give anything in the dictator game and in a second step tests participants who gave something corroborated this result. The significant interaction between the chilling effects treatment and consent (yes/no) demonstrates that the correlation between consent and the amount shared was stronger in the chilling effects treatment (Table 2, column 3). After controlling for participants who kept the entire endowment for themselves, the amounts were not significantly different by conditions (Table 2, column 4). In line with these results, a two-sample Kolmogorov-Smirnov test rejects the equality of distributions for participants who consented ($p$ = .043, *exact* = .033). This provides further evidence for a chilling effect resulting from the uncertain prospect of being exposed to networked publicity.

*Result 2:* Consenting individuals share higher amounts than non-consenting individuals.

19 Out of the 19 participants who did not consent, 8 refused consent in the baseline treatment, while 11 refused consent in the chilling effects treatment.

### 5.1.2. What Does Consent Really Reveal?

In the baseline treatment, the propensity to consent did not hinge on participants' previous behavior in the dictator game. Participants who refused consent did not share significantly less ($M$ = 16.63) than participants who gave their consent ($M$ = 20.06, $z$ = .26, $p$ = .79). A logistic regression with amount shared as a predictor of consent revealed similar results ($b$ = .008, $z$ = .43, $p$ = .67). This suggests that by giving their consent, individuals do not signal that they have complied with social norms *in the past*. In the chilling effects treatment, however, participants shared significantly higher amounts in the dictator game if they had previously given their consent ($M$ = 29.27) than if they had refused consent ($M$ = 8.64, $z$ = 3.25, $p$ = .001). This result was supported by a logistic regression analysis of consent predicted by amount shared ($b$ = .073, $z$ = 2.79, $p$ = .005). Against this backdrop, consent may be interpreted as a signal of social norm compliance *in the future*. This is a surprising result, given that the reputational costs associated with consent should not depend on the ordering of the dictator game and the consent stages. One possible explanation is that participants in the baseline treatment anticipated that the average amount shared in the dictator game would be rather low. They might have realized that consent would not allow sound inferences about their cooperativeness and that reputational costs would be relatively low. Conversely, consenting participants in the chilling effects treatment might have anticipated that other consenting participants would want to signal a good reputation by sharing relatively large amounts.

*Result 3:* Consenting individuals only share higher amounts than non-consenting individuals when facing the uncertain prospect of networked publicity before the dictator game.

### 5.1.3. Privacy Valuations

We next examined the impact of the chilling effects treatment on participants' privacy valuations. Participants did not differ statistically in their mean privacy valuations ($M$ = 4.90, SD = 3.27 in the chilling effects treatment; and $M$ = 4.28, SD = 3.02 in the baseline treatment, $z$ = 1.00, $p$ = .32). Furthermore, we did not find any evidence for a bimodal distribution of privacy valuations. An Epps-Singleton test showed that distributions were not significantly different ($p$ = .19). We also examined whether privacy valuations could be predicted by the amount shared in the dictator game. Results of a linear regression analysis are presented in Table 3 (columns 5 and 6) and show that, as expected, lower amounts shared predicted higher privacy valuations. This did not depend on whether participants were in the baseline or chilling effects condition, as a non-significant interaction shows. These results indicate that privacy is not just a value *per se*, but an instrumental good that individuals use to satisfy their normative preferences. The reservation price of this good seems to be determined by the degree to which an individual wishes to deviate from a social norm.

**Table 3. Regression results (columns 5-9)**

| | (5) Privacy valuation | (6) Privacy valuation | (7) Give something (yes = 1 / no = 0) | (8) Privacy valuation | (9) Used the right to be forgotten |
|---|---|---|---|---|---|
| Privacy valuation | | | | | -0.067 (-0.36) |
| Chilling effect (1 = consent before DG) | | 1.121 (1.31) | | | |
| Amount shared x Chilling effect | | -0.012 (-0.44) | | | |
| Automatic deletion (1 = automatic) | | | -0.693 (-0.73) | -0.220 (-0.38) | |
| Consent (1 = gave consent) | | | 0.888 (1.28) | | |
| Automatic deletion x Chilling effect | | | 0.628 (0.60) | | |
| Amount shared | -0.034* (-2.43) | -0.031+ (-1.65) | | | -0.002 (-0.06) |
| Amount shared x Privacy valuation | | | | | 0.008 (0.82) |
| Constant | 5.34** (12.76) | 4.89** (9.09) | 0.182 (0.30) | 4.699** (11.32) | 0.236 (0.19) |
| *N* | 122 | 122 | 122 | 122 | 26 |

**Note.** + $p < 0.10$, * $p < 0.05$, ** $p < 0.01$. *t*- and *z*-values in parentheses.

## 5.2. Effects of the Right to Be Forgotten

### *5.2.1. Chilling Effects and Privacy Valuations*

Our experiment was also designed to examine whether automatic deletion has an effect on privacy valuations and decisions in the dictator game. Results revealed no differences in the amount shared by the participants in the automatic deletion and the non-automatic deletion condition ($z = .53$, $p = .59$). In line with this result, a logistic regression did not reveal any significant effects on participants' propensity to share anything in the dictator game based on automatic vs. non-automatic deletion (Table 3, column 7). Moreover, participants did not differ in their privacy valuations ($M = 4.70$, SD = 3.27 in the non-automatic deletion treatment; and $M = 4.48$, SD = 3.06 in the automatic deletion treatment, $z = .31$, $p = .76$) (see also Table 3, column 8). Thus, it seems that the manipulation of the deletion modality influenced neither participants' privacy valuations nor their behavior in the dictator game.

### 5.2.2. Stickiness of the Retention Default

Out of 26 participants whose information was made public in the non-automatic deletion treatment, only 6 requested the deletion of their information published on the Google website (23.08 %). A logistic regression analysis of these participants did not reveal any significant effect (Table 3, column 9), which could be due to low statistical power and reduced cell sizes. Even though we cannot make any inferential claim with respect to the reasons for this stickiness, this descriptively suggests that users may only actively request deletion if they sense reputational harm.

*Result 4:* Only about 25 % of participants actively claim deletion.

## 5.3. Behavioral Implications of Experience, Privacy Attitudes, and Privacy Types

In the following section, we present additional analyses intended to highlight the factors that influence privacy valuations and participants' behavior in the dictator game. Here we investigate possible effects of experience with privacy issues in cyberspace and the coherence between privacy attitudes, risk preferences, and behavior in our experiment.[20]

### 5.3.1. Effects of Experience

The experience of regret does not seem to have any impact on privacy valuations. Participants who state to have experienced regret after posting personal information in networked publics do not have higher privacy valuations ($M$ = 4.59) than participants who have never experienced regret ($M$ = 4.58, $z$ = .008, $p$ = .99). In a similar vein, bad experiences resulting from the publication of personal information do not entail higher privacy valuations. Participants who stated to have made bad experiences do not have significantly higher privacy valuations ($M$ = 4.87) than participants who never made bad experiences ($M$ = 4.52, $z$ = .44, $p$ = .66). However, the 51 participants who reported having previously requested deletion of their information on public websites had significantly higher privacy valuations ($M$ = 5.46) than the 71 participants who had never requested deletion ($M$ = 3.96, $z$ = 2.45, $p$ = .01).[21] Finally, while participants who had read the privacy policy of their preferred social network expressed significantly higher privacy valuations ($M$ = 5.35) than those who had not done so ($M$ = 4.02, $z$ = 2.48, $p$ = .01), they were not less inclined to give their consent ($z$ = 1.46, $p$ = .14). One possible explanation for these results is that people do not learn from bad experiences. An alternative explanation might be that the privacy implications of our experiment were not perceived as strong enough by participants who had made bad experiences.

20 The survey questions used for the additional analyses are attached in Appendix B.

21 While this result does not allow for any causal inference, it indicates that privacy valuations are positively correlated with the exercise of control over personal information. A learning effect resulting from unsuccessful deletion requests cannot be shown due to the very small number of observations; out of the 51 participants having requested deletion only 5 stated that they were unsuccessful.

### 5.3.2. Privacy Attitudes and Privacy Valuations

Our results suggest that participants' privacy attitudes are not reflected in their privacy choices, but in their degree of sharing in the dictator game. A linear regression shows that specific concerns about how much information is publicly available in the Internet do not predict participants' privacy valuations ($b = -.11$, $t(121) = -.59$, $p = .55$).[22] Similarly, specific concerns about the way in which personal information is used by social networks generally can predict neither consent ($b = .36$, $z = 1.40$, $p = .16$)[23] nor privacy valuations ($b = -.38$, $t(121) = -1.40$, $p = .16$). Moreover, worries about who can access personal information in social networks and how personal information may be used are not reflected in privacy valuations ($b = .03$, $t(121) = .16$, $p = .87$). However, our results revealed that privacy valuations were predicted by how important control of information was for participants ($b = -1.92$, $t(121) = -3.40$, $p = .001$). More specifically, privacy valuations were significantly higher for those who expressed greater need to control information. Surprisingly, neither risk aversion ($b = -.07$, $t(121) = -0.53$, $p = .60$) nor income ($b = .001$, $t(121) = 1.51$, $p = .13$) predicted participants' privacy valuations. Further regression analyses revealed that women valued private information slightly lower than men ($b = -.96$, $t(121) = -1.69$, $p = .09$) and that women shared slightly higher amounts in the dictator game ($b = 6.11$, $t(121) = 1.67$, $p = .09$).

### 5.3.3. Privacy Types and Norm Compliance

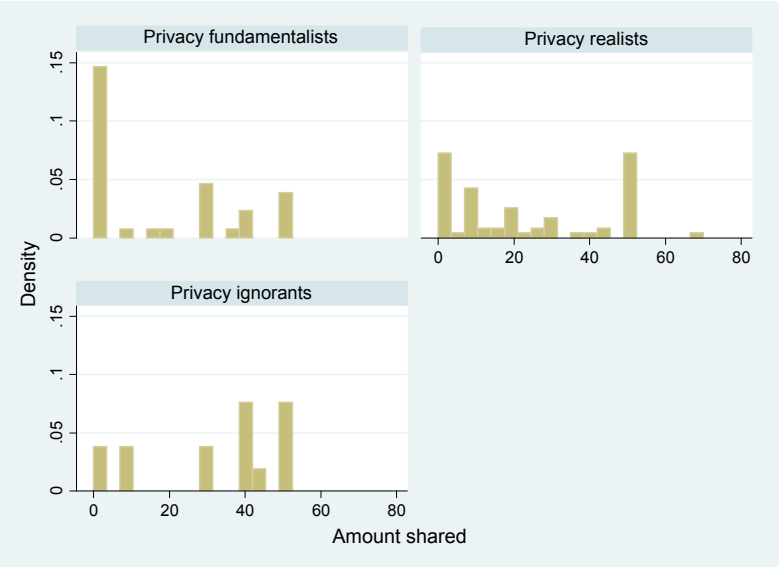
Our analysis confirms that individuals consider some privacy parameters to be instrumental for escaping normative pressure. A regression analysis shows that the less individuals use differential privacy settings for different types of friends in social networks, the more they give in the dictator game ($b = 2.16$, $t(121) = 2.44$, $p = .016$). Even more surprisingly, our results suggest that different privacy types categorized on the basis of a variant of the Westin Privacy Index do not differ on the dimension of privacy valuations but on the dimension of decisions in the dictator game (Fig. 3).[24] A regression analysis showed that privacy fundamentalists shared lower amounts in the dictator game ($M = 17.1$, SD = 19.62) than privacy realists ($M = 23.24$, SD = 20.45) and privacy ignorants ($M = 32.4$, SD = 18.44, $b = 15.32$, $t(121) = 2.51$, $p = .014$). Conversely, no differences emerged for privacy valuations ($ps > .358$). These results allow us to conclude that privacy preferences are strongly correlated with social preferences.

22 All regressions used in this section are OLS regressions if not reported otherwise.

23 These are the results of a logistic regression.

24 Our categorization is based on the *Privacy Segmentation Index* (Kumaraguru and Cranor 2005). The privacy fundamentalists and the privacy unconcerned were coded in accordance with the original Privacy Segmentation Index. Since we gave participants the opportunity to not know the response to the questions of the Privacy Segmentation Index, the privacy pragmatists were subdivided in "privacy realists" (who differ from the first two categories, but state that they do not know the response only once) and "privacy ignorants" (who differ from the first two categories, but state that they do not know the response more than once). In our experiment, 30.33 % are privacy fundamentalists, 54.92 % are "privacy realists", 12.30 % are "privacy ignorants", and 2.46 % are privacy unconcerned.

**Figure 3. Amounts shared in the dictator game by privacy type (Note. The privacy unconcerned are not included in the figure because of the small number of observations.)**




*Result 5:* Control claims are reflected in the valuation of privacy per se, while privacy claims reflect the strength of normative preferences.

# 6. Discussion

## 6.1. Interpretation

In our experiment, we tested whether the chilling effects hypothesis also holds when individuals autonomously consent to the publication of personal information, how the design of the right to be forgotten affects privacy valuations or social norm compliance, and whether privacy valuations reflect individuals' inclination to deviate from social norms.

### *6.1.1. Reducing Chilling Effects by Framing Consent Options*

Our main finding is that the prospect of networked publicity does not affect individuals' privacy valuations, but significantly increases their propensity to engage in costly compliance with social norms. Even when facing cues signaling the risk of having personal information published, individuals voluntarily trade personal information for conformity, which indicates that their valuation of the benefits from consent exceeds their benefits from satisfying their normative or social preferences. This is an interesting finding, given that the chilling effects argument is generally only upheld if (1) individuals have no choice whether to disclose personal information and (2) information is processed by a governmental entity. Should the law therefore prevent people from behaving *normally* or nudge them away from self-exposing to a normalizing gaze? This will ultimately depend on the strength of chilling effects and whether the suppressed behaviors are deemed to be socially beneficial or contribute to well-being. In our experiment, networked publicity does not seem to dampen behavioral idiosyncrasies and

reduce the panoply of different behaviors. It simply reduces the frequency of non-conforming or selfish behaviors.

Against this backdrop, we may conclude that the dystopian pictures of a uniform society, which constitutional and privacy scholars tend to draw, might overstate the social problem at stake. It is quite likely that publicity in small web communities where normative expectations are commonly shared by community members due to selection effects will not generate any chilling effect. However, we cannot rule out that self-exposure could entail the complete suppression of behaviors in other contexts or when norm compliance hinges on a binary choice ("do it or don't do it"). More importantly, our chilling effects treatment shows that privacy choices are strongly influenced by non-normative factors, such as the timing of a consent option. Revealed privacy preferences might thus not always reflect people's true preferences for privacy (Acquisti et al., forthcoming). If social norm compliance, in turn, is a function of people's privacy choices, we may, in a second step, conclude that observed compliance with social norms might not always reflect people's true preferences for social norm compliance either. Consent to the disclosure of personal information may thus induce people to comply with a social norm, which they would not have complied with if the consent option had been framed differently.

### *6.1.2. Unsticking from Retention*

As regards the right to be forgotten, our results suggest that the default of non-automatic deletion does not significantly affect privacy valuations. Similarly, our data do not support the claim that the prospect of being remembered forever may enhance chilling effects (Mayer-Schönberger 2009). This should not discharge lawmakers of their responsibility to ponder the behavioral implications of the right to be forgotten. As our results suggest, only about 25 % of individuals use their right to be forgotten when there is no threat of immediate harm. This is a surprising result, given that the opportunity costs of requesting deletion via Email are quite low. One possible explanation is that the disadvantages of leaving the retention regime loom larger than the advantages of inertia (see Kahneman et al. 1991). Participants might have feared that by sending an Email they would have to share even more personal information or that a deletion request may signal that they are inconsistent with their previous choice. Some people might have interpreted the default as indicating the recommended course of action (McKenzie et al. 2006). Others might have feared that a deletion request might draw unwanted attention to their personal information (Streisand effect). An alternative explanation is that participants might simply have forgotten their right to be forgotten. If the right to be forgotten is to foster *precaution*, non-automatic deletion is likely to be ineffective in many contexts, since most users will use it after their reputation has been harmed (*Google Spain, S.L., Google Inc. v AEPD, Mario Costeja González*, European Court of Justice, Case C-131/12 [2012]). One way of counterbalancing the risks associated with users' forgetfulness might be to remind them of their right to be forgotten after the storage period has expired. Our experiment also

calls for a further test of whether the willingness to accept for waiving the right to be forgotten exceeds the willingness to pay for acquiring it.

### *6.1.3. Valuing Privacy Without Wanting to Pay for It?*

Finally, our results indicate that a much more careful approach to the oft-cited privacy paradox (Acquisti and Grossklags 2005a; Berendt et al. 2005; Strandburg 2006) is needed. Many scholars have conceived the discrepancy between high privacy concerns and low privacy valuations as a paradox. The problem of this so-called paradox is that it fails to explain why stated privacy preferences or concerns should influence privacy valuations and information revelation rather than any other type of behavior. While privacy concerns do not necessarily concur with a high willingness to pay, they are reflected in behaviors that can be qualified as deviant from existing social norms. This proposition is confirmed by our finding that strong cues signaling the possibility of being exposed to networked publicity did not affect the distribution of privacy valuations. Interpreting this result in light of our main effect, we can conclude that cuing publicity is likely to enhance conformity instead of privacy valuations. On the one hand, this indicates that the privacy paradox may not exist. On the other hand, regulators should be aware that nudging users towards the risk of having personal information published might generate counterproductive effects: Instead of reducing people's propensity to consent, such nudges may induce people to engage in conforming behavior without any effect on consent.

### *6.1.4. Tearing the Veil of Privacy by Not Tearing It?*

Even though we did not find significant differences in privacy valuations across treatments, we cannot conclude that people are generally unable or unwilling to value their privacy. Privacy valuations can be considered a function of an individual's normative preferences: The less an individual has behaved or will behave in a non-conforming or selfish manner, the higher her privacy valuation. Surprisingly, privacy valuations that exceed the upper threshold and reflect a refusal of consent do not signal that individuals have behaved unfairly in the past. However, a refusal to consent before having to decide about compliance with a social norm is generally followed by strong deviations. This is an important finding, which indicates (1) that consent is only a signal of future conformity and (2) may generate unraveling effects with respect to future behavior (Peppet 2011). It suggests that the risk of inferences about personal traits not only results from the aggregation of "Big Data". In situations where people are offered monetary rewards for the disclosure of a single piece of information, a refusal to give consent (and disclose information about one's type) may be just as revealing as consent (Baird et al. 1994). The risk of an unraveling result should be a challenge to privacy and constitutional scholars who tend to claim that privacy protection hinges on the self-controlled concealment of personal information (Bull 2011).

## 6.2. Caveats

Even though we contextualized our experiment to a certain degree, users do not always disclose personal information about a specific type of social behavior in networked publics. Which information users disclose depends on various contextual factors (John et al. 2011). More generally, users are subject to a much richer decision-making environment than in our setting. A possible response to this critique is that interpersonal comparisons are only possible if the choice set is restricted to a specific type of information. Furthermore, a rich context may have added unexplained noise and hampered generalizability. A second critique may be that, in our setting, networked publicity is a function of an endogenous choice, making causal inferences about the factors driving social norm compliance more difficult. Individuals may have self-selected into networked publicity *because* of their stronger inclination to comply with social norms. However, since privacy valuations do not differ across treatments, our results allow us to conclude that the inclination to conform is stronger when individuals have previously bound themselves by their consent. This suggests that individuals are likely to tolerate higher costs on their liberty when facing the prospect of publicity, either because they overvalue the reputational cost associated with publicity or because they undervalue their privacy. Finally, we cannot rule out differences in mental accounting processes between the baseline and the chilling effects treatment. It may well be that the trade-off between the benefits from the dictator game and the benefits from consent is more difficult to operate in the chilling effects treatment because participants have to anticipate their decision in the dictator game. A possible objection to this critique is that privacy choices usually do not only require sequential thinking. Almost all privacy-relevant decision situations also require thinking about future choices conditional on disclosing personal information, and thus involve mental accounting (Brandimarte et al. 2012).

## 6.3. Conclusion

Publicity indeed is an "insufficiently appreciated problem for the modern era" (Sunstein 2009), precisely because we have lost track of the behavioral consequences related with voluntary disclosure of personal information. Even if consent is agnostic about substance, it should not be agnostic about consequence. Many of the choices that individuals make once they have consented to the disclosure of personal information are driven by rational fears. Privacy law, however, has not responded to these rational fears. One reason is that fear-related theories of freedom (see Goodin and Jackson 2007) do not tell us how to deal with behavioral impediments resulting from fears which people have deliberately exposed themselves to. However, privacy and constitutional scholarship should be aware of the fundamental paradox resulting from the autonomous decision to disclose personal information in networked publics: By the same token that an individual autonomously decides to give her consent under conditions of uncertain publicity, she is likely to self-inflict a chilling effect on her own liberty. This constraint may be interpreted as a self-imposed cost or internality (Loewenstein and Haisley 2008). Conversely, any legal intervention and any nudge towards or away from con-

sent will alter the conditions and intensity of the chilling effects. Arguments based on the implicit claim that freedom of choice equals autonomy should thus raise doubt as to their consistency with the behavioral impediments that "free choice" may entail. Regulators of consent architectures should not dismiss the normative claim that societies need an adequate portion of dissent (Sunstein 2003) and discomfort to flourish. There is a risk that increasing the monetary benefits resulting from consent will change the very structure of the trade-off between the immediate benefit of consent (with the cost to future liberty) and the future benefit of liberty (with the foregone benefits of consent).

## References


Acquisti, Alessandro, Leslie John, and George Loewenstein. Forthcoming. What Is Privacy Worth? *Journal of Legal Studies*.

Acquisti, Alessandro, and Jens Grossklags. 2005a. Privacy and Rationality in Decision Making. *IEEE Security & Privacy* 3: 26-33.

Acquisti, Alessandro, and Jens Grossklags. 2005b. Uncertainty, Ambiguity and Privacy. Working Paper. Submitted to the 4th Annual Workshop on Economics and Information Security (WEIS 2005). Carnegie Mellon University, Pittsburgh, PA.

Acquisti, Alessandro. 2004. Privacy in Electronic Commerce and the Economics of Immediate Gratification. Working Paper. Carnegie Mellon University, Pittsburgh, PA.

Acquisti, Alessandro, and Jens Grossklags. 2004. Privacy Attitudes and Privacy Behavior. Losses, Gains, and Hyperbolic Discounting. Pp. 179-186 in *The Economics of Information Security*, edited by L. Jean Camp and Stephen Lewis. New York, NY: Springer.

Andreoni, James, and B. Douglas Bernheim. 2009. Social Image and the 50-50 Norm: ATheoreticalandExperimentalAnalysisofAudienceEffects. *Econometrica* 77: 160 7- 1636.

Backes, Julian, Michael Backes, Markus, Dürmuth, Sebastian Gerling, and Stefan Lorenz. 2011. X-Pire! – A digital expiration date for images in social networks. Working Paper. Universität des Saarlandes, Saarbrücken, Germany.

Baird, Douglas G., Robert H. Gertner, and Randall C. Picker. 1994. *Game Theory and the Law*. Cambridge, MA: Harvard University Press.

Bannon, Liam J. 2006. Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing. *CoDesign* 2: 3-15.

Becker, Gordon M., Morris H. DeGroot, and Jacob Marschak. 1964. Measuring utility by a single-response sequential method. *Behavioral Science* 9: 226-232.

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. 2005. Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. *Communications of the ACM* 48: 101-106.

Beresford, Alastair R., Dorothea Kübler, and Sören Preibusch. 2012. Unwillingness to pay for privacy: A field experiment. *Economics Letters* 117: 25-27.

Bernheim, B. Douglas. 1994. A Theory of Conformity. *Journal of Political Economy* 102: 841-877.

Bicchieri, Cristina. 2006. *The Grammar of Society: The Nature and Dynamics of Social Norms*. Cambridge: Cambridge University Press.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. 2012. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, in press.

Brandts, Jordi, and Gary Charness. 2011. The strategy versus the direct-response method: a first survey of experimental comparisons. *Experimental Economics* 14: 375-398.

Britz, Gabriele. 2010. Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts. Pp. 561-596 in *Offene Rechtswissenschaft*, edited by Wolfgang Hoffmann-Riem. Tübingen: Mohr Siebeck.

Bull, Hans Peter. 2011. *Informationelle Selbstbestimmung – Vision oder Illusion?* 2nd ed. Tübingen: Mohr Siebeck.

Camerer, Colin F. 2003. *Behavioral Game Theory: Experiments in Strategic Interaction*. Princeton, NJ: Princeton University Press.

Charness, Gary, and Uri Gneezy. 2008. What's in a Name? Anonymity and Social Distance inDictator and Ultimatum Games. *Journal of Economic Behavior & Organization* 68: 29-35.

Chellapa, Ramnath K., and Raymond G. Sin. 2005. Personalization Versus Privacy: An Empirical Examination of the Online Consumers' Dilemma. *Information Technology and Management* 6: 181-202.

Cohen, Julie E. 2012. *Configuring the Networked Self*. New Haven, CT: Yale University Press.

Cohen, Julie E. 2013. What Privacy Is For. *Harvard Law Review* 126: 1904-1933.

Ellickson, Robert C., 1991. *Order without Law. How Neighbors Settle Disputes*. Cambridge, MA: Harvard University Press.

Elster, Jon. 1989. *The Cement of Society*. Cambridge: Cambridge University Press.

Engel, Christoph. 2011. Dictator games: A meta study. *Experimental Economics* 14: 583-610.

European Data Protection Supervisor. 2011. Opinion on the communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. "A comprehensive approach on personal data protection in the European Union", § 85.

Fehr, Ernst, and Klaus M. Schmidt. 1999. A Theory of Fairness, Competition, and Cooperation. *Quarterly Journal of Economics* 114: 817-868.

Feinberg, Matthew, Robb Willer, Jennifer Stellar, and Dacher Keltner. 2012. The Virtues of Gossip: Reputational Information Sharing as Prosocial Behavior. *Journal of Personality and Social Psychology* 102: 1015-1030.

Fischbacher, Urs. 2007. z-Tree. Zurich Toolbox for Ready-made Economic Experiments. *Experimental Economics* 10: 171-178.

Forsythe, Robert, Joel L. Horowitz, N. Eugene Savin, and Martin Sefton. 1994. Fairness in Simple Bargaining Experiments. *Games and Economic Behavior* 6: 347-369.

Foucault, Michel. 1977. *Surveiller et punir*. Paris: Gallimard.

Frey, Bruno, and Iris Bohnet. 1999. Social Distance and Other-Regarding Behavior in Dictator Games: Comment. *American Economic Review* 89: 335-339.

Geambasu, Roxana, Tadayoshi Kohno, Admit A. Levy, and Henry M. Levy. 2009. Vanish: Increasing data privacy with self-destructing data. Proceedings of the 18th Usenix Security Symposium.

Goodin, Robert E., and Frank Jackson. 2007. Freedom from Fear. *Philosophy & Public Affairs* 35: 249-265.

Greiner, Ben. 2004. An Online Recruitment System for Economic Experiments. Pp. 79-93 in *Forschung und wissenschaftliches Rechnen. GWDG Bericht 63. Ges. für Wiss. Datenverarbeitung*, edited by Kurt Kremer and Volker Macho. Göttingen.

Grimmelmann, James. 2009. Saving Facebook, *Iowa Law Review* 94: 1137-1206.

Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51: 605-622.

Haley, Kevin J., and Daniel M. T. Fessler. 2005. Nobody's Watching? Subtle Cues Affect Generosity in an Anonymous Economic Game. *Evolution of Human Behavior* 26: 245-256.

Hoffman, Elizabeth, Kevin McCabe, Keith Shachat, and Vernon L. Smith. 1994. Preferences, Property Rights, and Anonymity in Bargaining Games. *Games and Economic Behavior* 7: 346-380.

Hoffman, Elizabeth, Kevin McCabe, and Vernon L. Smith. 1996. Social Distance and Other-Regarding Behavior in Dictator Games. *American Economic Review* 86: 563-660.

Holmes, Oliver W. 1872. *The Poet at the Breakfast-Table*. Cambridge, MA: University Press: Welch, Bigelow, & Co.

Holt, Charles A., Susan K. Laury. 2002. Risk Aversion and Incentive Effects. *American Economic Review* 92: 1644-1655.

Huberman, Bernardo A., Eytan Adar, and Leslie R. Fine. 2005. Valuating Privacy. *IEEE Security & Privacy* 3: 22-25.

Hui, Kai-Lung, Hock H. Teo, and Sang-Yong T. Lee. 2007. The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly* 31: 19-33.

Hui, Kai-Lung, and Ivan P. L. Png. 2006. The Economics of Privacy. Pp. 471-498 in vol. 1 of the *Handbooks in Information Systems: Economics and Information Systems*, edited by Terrence Hendershott. Bingley: Emerald.

Jentzsch, Nicola, Sören Preibusch, and Andreas Harasser. 2012. European Network and Information Security Agency, Study on monetising privacy: An economic model for pricing personal information.

John, Leslie, Alessandro Acquisti, and George Loewenstein. 2011. Strangers on a Plane:Context-Dependent Willingness to Divulge Personal Information. *Journal of Consumer Research* 37: 858-873.

Johnson, Eric, Steven Bellman, and Gerald Lohse. 2002. Defaults, Framing and Privacy: Why Opting In-Opting Out. *Marketing Letters* 13: 5-15.

Jolls, Christine. 2010. Rationality and Consent in Privacy Law. Working Paper. Yale Law School, New Haven, CT.

Kahneman, Daniel, Jack L. Knetsch, and Richard H. Thaler. 1991. Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias. *Journal of Economic Perspectives* 5: 193-206.

Kahneman, Daniel, and Ilana Ritov. 1994. Determinants of Stated Willingness To Pay for Public Goods: A Study in the Headline Method. *Journal of Risk and Uncertainty* 9: 5-38.

Krupka, Erin L., and Roberto A. Weber. 2013. Identifying Social Norms Using Coordination Games: Why Does Dictator Game Sharing Vary? *Journal of the European Economic Association* 11: 495-524.

Kumaraguru, Ponnurangam, and Lorrie F. Cranor. 2005. Privacy Indexes: A Survey of Westin's Studies. Working Paper. Institute for Software Research International,School of Computer Science, Carnegie Mellon University, Pittsburgh, PA.

Laibson, David. 1997. Golden Eggs and Hyperbolic Discounting. *Quarterly Journal of Economics* 112: 443-477.

Lessig, Lawrence. 2007. The Code of Privacy. *Proceedings of the American Philosophical Society* 151: 283-290.

Levitt, Steven D., John A. List. 2007. What Do Laboratory Experiments Measuring Social Preferences Reveal about the Real World? *Journal of Economic Perspectives* 21: 153-174.

List, John A. 2007. On the Interpretation of Giving in Dictator Games. *Journal of Political Economy* 115: 482-493.

Loewenstein, George. 1992. The Fall and Rise of Psychological Explanations in the Economics of Intertemporal Choice. Pp. 3-34 in *Choice Over Time*, edited by George Loewenstein and Jon Elster. New York, NY: Russell Sage Foundation.

Lyon, David. 2006. 9/11, Synopticon, and Scopophilia: Watching and Being Watched. Pp. 35-54 in *The New Politics of Surveillance and Visibility*, edited by Richard V. Ericson and Kevin D. Haggerty. Toronto: University of Toronto Press.

Mayer-Schönberger, Viktor. 2009. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

McAdams, Richard H., and Eric B. Rasmusen. 2007. Norms and the Law. Pp. 573-618 in vol. 1 of the *Handbook of Law and Economics*, edited by A. Mitchell Polinsky and Steven Shavell. Amsterdam: Elsevier.

McAdams, Richard H. 1997. The Origin, Development and Regulation of Norms. *Michigan Law Review* 96: 338-433.

McKenzie, Craig R. M., Michael J. Liersch, and Stacey R. Finkelstein. 2006. Recommendations Implicit in Policy Defaults. *Psychological Science* 17: 414-420.

Mitrou, Lilian. 2010. The Impact of Communications Data Retention on Fundamental Rights and Democracy. Pp. 127-147 in *Surveillance and Democracy*, edited by Kevin D. Haggerty and Minas Samatas. London: Routledge.

Nissenbaum, Helen. 2010. *Privacy in Context. Technology, Policy, and The Integrity of Social Life*. Stanford, CA: Stanford University Press.

Nozick, Robert. 1974. *Anarchy, State and Utopia*. New York, NY: Basic Books.

O'Donoghue, Ted, and Matthew Rabin. 2001. Choice and procrastination. *Quarterly Journal of Economics* 116: 121-160.

Peppet, Scott R. 2011. Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future. *Northwestern University Law Review* 105: 1153-1204.

Posner, Eric A. 2000. *Law and Social Norms*. Cambridge, MA: Harvard University Press.

Posner, Richard A. 1978. The Right of Privacy. *Georgia Law Review* 12: 393-422.

Posner, Richard A. 1981. The Economics of Privacy. *American Economic Review* 71: 405-409.

Posner, Richard A. 2008. Privacy, Surveillance, and Law. *University of Chicago Law Review* 75: 245-260.

Post, Robert C. 1989. The Social Foundations of Privacy: Community and Self in the Common Law Tort. *California Law Review* 77: 957-1010.

Richards, Neil M. 2013. The Dangers of Surveillance. *Harvard Law Review* 126: 1934-1965.

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

Rosen, Jeffrey. 2001. *The Unwanted Gaze. The Destruction of Privacy in America*. New York, NY: Random House.

Rosen, Jeffrey. 2011. Free Speech, Privacy, and the Web that Never Forgets. *Journal on Telecommunications & High Technology Law* 9: 345-356.

Rosen, Jeffrey. 2012. The Right To Be Forgotten. *Stanford Law Review Online* 64: 88-92.

Samuelson, William, and Richard Zeckhauser. 1988. Status Quo Bias in Decision Making. *Journal of Risk and Uncertainty* 1: 7-59.

Selten, Reinhard. 1967. Die Strategiemethode zur Erforschung des eingeschränkt rationalen Verhaltens im Rahmen eines Oligopolexperiments. Pp. 136-168 in *Beiträge zur experimentellen Wirtschaftsforschung*, edited by Heinz Sauermann. Tübingen: Mohr Siebeck.

Sen, Amartya. 2010. *The Idea of Justice*. London: Penguin.

Slovic, Paul. 2000. *The Perception of Risk*. London: Routledge.

Stigler, George J. 1980. An Introduction to Privacy in Economics and Politics. *Journal of Legal Studies* 9: 623-644.

Strahilevitz, Lior J. 2008. Reputation Nation: Law in an Era of Ubiquitous Personal Information. *Northwestern University Law Review* 102: 1667-1738.

Strandburg, Katherine J. 2006. Social Norms, Self-Control, and Privacy in the Online World. Pp. 31-53 in *Privacy and Technologies of Identity: A Cross-disciplinary Conversation*, edited by Katherine J. Strandburg and Daniela Stan Raicu. New York, NY: Springer.

Sugden, Robert. 1986. *The Economics of Rights, Cooperation and Welfare*. London: PalgraveMacmillan.

Sunstein, Cass R. 2003. *Why Societies Need Dissent*. Cambridge, MA: Harvard University Press.

Sunstein, Cass R. 2009. *On Rumors. How Falsehoods Spread, Why We Believe Them, What Can Be Done*. New York, NY: Farrar, Straus and Giroux.

de Terwangne, Cécile. 2012. Internet Privacy and the Right to Be Forgotten/Right to Oblivion, Revista de Internet. *Derecho y Política* 13: 109-121.

Tönnies, Ferdinand. 1887. *Gemeinschaft und Gesellschaft. Abhandlungen des Communismus und des Socialismus als Empirischer Culturformen*. Leipzig: Fues.

Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research* 22: 254-268.

Tucker, Catherine. 2011. Social Networks, Personalized Advertising, and Privacy Controls. MIT Sloan School Working Paper 4851-10. Massachusetts Institute of Technology, Cambridge, MA.

Wathieu, Luc, and Allan Friedman. 2007. An Empirical Approach to Understanding Privacy Valuation. Working Paper. Harvard University, Cambridge, MA.

White, Gregory L., and Philip G. Zimbardo. 1975. The Chilling Effects of Surveillance: Deindividuation and Reactance, Office of Naval Research, Technical Report Z-15.

Young, H. Peyton. 2008. Social Norms. *The New Palgrave Dictionary of Economics Online*, edited by Steven Durlauf and Lawrence E. Blume. 2nd Ed. London: Palgrave Macmillan.

Zittrain, Jonathan. 2008. *The Future of the Internet – And How to Stop It*. New Haven, CT: Yale University Press.

# APPENDIXES

## Appendix A: Proof

Participants give their consent if

$$\langle U(\pi_{ic}) = e_i - s_j - \beta_{ic} \max\{e_i - 2s_j, 0\} + c\rangle \;\geq\; \langle U(\pi_{ip}) = e_i - s_j - \beta_{ip} \max\{e_i - 2s_j, 0\}\rangle$$

Building on our assumptions and the corner solutions determined by Fehr and Schmidt (1999), we can determine $c$ for the following cases:

(1) $(\beta_{ic} \geq \frac{1}{2}, \beta_{ip} \geq \frac{1}{2})$ (*no chill, always egalitarian*)

$e_i - \frac{1}{2}e_i + c \geq e_i - \frac{1}{2}e_i \qquad c \geq 0$

(2) $(\beta_{ic} \geq \frac{1}{2}, \beta_{ip} \leq \frac{1}{2})$ (*chill from selfish to egalitarian*)

$e_i - \frac{1}{2}e_i + c \geq e_i \qquad c \geq \frac{1}{2}e_i$

(3) $(\beta_{ic} \leq \frac{1}{2}, \beta_{ip} \leq \frac{1}{2})$ (*no chill, always selfish*)

$e_i + c \geq e_i \qquad c \geq 0$

(4) $(\beta_{ic} \leq \frac{1}{2}, \beta_{ip} \geq \frac{1}{2})$ (*chill from egalitarian to selfish*)

$e_i + c \geq e_i - \frac{1}{2}e_i \qquad c \geq -\frac{1}{2}e_i$

## Appendix B: Instructions

***General explanations for participants***

In the following three experiments you can earn a considerable amount of money based on the choices you make. It is therefore very important to read the following instructions carefully.

You are not allowed to communicate with the other participants during the experiment. If you have questions, please ask one of the experimenters. If you do not comply with this rule, you will be excluded from the experiment and all payoffs. The experiment will last no more than 90 minutes. Please make sure that you can stay until the end.

You will be paid 2.50 € for participating in the experiment. You will have the opportunity to increase your earnings through the decisions you make in the experiment. The money you earn today will be cashed out to you immediately after the end of the experiment. Please note that in order to fetch your payoffs you will need a personal identification number (PIN). Prior to the beginning of the first part of the experiment, you will have the opportunity to create a PIN by filling the corresponding boxes on the screen. The PIN shall consist of the following elements: First letter of your mother's first name (if unknown, insert "*"). First letter of your father's first name (if unknown, insert "*"). Second letter of your favorite animal. Second letter of your favorite city. A number between 100 and 999.

Example:
Your mother's first name is Eve. Your father's first name is Adam. Your favorite animal is the camel. Your favorite city is Cologne. You chose the number 144. Your PIN would be: eaao144.

Please note that we cannot establish any link between the PIN and your identity. The PIN does not provide us any means to determine who you are and which decision you made in the lab. By entering the PIN you remain completely anonymous.

We will provide you with separate instructions for every experiment.

***First experiment***

In the first experiment, there are two roles: player A and player B. Player A is the only one to make a decision. Player B does not make any decision. The decisions made by player A will affect player B. You will first make a decision in the role of player A. After having made a decision in the role of player A, the computer will randomly assign you the role of player A or the role of player B. Every participant assigned the role of player A will then randomly be matched with a participant assigned the role of player B. If you are assigned the role of player A, the choices you previously made will be implemented. If you are assigned the role of player B, the choices of the player A you are matched with will be implemented.

The first experiment consists of two stages. The roles determined by the computer remain identical in both stages. You start with the decisions in the first stage. Afterwards you will make your decisions in the second stage.

1st stage

In this stage, each player A is endowed with an amount of 100 Taler. We refer to this amount as your endowment. The conversion rate is:

1 Taler = 9 Eurocents.

Player A can decide over the distribution of his endowment. He can choose to share any amount with player B or keep the entire amount for himself.

If you are player A, your payoffs consist of the amount you choose to keep for yourself. If you are player B, your payoffs consist of the amount which player A has shared with you.

The instructions of the second stage will be distributed after having made your choice in the first stage.

[In the chilling effects treatment, the instructions were identical, except that the dictator game was now described as being the second stage and that participants obtained the instructions of both the second stage and the first stage prior to making their decisions.]

2nd stage

If you are assigned the role of player A, you can increase your payoffs under the following conditions:

If you are player A, you have the opportunity to give your consent to the publication of your real name (first name and last name) and the amount you shared with player B. Both pieces of information will only be published if you consent to the publication (§ 4a Abs. 1 S. 1 BDSG)[25].

You have the opportunity to indicate how much money you are willing to accept in exchange for the publication of your real name (first name and last name) and the amount you shared with player B on a website. The computer will randomly determine an amount between 0 € and

25 Paragraph 4a Section 1 Phrase 1 of the German Federal Data Protection Act.

9.00 €. All amounts between 0 € and 9.00 € are equally probable. The choice you will have to make will be presented as in the following example: [screenshot].

In case the randomly determined amount exceeds the minimum amount you are willing to accept, your consent is valid. In this case, you will receive the randomly determined amount on presentation of your ID. In case the randomly determined amount is inferior to the minimum amount you are willing to accept, your consent is invalid. In this case, you do not receive payoffs for your consent. Neither your real name nor the amount you shared with player B will be published. If you do not want to give your consent, you can refuse all amounts.

Example 1: Alpha is willing to accept 2.43 €. The computer randomly determines an amount of 8.87 €. We are willing to pay more than Alpha is willing to accept. Alpha's consent is valid. Alpha has to present his ID when fetching his payoffs. Alpha receives 8.87 € for his consent.

Example 2: Beta is willing to accept 1.27 €. The computer randomly determines an amount of 0.98 €. We are willing to pay less than Beta is willing to accept. Beta's consent is invalid. Beta will not have to present her ID when fetching her payoffs. Beta does not receive payoffs for her consent.

Example 3: Gamma does not want to give his consent. He indicates an amount which exceeds 9.00 € (e.g., 9.01 €). Gamma has not consented.

Please note that you will forego possible gains if you do not indicate the true minimum amount you are willing to accept in exchange for your consent.

If you give your consent, the information mentioned above (first name, last name and amount shared with player B) will be published on a publicly accessible website managed by the experimenters. The name of the website is "Kölner Internet-Experimente 2012".

The information will be displayed on the website as in the following example: [screenshot].

This is the only information that will be displayed on the website. The names will be ranked according to the amounts shared by player A. The amounts will be listed from the top in an increasing order. As shown in the example above, amounts will be ordered according to the pattern a < b < c < d. Neither participants nor anyone else will be allowed to post anything on the website.

Please note that even in case of valid consent, the information will only be published with a probability of 80 % (4 out of 5 valid consents). If you give your valid consent, the information will thus not be published with a probability of 20 % (1 out of 5 consents). Whether you belong to the 80 % or to the 20 %, will be determined by a random draw of the computer. We will inform you about the result of the draw when picking up your payoffs.

During the experiment, we will not be able to determine the identity of participants who have given their consent. In order to validate your consent, we will give you the opportunity to disclose your real name when cashing out your payoffs. Your consent will be validated on presentation of your PIN and a valid photo ID with (government-issued ID card, passport, student ID). A link between your real name and the amount you shared can only be established after you presented an ID. Beforehand, such a link cannot be established.

Please note that any consent given during the experiment is binding. If you give your consent during the experiment and present your ID when picking up your payoffs, you will obtain the payoffs for your consent and the other parts of the experiment. You will also obtain the payoffs for giving your consent if you belong to the 20 % of consenting participants whose information will not be published. If you give your consent during the experiment, but refuse to present your

ID when picking up your payoffs, you will only obtain the payoffs for participating in the experiment (2.50 €).

If you do not give your consent during the experiment or if you are assigned the role of player B, you will only obtain the payoffs for participating and your other decisions in the experiment.

Deletion on request

In case you have given your consent and your information has been published, this information (first name, last name and amount shared with player B) will be deleted from the website on your request. You will be able to request deletion by sending an Email mentioning your PIN to koelnerinternetexperimente@gmail.com. The administrators will then delete the information from the website without delay. Deletion may be requested four weeks after the date of publication at the earliest (December 9, 2012). After the end of the four-week period, you can request the complete deletion of your information any time. Deletion before the end of this period is not possible.

[In the automatic deletion treatment, participants received the following instructions instead.]

Automatic deletion

In case you have given your consent and your information has been published, this information (first name, last name and amount shared with player B) will be automatically deleted from the website four weeks after the date of publication (December 9, 2012). After the end of the four week period, your information will be completely deleted without your having to do anything. Deletion before the end of this period is not possible.

Appendix

In addition, we would like to inform you about different privacy policies, which are not immediately relevant for the process of this experiment.

Please note that the purpose of this experiment is scientific and subject to the limitations of § 40 BDSG. The only form of data processing, which we engage in, is the publication of information covered by your consent. If you give your valid consent, we will only publish your information on the Google website. We will not, however, transfer it to third parties or publish it elsewhere. Extracts of the Google privacy policy are attached to these instructions.

We would like to point out that the information covered by your consent will not be linked with personal information stored in other databases used by the experimenters. The invitation to future experiments does not depend on the decisions you make in this experiment. Furthermore, we guarantee that other participants will not learn about the decisions you made in this experiment when cashing out your payoffs.

Please note that according to the usual technical and legal standards, personal information (e.g., your name) cannot be linked with the decisions that participants have made in this lab. Therefore, consent may be validly given only under the procedure explained above.

***Second experiment***

In this experiment, you are not matched with another player. Your decisions are only relevant for yourself and only affect your own payoffs. Conversely, the other players' decisions only affect their own payoffs.

In this experiment, you will have to decide between option a and option b in ten different cases (lotteries). Each option represents two different payoffs (a high one and a low one), which are cashed out with different probabilities.

Options a and b will be presented as in the following example:

| Lottery | Option a | Option b | Your decision |
|---|---|---|---|
| 1 | 2.00 € with probability 10 %<br><br>or<br><br>1.60 € with probability 90 % | 3.85 € with probability 10 %<br><br>or<br><br>0.10 € with probability 90 % | Option a<br><br>Option b |

The computer will provide that the payoffs will be realized with precisely the associated probabilities.

In the example depicted above, this means:

In case of option a, the gain of 2 € will be realized with probability 10 %, while the gain of 1.60 € will be realized with probability 90 %.

In case of option b, the gain of 3.85 € will be realized with probability 10 %, while the gain of 0.10 € will be realized with probability 90 %.

You will be able to indicate your preferred option in the right-hand column.

Please note that at the end, only one of the ten lotteries will determine your payoff. All lotteries are equally relevant. The computer will randomly determine one of the ten lotteries.

Afterwards, the computer will determine with the indicated probabilities, whether the higher payoff of the chosen option (2.00 € or 3.85 € respectively) or the lower payoff of the chosen option (1.60 € or 0.10 € respectively) will be cashed out to you.

***Third Experiment***

[Only the survey questions used for this article are presented.]

1) How strongly do you agree with the following statements? Please indicate your response on a scale from 1 to 5 (1 = strongly agree, 5 = strongly disagree).

a) Consumers have lost all control over how personal information is collected and used by companies.
b) Most businesses handle the personal information they collect about consumers in a proper and confidential way.
c) Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

2) Privacy means something different for every person. How important is each of the following aspects to you? Please indicate for each of the following aspects whether it is extremely important, important or not very important/not important at all.

a) Being able to control who can obtain information about you.
b) Being able to share confidential matters with someone you trust.
c) Knowing that nobody can observe you or listen to you without your consent.
d) Being able to control which information about you is registered.
e) Not being disturbed at home.
f) Being able to be alone in certain situations without anyone else being present.
g) Having persons in your social and working environments who don't ask you intimate questions.
h) Not being observed at work.

3) How strongly do you differentiate between close persons (e.g., your best friends) and less close persons (e.g., mere acquaintances) in the privacy settings of your preferred social network (the one you use most frequently)? Please indicate your response on a scale from 1 to 7 (1 = very strongly, 7 = not at all).

4) Have you ever tried to delete information (comments, pictures, videos) because you regretted having posted it? Yes__ No__

5) Are you concerned about how much information about you is publicly available on the Internet? Please indicate your response on a scale from 1 to 7 (1 = very concerned, 7 = not concerned at all).

6) Have you ever made bad experiences, because embarrassing or erroneous information about you was posted on the Internet? Yes__ No__

7) Have you ever asked another person to delete information about you (comments, pictures, videos) about you from the Internet? Yes__ No__

8) Was your request successful? Yes__ No__

9) Have you read the privacy policy of your preferred social network (the one you use most frequently)? Yes__ No__

10) How concerned are you about the way in which your preferred social network (the one you use most frequently) handles your personal information? Please indicate your response on a scale from 1 to 5 (1 = not concerned at all, 5 = very concerned).

11) Are you concerned about the following things with respect to your preferred social network (the one you use most frequently)? Please indicate your response on a scale from 1 to 7 (1 = not concerned at all, 7 = very concerned).

a) The type of information which you disclose to other members the social network.
b) What the social network operator can know about you.
c) Who has access to the information you post in the social network.
d) How the information you post in the social network may be used.
e) The type of personal information which the government generally registers about you.
f) The type of personal information which the government registers in the social network.