Relative Privacy Valuations under Varying Disclosure Characteristics

Joseph R. Buckman
jbuckman@ksu.edu

Kansas State University
Department of Management
3091 Business Building
Manhattan, KS 66506

Jesse C. Bockstedt
bockstedt@emory.edu

Emory University
Goizueta Business School
1300 Clifton Road
Atlanta, GA 30322

Matthew J. Hashim
mhashim@email.arizona.edu

University of Arizona
Department of MIS
P.O. Box 210108
Tucson, AZ 85721

Abstract

We investigate changes to the value individuals place on the online disclosure of their private information in the presence of multiple privacy factors. We use an incentive compatible mechanism to capture individuals' willingness-to-accept (WTA) for a privacy disclosure in a series of three randomized experiments. Each experiment manipulates characteristics of a required privacy disclosure by altering the information context, intended secondary use of the disclosed private information, and the requirement to disclose personally identifying information. We collect data from two populations (college students and Amazon Mechanical Turk workers) to aid with generalizability of our results. As methodological checks to rule out lack of awareness in the participants, we first increase the saliency of the privacy disclosure characteristics in the second experiment and then require participants to watch a video on the potential consequences of disclosing private information in the third experiment. Across the three experiments, we consistently observe null effects for each of the privacy factors with the exception of two population dependent exceptions in the second study. Our participants do acknowledge the increased risk introduced by the experimental factors and the increased saliency and awareness do lead to higher privacy valuations on average. However, there is no consistent manifestation as significant main effects for the three privacy factors. This is in contrast to prior research, which has found significant effects for each of these factors when studied separately. The results provide a unique perspective on privacy valuations by demonstrating that results from prior research on simple privacy decisions may not translate to more realistic, complex privacy disclosure decisions that involve multiple factors.

Keywords: online privacy, information disclosure, experimental methods, willingness-to-accept, privacy valuations, Amazon Mechanical Turk

1. Introduction

Economists and industry leaders consider consumer data to be the primary asset that fuels the digital economy (Burke 2015). Consumer data enables firms to provide accurate product recommendations and customized content in order to personalize the consumer's online experience. Personalization can boost sales by an average of 20% (Soojian 2015), leading firms to enhance their data gathering capabilities and maximize the amount and quality of data obtained about consumers. Firms also create revenue streams by selling consumer data to information brokers (Steel et al. 2013). For example, Acxiom claims to have on average 1,500 pieces of data on each of more than 200 million Americans (Kroft 2014). Technology firms, such as Facebook, Google, and Amazon, collect well over one billion discrete units of data from their users every month (Simonite 2012). Such data collection and usage practices lead directly to an increase in privacy concerns among consumers (Flaherty 2013).

As consumers become aware of increasingly pervasive data collection practices, empirical and anecdotal evidence suggest that they place value on their private information[1]. Research has shown that the monetary value that consumers demand for their private information has increased significantly over time (Huberman et al. 2005; Danezis et al. 2005; Cvrcek et al. 2006; Acquisti et al. 2013; Staiano et al. 2014). In addition, consumers expect decision-making enhancements and personalization services in exchange for the disclosure of private information (Shah 2015). However, it is not clear consumers understand the real market value of private information. It is also not clear that consumers understand the implications from disclosing personal information, that is, how and where their information is used, aggregated, packaged, and resold to other parties.

Many internet companies trade services for access to personal information, demonstrating a possible misalignment between expectations of privacy and actual privacy. In 2017, consumers and Internet pundits caused an uproar when Unroll.me, a website that helps users unsubscribe from email lists,

[1] Throughout the paper, we use the term "private information" to refer to any information an online firm would not know unless disclosed by the consumer. Thus, private information may include personal information such as gender and race, which may not be considered private in a face-to-face exchange.

revealed it had been selling user data to generate revenue for their free to consumer service (Feldman 2017). In 2018, the #DeleteFacebook social media campaign began in response to Cambridge Analytica acquiring personal data on approximately 87 million unknowing Facebook users (Bever 2018). The US government even took notice of the incident and held congressional hearings with Facebook CEO Mark Zuckerberg. Despite all of this, recent data compiled by the strategic marketing firm Kepios indicate that very few people actually left Facebook and instead the number of monthly active users grew by approximately 4% (Zetlin 2018). These examples indicate a potential for missed expectations because consumers do not understand the value of their personal information for these service providers. It is this aspect that we focus on in this paper: understanding what dimensions of an information disclosure online affect a consumer's valuation for their private information.

Thus far, privacy valuation research has primarily been concerned with unidimensional disclosure decisions that either discover the compensation consumers require for disclosing specific, single pieces of information, or measure the consumer's willingness to pay for privacy protection. To deepen the understanding of consumer privacy valuations, we study relative changes in private information valuations in a realistic, multidimensional disclosure decision. Using economic experiments, we study how the information context, the requirement to disclose personally identifying information, and the service provider's plans to sell personal information to third parties affect the value consumers place on their private information. Interestingly, with the exception of two sample-specific instances, we largely find null effects, which are in contrast to prior work that has typically looked at these dimensions independently (e.g., Culnan 1993; Berendt et al. 2005). We also find that the null effects persist even after increasing the saliency of the privacy factors in the disclosure decision and highlighting the consequences associated with disclosing information to the service provider. However, post hoc analysis and insights from a post-experiment survey suggest that some participants do acknowledge the increased risk introduced by these disclosure dimensions by pricing themselves out of the market altogether. Our findings suggest it might be an all or nothing type of decision as opposed to an activation of individual factors the prior literature suggests are important in a multi-dimension private information disclosure. The

results also suggest that online disclosure decisions are evolving, especially in settings that incorporate multiple disclosure dimensions.

2. Related Literature

Existing economics of privacy research shows that individuals act strategically within an information market of buyers and sellers (Posner 1981), only disclosing information after considering privacy-related consequences. Laufer and Wolfe (1977) defined this situation as a privacy calculus of costs and benefits associated with every information disclosure decision. Later, the privacy calculus was extended to show that individuals consider their general concerns, prior experiences, Internet trust, and personal Internet interest, before making a disclosure decision (Culnan and Armstrong 1999; Dinev and Hart 2006).

Regarding benefits in the privacy calculus, empirical studies have identified monetary rewards to be an effective means of obtaining information in privacy decisions (Phelps et al. 2000; Caudill and Murphy 2000; Hui et al. 2007; Xu et al. 2010; Preibusch 2013). Auction mechanisms (e.g., second-price) have frequently been used to establish point estimates of the monetary value individuals require to disclose single pieces of private information, such as age, weight, or location (Danezis et al. 2005; Huberman et al. 2005; Cvrcek et al. 2006; Staiano et al. 2014). Their observed values varied widely, suggesting subjectivity and difficulty establishing a single, generalized monetary value for an average person's private information. Further, an auction mechanism may introduce unnatural competition among study participants for selling their private information.

Prior research has also argued that the point estimates consumers place on their private information may be misguided due to inherent instability (Acquisti et al. 2015) and uncertainty regarding consequences (Acquisti et al. 2013). Klopfer and Rubenstein (1977) proposed that the instability of valuations stems from the subjective nature of the interpretation of privacy and the reward for revealing information. An individual's subjective interpretation may also be flawed due to incomplete information about the disclosure (Acquisti and Grossklags 2005). That is, individuals may have little knowledge about the information an organization has already captured and organizations do not always explicitly state their intentions or planned usage for gathered information. Thus, consumers struggle to determine what types

and how much information should be disclosed (Acquisti et al. 2015). Even when consumers receive full details in the disclosure decision, they continue to struggle with optimal decision-making due to bounded rationality (Acquisti and Grossklags 2005). In other words, consumers possess cognitive limitations that hinder their ability to acquire and process the dimensions of a disclosure decision (Acquisti 2004).

In addition, empirical studies found that non-normative factors influence privacy disclosure decisions. Tsai et al. (2011) implemented a lab experiment using a search engine to find products from multiple websites. Search results included the price of the product and a rating for each website's privacy policy, among other information. The authors found that consumers pay premium prices for products from websites with greater privacy protection when differences in protection are salient and accessible. Acquisti et al. (2013) used a field experiment to investigate non-normative privacy behavior and the presence of an endowment effect. In their experiment, mall shoppers received one of two types of gift cards with either traceability or non-traceability of the purchases with the gift card. Results show that those with a lower value, non-traceable gift card were unwilling to exchange for a higher value, traceable card. Thus, consumers' value endowed privacy protections greater than non-endowed privacy protections.

Given the landscape of prior literature on privacy valuations, we contribute in two important ways. First, we study multi-dimensional information disclosure decisions, which combine important privacy factors that to the best of our knowledge have not been considered together in the prior literature. We discuss these dimensions and our corresponding hypotheses in the next section. Second, we address the limitations identified in the prior literature for measuring privacy valuations by introducing methodology from experimental economics. We discuss our experimental procedures and methodology in Section 4.

3. Research Model and Hypotheses

We focus our attention on three important factors in privacy disclosure: the *context of the information disclosure*, the intended *secondary use of the disclosed information*, and the *requirement to disclose identifying information*. These factors can affect an individual's privacy and potentially the value an individual places on their privacy. Of the commonly studied privacy factors, these three frequently appear

in real online information disclosures, whereas other commonly studied privacy factors such as information accuracy and improper access are less common in practice. Information context directly affects an individual's trusting beliefs, risk beliefs, and behavioral intentions toward an information disclosure (Malhotra et al. 2004). The secondary use of information, i.e., the distribution of disclosed information to third parties, affects an Internet user's privacy decisions and can result in stricter privacy settings (Chellappa and Sin 2005; Angst and Agarwal 2009). Requiring the disclosure of personally identifying information increases vulnerability and the likelihood of experiencing negative consequences from disclosure (Solove 2006).

From an economic view, consumers require utility (e.g., a payoff) to transition from a state of high privacy to a state of low privacy. In the case of monetary payoffs, we use willingness-to-accept (WTA) to represent the monetary value a consumer will accept in order to make this transition (Hanemann 1991). A formal utility function of privacy decision-making that includes WTA follows (cf. Acquisti et al. 2013, page 258). Let $u(w, p)$ be a consumer's utility regarding wealth, w, and privacy, p, with p^- representing less privacy and p^+ representing more privacy. For any consumer in a position of $u(w, p^+)$, the minimum amount that the consumer would require to enter a state of p^- is given by $u(w + \text{WTA}, p^-) = u(w, p^+)$. Thus if a consumer perceives they are transitioning to a state of lower privacy, they should require a gain in utility in return.

Our first hypothesis considers the effect of information context on a privacy valuation. In a review of the privacy literature, Smith et al. (2011) identified eight differing contexts of private information. The list includes behavioral, biographical, financial, medical, consumer, personal, employee, general, and publicly available information. Each type of private information creates different perceptions of privacy among individuals, and prior research has observed that individuals generally perceive information disclosed in the consumer context as less private and information disclosed in the medical context as more private (Nowak and Phelps 1992; Phelps et al. 2000; Sheehan and Hoy 2000). Thus, in an information disclosure decision we expect that a context perceived as more private leads to a higher WTA

for making the disclosure in comparison to a context perceived to be less private.[2] Therefore, we hypothesize the following:

Hypothesis 1: Participants asked to disclose information in a more private context (e.g., medical information) will exhibit a higher privacy valuation (WTA) than participants asked to disclose information in a less private context (e.g., consumer shopping information).

Our second hypothesis predicts the influence of an organization's secondary use intentions on a privacy valuation. When organizations gather information on consumers and users they have the option to either distribute (or sell) this information to an external party (external secondary use), or restrict this information for use only in internal operations (internal secondary use) (McMillan 2014). The literature has shown that consumers hold a negative attitude towards external secondary information use (Culnan 1993; Sutanto et al. 2013), which influences their purchasing behavior (Hoffman et al. 1999; Sutanto et al. 2013). In contrast, the same research has shown that consumers hold a positive attitude towards internal secondary information use when it results in enhanced custom product offerings. Further, consumers are willing to pay premium prices to prevent the external secondary use of private information (Hann et al. 2007). Therefore, an individual should require greater compensation to disclose their private information to an organization that practices external secondary use. Formally, we hypothesize the following:

Hypothesis 2: Participants asked to disclose information that will be distributed to a third party (i.e., external secondary use) will exhibit a higher privacy valuation (WTA) than participants asked to disclose information that will not be distributed to a third party (i.e., internal secondary use).

Our third hypothesis predicts that the requirement to disclose identifiable information (PII) will affect a person's WTA because it can increase direct risk. Individuals have a strong desire to protect identifying information because it increases vulnerability and the likelihood for others to inflict harm (Solove 2006; Ohm 2010). Consumers also prefer using online services that have high online privacy

[2] We acknowledge that is possible for the specific type of information disclosed to modify the perceived level of privacy for the context. For example, revealing the purchase of adult videos (shopping context) would be perceived as more private than revealing if an individual is a smoker (medical context). We control for these exceptions to the general perceptions of information context in the design of our experiments as described in Section 4.

protections, such as those that do not collect identifying information, unless they receive adequate financial gain or convenience (Hann et al. 2007). The National Institute of Standards and Technologies (NIST) defines (McCallister 2010, p. ES-1) PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." We focus our study on NIST's type 1 in the manipulation of the PII factor, and acknowledge the potential impact of linkable information (type 2) by also testing for interaction effects (discussed in the next section). Markets for securities, bonds, and insurance demonstrate the common economic principle that taking on higher risks leads to higher expectations for compensation. Disclosing PII is inherently risky, therefore we expect a market for privacy to act in a similar manner to these other markets and hypothesize the following:

Hypothesis 3: Participants asked to disclose information that requires the inclusion of personally identifying information (PII type 1) will exhibit a higher privacy valuation (WTA) than participants asked to disclose information that does not require personally identifying information.

To the best of the knowledge, we are the first to study the influence of these three privacy factors together in their impact on privacy valuations. Below we discuss the design and implementation of a set of experiments that allow us to combine these effects into a single disclosure scenario for our participants.

4. Experimental Procedures, Analyses, and Results

We designed and implemented three studies, with each study building upon the previous one. As will be discussed, the results of our first study were surprising – none of the factors showed significant effects on privacy valuations. Therefore, in Study 2 we increased the saliency of privacy factors for participants to help ensure the participants were fully aware of the disclosure dimensions. In Study 3, we went one step further and present a video that explicitly communicates to participants the potential consequences of disclosing private information. In the following subsections, we describe the experimental procedures and post-experiment survey that are common among the three studies, followed by the unique features and

analysis of the studies individually.

4.1 Experimental Procedures Common to Each Study

We used Qualtrics software to implement a randomized, between-subjects design consisting of eight experimental treatments (2^3 factorial design). The factorial design allowed us to combine factors, test interactions, and gain power advantages with our sample sizes. We advertised the study as joint research collaboration between Google and the University of Arizona to gather user feedback in the design of new services. Participants were not aware they were participating in a purely academic study until they were debriefed at the conclusion of their participation, as was required by our university review board. Participants were told Google was conducting market research with the help of the University of Arizona and they would be paid for the disclosure of private information to help Google test compensation models. We used Google as the focal organization across all treatments and all participants to limit potential biases manifesting as treatment effects. Google is a real and well-known firm that regularly collects data about their customers, and with which most participants should have prior experience. Alternatively, using a fictitious or unknown firm would introduce uncontrolled uncertainty into the decision scenario.

The experiment treatments consisted of combinations of the following two-level factors: (1) the context of the information Google requires for their new application (high privacy is a request for medical history, low privacy is a request for shopping preferences), (2) the planned secondary use of the private information by Google (will or will not distribute the information to a third party), (3) whether or not Google requires the disclosure of PII. Participants in the high (low) information context condition were told they must disclose their medical (shopping) history information for a new Google medical (shopping) service. To ensure participants understood what to expect and control for the potential that their expectations of disclosure could impact their perceptions of the context privacy level, we provided participants with a list of items for each context condition prior to requiring their disclosure (see Online Appendix Table A2). Participants in the secondary (non-secondary) use condition were told that Google will (will not) distribute the information they disclose to third party marketing and advertising agencies.

Participants in the identifying (non-identifying) information condition were told that they must (will not have to) disclose PII including their full name, email address, and phone number.

To elicit WTA, we implemented the incentive compatible Becker-DeGroot-Marschak (BDM) procedure (Becker et al. 1964). In the absence of an incentive compatible procedure such as the BDM, participants tend to overstate their WTA (Coursey et al. 1987; Plott and Zeiler 2005; Shogren et al. 1994; Hanemann 1991; List and Shogren 2002). The BDM procedure is commonly used in experimental and behavioral economics studies when the good in question is subjective and there is not an established market price (List and Shogren 2002), and in abstract experimental contexts eliciting private values (Rivenbark 2011). Private information is representative of such a good.

BDM's incentive compatibility comes from the binding nature of the exchange. BDM incentivizes participants to be truthful in our experiment because those who sell their information must disclose their real private information and receive real payment for doing so.[3] We implemented the BDM procedure as follows. The system draws a random price for each participant from a uniform distribution between \$0 and \$5. Without knowing the drawn price, the participant provides their WTA for disclosing their information. Their WTA is compared with the drawn price and if the participant's WTA is lower than or equal to the drawn price then their information must be sold at the drawn price. For example, if a participant's WTA is \$2.50 (i.e., they are willing to disclose private information for \$2.50), and the system draws a price of \$3.00, the participant receives \$3.00 and must disclose their information. If the participant's WTA is greater than the drawn price, the participant does not sell their information. For example, if a participant's WTA is \$2.50 and the system draws a price of \$1.00, then no transaction occurs. The participant does not disclose their information and is directed to the post-experiment survey. Therefore, the BDM results in accurate stated valuations because stating a WTA that is higher than an actual valuation may result in a missed opportunity to sell information (i.e., disadvantageous non-selling). In contrast, stating a WTA lower than an actual valuation may result in the participant selling for less than

[3] We asked participants in the debrief if they disclosed false information and if so removed them from the analysis.

their desired value (i.e., disadvantageous selling). To ensure understanding of the BDM, we trained participants on the procedure and required them to pass a quiz before moving on to the experiment.

As noted above, we presented participants with a sample of the disclosure form they must complete if they sell their information, prior to entering their WTA. The sample form included the required identifying information fields if they were in that treatment. Participants viewed and disclosed the same number and types of items in both context treatments. Prior presentation of the sample form helped to control for participant uncertainty prior to the WTA decision.

Following the presentation of the sample form, we asked participants to enter their WTA for disclosing their information, given their treatment scenario. Participants had an unlimited amount of time to enter their WTA and they could opt-out at any point during the experiment. The acceptable range of WTA values was $0.00 - $5.00. As would be expected, actual market prices for private information vary based on specific data types, context, and time. For example, legally obtained batches of user profiles sell for as low as $0.005 per account (Madrigal 2012). The service Datacoup, who pays users to collect and share their social media data and credit card transactions, pays roughly $8 per month for this right. Furthermore, Facebook reported average revenue per user of $5.07 in 2017 (Shinal 2017), a value largely driven by leveraging user information for targeted advertising. Therefore, the $0.00-$5.00 range we chose for WTA measurements is fair and reflects the approximate magnitude of current market prices for private information. We also note that in our post-hoc analyses zero participants reported opting out because of the WTA range. Additionally, we use Tobit regression models in our analysis to control for WTA censoring due to the selected price range.

After participants submitted their WTA, the system reported the drawn price and the sales outcome. Those who successfully sold their private information then viewed a form that required them to complete all fields before continuing to the post-experiment survey and receiving payment. Participants who did not sell were directed to the post-experiment survey without completing the form. All items in the post-experiment survey used a 7-point Likert-type scale to capture demographics and relevant

controls.[4] To control for Internet experience, survey items included Internet usage, online privacy breach history, and propensity to falsify information online. Participants were instructed on how to receive credit and any monetary payment they were owed for their disclosure upon completion of the survey. Participants were always aware they would receive credit regardless of whether or not they disclosed their private information, in addition to monetary payments for their disclosure.

4.2 Study 1: Information Disclosure Factors and WTA

We recruited students from large, upper-division courses that frequently engage in research from the college of management and the school of public policy at the University of Arizona. We provided a link to the Qualtrics site to interested participants and allowed them to complete the study at their convenience. We sample from a fairly homogeneous population of undergraduate students in Study 1 (Druckman and Kam 2009; Compeau et al. 2012), so any deviations in WTA will likely be due to specific treatment manipulations and not underlying heterogeneity of the participants in the sample (e.g., wealth and other factors that vary across a diverse population). However, there may be specific limitations to generalizability due to the student sample. So in Studies 2 and 3 we sample from both homogenous (i.e., student) and heterogeneous (i.e., Amazon Mechanical Turk) populations to generalize results to a broader population.

Data Analysis and Results

In our first study, we collected data from 394 participants and omitted those who failed attention and manipulation-checking questions, had no variation in their survey responses, failed to complete the experiment, or declined to sell their information by opting out and not providing a WTA. In total, we removed 94 participants based on these criteria, leaving data from 300 participants.[5] Table 1 provides the summary statistics.

[4] The survey items can be found in the Online Appendix.

[5] A limitation of Qualtrics is that a new response is generated each time the hyperlink to begin the study is clicked. Therefore, it is necessary to remove more than 16% of responses due to being substantially incomplete. Please refer to Tables A9 and A10 in the Online Appendix for a detailed breakdown of responses removed from each study.

Table 1: Summary Statistics by Population, Study, and Treatment ($\overline{WTA}$ grouped by context)

Population	Study	Male	Female	$\overline{WTA}$	Treatment	Obs.	Count of Sold	$\overline{WTA}$ Sold
Students	1	170	130	$3.31	Med-SU-Id	33	9 (27.27%)	$2.91
					Med-No SU-Id	43	11 (25.58%)	$2.79
					Med-SU-No Id	40	12 (30.00%)	$2.93
					Med-No SU- No Id	35	11 (31.43%)	$2.45
				$3.05	Shop-SU-Id	39	9 (23.08%)	$2.36
					Shop-No SU-Id	38	11 (28.95%)	$1.72
					Shop-SU-No Id	35	12 (34.29%)	$2.45
					Shop-No SU-No Id	37	15 (40.54%)	$1.98
	2	114	88	$3.72	Med-SU-Id	21	5 (23.81%)	$2.50
					Med-No SU-Id	27	7 (25.93%)	$2.64
					Med-SU-No Id	27	8 (29.63%)	$2.94
					Med-No SU- No Id	25	10 (40.00%)	$2.29
				$3.28	Shop-SU-Id	25	7 (28.00%)	$1.70
					Shop-No SU-Id	24	7 (29.17%)	$2.07
					Shop-SU-No Id	24	9 (37.50%)	$1.85
					Shop-No SU-No Id	29	8 (27.59%)	$2.06
	3	77	63	$3.36	Shop-SU-Id	32	9 (28.13%)	$1.75
					Shop-No SU-Id	36	13 (36.11%)	$2.00
					Shop-SU-No Id	34	11 (32.35%)	$2.24
					Shop-No SU-No Id	38	14 (36.84%)	$1.79
AMT	2	237	199	$3.49	Med-SU-Id	58	9 (15.52%)	$1.76
					Med-No SU-Id	49	13 (26.53%)	$2.06
					Med-SU-No Id	65	26 (40.00%)	$1.88
					Med-No SU- No Id	54	17 (31.48%)	$2.31
				$3.47	Shop-SU-Id	49	12 (24.49%)	$2.08
					Shop-No SU-Id	58	18 (31.03%)	$2.35
					Shop-SU-No Id	54	21 (38.89%)	$2.18
					Shop-No SU-No Id	49	20 (40.82%)	$2.07
	3	91	91	$3.76	Shop-SU-Id	46	10 (21.74%)	$1.95
					Shop-No SU-Id	46	9 (19.57%)	$1.53
					Shop-SU-No Id	45	16 (35.56%)	$1.80
					Shop-No SU-No Id	45	9 (20.00%)	$2.04

Note: Med = Medical Context; Shop = Shopping Context; SU = Secondary Use; Id = Identifying Information

First, we tested for treatment effects using an ANCOVA model that includes the dependent variable WTA, control variables (gender, web usage, propensity to provide false information, indicated prior privacy breach), and main effects (three indicator variables representing the manipulated factors: information context; secondary use; identifying information). Results indicate a marginal difference (yet not significant at the $\alpha = 0.05$ level) in the mean of WTA for the information context main effect ($F = 3.17$, $p = 0.076$).

Next, we used a Tobit regression to uncover the magnitude of the effects. Tobit estimations are common in modeling willingness-to-pay/accept measurements because of the natural censoring of the dependent variable (e.g., Donaldson et al. 1998). We report only the average marginal effects because the baseline Tobit estimates reflect the marginal effects on the unobserved and uncensored dependent variable (McDonald and Moffitt 1980). Table 2 Model 1 presents the results for Study 1. The results do

not suggest any significant main effects.[6]

Table 2: Main Experimental Results Using Tobit Regressions

	Study 1	Study 2		Study 3	
Population	Students		AMT	Students	AMT
Variables	(1)	(2)	(3)	(4)	(5)
Gender	0.079	0.029	-0.246*	0.244	-0.215
	(0.147)	(0.182)	(0.125)	(0.257)	(0.217)
Age			0.205**		0.077
			(0.058)		(0.096)
Education			-0.052		-0.033
			(0.055)		(0.081)
False Information	-0.031	0.143	0.166*	0.000	0.040
	(0.082)	(0.105)	(0.066)	(0.163)	(0.123)
Web Usage	-0.113	0.055	0.010	-0.059	-0.111
	(0.083)	(0.104)	(0.057)	(0.141)	(0.085)
Breach History	0.022	0.044	0.056	-0.040	-0.084
	(0.052)	(0.064)	(0.047)	(0.091)	(0.075)
Information Context	0.223	0.416*	0.111		
	(0.144)	(0.175)	(0.129)		
Secondary Use	-0.005	-0.112	-0.106	0.137	-0.091
	(0.146)	(0.176)	(0.130)	(0.251)	(0.216)
Identifying Information	0.149	0.150	0.289*	0.259	0.204
	(0.147)	(0.178)	(0.130)	(0.255)	(0.221)
Constant	3.371**	2.621**	2.509**	3.661**	5.281**
	(0.406)	(0.571)	(0.552)	(0.913)	(1.065)
F-value	0.950	1.550	3.040**	0.520	0.750
Log pseudolikelihood	-498.865	-329.653	-729.350	-245.276	-293.726
Censored Observations	3 censored at 0	1 censored at 0	7 censored at 0	4 censored at 0	8 censored at 0
	43 censored at 5	52 censored at 5	130 censored at 5	41 censored at 5	76 censored at 5
	254 uncensored	149 uncensored	299 uncensored	95 uncensored	98 uncensored

Robust standard errors in parentheses, †$p \leq 0.10$, *$p \leq 0.05$, **$p \leq 0.01$. Average marginal effects reported for the coefficients.

4.3 Study 2: Increasing the Saliency of Treatment Factors

Consumers make privacy conscious decisions when privacy information is salient (Tsai et al. 2011). Furthermore, a common explanation for the privacy paradox is that users lack awareness of the risks involved in disclosing private information (e.g., Acquisti and Gross 2006, Barnes 2006, Tufekci 2008). Therefore, in Study 2 we increased the saliency of privacy factors as a methodological check to help rule out a lack of awareness as to what was being asked of the participants. According to Taylor and Fiske (1978), changing the color (e.g., bolding) and size of images (e.g., enlarging font) within textual descriptions lead to greater participant attention and recall of information. Further, prior work in computer vision has termed visual saliency as the idea that humans have significant visual arousal from changes in scene (Kadir and Brady 2001). Julesz (1995) and Treisman (1985) identify these changes as 'pop-out' and

[6] We also estimated a control variables only model, a fully interacted model, standard OLS regression models, and models incorporating (-1,1) effect coding for the main effects. Results of these models are consistent with those reported in Table 2. No significant interaction effects were found in any of the models.

create visual cues that stand out and aid in human visual saliency (i.e., attention grabbing). Accordingly, we enhanced the text describing each factor in the experiment, using larger bold fonts with italics and underlining, to increase visual saliency. We also included a summary page that reiterated the three manipulations immediately before participants were asked to enter their WTA (please refer to Tables A1, A4, and A6 of the Online Appendix). Otherwise, the procedure remained identical to that of Study 1.

To broaden the generalizability and implications of our research, we conducted Study 2 using two different populations: a homogenous student population and a heterogeneous Amazon Mechanical Turk (AMT) population. We implemented qualification controls and payments on AMT following prior work (e.g., Balebako et al. 2015), required the workers to be aged greater than 18, from the United States (US), have an acceptance rate greater than or equal to 89%, and a time limit of 30 minutes. We paid AMT workers $1.35 for their time (based on the national average for the US minimum wage of $7.25 and the average time to complete the study in pilot testing) plus a bonus payment for selling their private information using the same BDM mechanism we used with students.

The student sample size for Study 2 is 202 after removing 68 participants for the same reasons as in Study 1.[7] The AMT sample size is 436 participants after removing eight participants for failing manipulation checks. Within the AMT sample, 46% of participants were female, age ranged from 18 to 74 (46% were older than 35), and 51% had at least a Bachelor's degree.

Data Analysis and Results

Consistent with Study 1, we first tested for treatment effects using an ANCOVA. Regarding the student sample, the results indicate a significant difference in the mean of WTA for the information context main effect ($F = 6.25$, $p = 0.013$). Regarding the AMT sample, the results indicate a marginal difference (yet not significant at the $\alpha = 0.05$ level) for the identifying information main effect ($F = 3.37$, $p = 0.067$). Again, we estimated a Tobit regression (Table 2) and the average marginal effects in Model 2 (students)

[7] Power analyses provide evidence that we have sufficient power to detect small to medium effect sizes using our factorial design. Please refer to the Online Appendix for additional details.

illustrate a significant impact of information context on WTA. Changing from the shopping context to the medical context results in a \$0.42 ($p = 0.017$) increase in WTA. We note the fit for Model 2 is marginal, thus the result is not conclusive. The average marginal effects in Model 3 (AMT) illustrate a significant impact of identifying information on WTA. Changing from not including identifying information in the disclosure to including identifying information results in a \$0.29 ($p = 0.026$) increase in WTA. Although we observed these two significant main effects, they were not consistent across populations or models.

4.4 Study 3: Highlighting the Consequences of Private Information Disclosure

The persistence of null effects in Study 2 led to our design of Study 3. It includes an educational video that clearly highlights and describes the consequences and risks of disclosing private information online (the video can be viewed at https://goo.gl/X2C5lj). The video provides an additional methodological check to help rule out the explanation that our participants were unaware of the risks associated with private information disclosure. Participants were required to watch the video before beginning Study 3.

The video covered three aspects related to the consequences of information disclosure. First, it clearly defined external secondary use of private information and personally identifying information. Second, the video included actual examples of firms using these practices. Third, the video discussed four consequences of disclosing private information when external secondary use and PII are present. The video also presented multiple news article snippets supporting each consequence. Following the video, participants completed a quiz on the consequences of disclosing private information. The experiment did not begin until a participant correctly answered all quiz questions.

We fixed the information context to shopping preferences for all participants in Study 3 to simplify the experimental design and focus on the two factors consumers would generally expect of Google as an organization. Doing so allowed us to focus substantial time during the video on only two factors, instead of spending smaller amounts of time split up among the three factors. This resulted in a 2x2 design for Study 3 with the remainder of the procedure replicating the procedure of Study 2.

The student sample size for Study 3 was 140 usable participants (initially 175), and the AMT sample size was 182 usable participants (initially 200). We followed the same procedures for removing

participants as in Study 2, with the addition of also removing those that did not watch the full video. Within the AMT sample, 50% of participants were female, age ranged from 18 to 74 (51.65% were older than 35), and 50% completed at least a Bachelor's degree. We paid AMT workers $2.66 for their time[8] plus a BDM-based bonus payment for selling their information as with the students.

Data Analysis and Results

As before, we first tested for treatment effects using an ANCOVA. The results are largely consistent with the previous studies except that we find no significant main effects, regardless of population. The Tobit regressions (Table 2) also demonstrate no significant main effects. Note the intercept in Model 5 (AMT) is greater than $5.00, which is unusual given the censoring of WTA at $5.00. We conducted several post estimation tests to identify the underlying cause, including the Shapiro-Wilk test for normality of the error term, Breusch-Pagan test for heteroscedasticity, and variance inflation for multicollinearity. Based on the results, we conclude that the model contains heteroscedasticity.[9] We estimated two models that are robust against heteroscedasticity and the results were consistent with the Tobit regressions already presented.[10]

4.5 Post Hoc Analyses and Comparisons across Studies

With the exception of two population dependent significant main effects in Study 2, null effects persisted across all three studies, even after increasing saliency of the disclosure factors and having participants watch a video on the consequences associated with disclosing information. At face value, it suggests that consumers are largely neutral to these privacy factors in a disclosure. However, it is also possible that there are effects that did not manifest in the analysis of the main factors. Therefore, we conducted several post hoc analyses to determine the manner in which WTA valuations were affected across studies.[11]

We pooled the data across studies to compare effects of each study on WTA as shown in Table

[8] The slightly higher base payment in Study 3 was used because the participants had to watch the approximately 7 minute video and complete a quiz on the video prior to starting the study. We again based this payment on the prorated US minimum wage.

[9] The null hypothesis for the Breusch-Pagan test is H_0: Constant Variance. The results from the test provide that $\chi^2 = 3.61$ and $p = 0.058$, suggesting the presence of heteroscedasticity.

[10] Omitted here for sake of brevity. Please refer to the Online Appendix for further details.

[11] Heteroscedasticity was not present in any of the post hoc analyses.

3.[12] Study 3 fixed information context to shopping preferences, so our comparison across studies is limited to that factor level. Tobit regressions included an indicator variable for Study 1, 2, or 3. We used Study 1 as the baseline for comparison in Models 1-2 and Study 2 as the baseline in Models 3-4. Increasing the saliency of the privacy factors associated with a disclosure request resulted in a statistically significant increase in average WTA (Study 2 indicator, Model 1). Interestingly, the average WTA did not significantly change across the studies when Study 2 is the baseline for comparison (Study 1 and Study 3 indicators, Model 3). However, increased saliency combined with consequences shown in the video did increase the average WTA for Study 3 in comparison to Study 1 (Model 2), and Study 3 in comparison to Study 2 (Model 4).

Table 3: Pooled Analysis Using Tobit Regressions

Context	Both	Shopping Only		
Pooled Studies	1, 2	1, 2, 3		2, 3
Population	Students			AMT
Variables	(1)	(2)	(3)	(4)
Gender	0.051	0.068	0.068	-0.171
	(0.114)	(0.141)	(0.141)	(0.138)
Age				0.115†
				(0.062)
Education				-0.027
				(0.058)
False Information	0.044	0.020	0.020	0.147*
	(0.065)	(0.087)	(0.087)	(0.070)
Web Usage	-0.033	-0.139†	-0.139†	-0.051
	(0.065)	(0.082)	(0.082)	(0.057)
Breach History	0.032	0.006	0.006	-0.022
	(0.040)	(0.050)	(0.050)	(0.050)
Information Context	0.329**			
	(0.112)			
Secondary Use	-0.054	-0.042	-0.042	0.015
	(0.112)	(0.138)	(0.138)	(0.137)
Identifying Information	0.147	0.195	0.196	0.316*
	(0.113)	(0.143)	(0.143)	(0.139)
Study 1 Indicator			-0.267	
			(0.165)	
Study 2 Indicator	0.378**	0.267		
	(0.117)	(0.165)		
Study 3 Indicator		0.399*	0.132	0.311*
		(0.165)	(0.187)	(0.139)
Constant	2.866**	3.349**	3.769**	3.224**
	(0.342)	(0.455)	(0.468)	(0.587)
F-value	2.850**	1.440	1.440	2.220*
Log pseudolikelihood	-832.075	-675.572	-675.572	-651.333
Censored Observations	4 censored at 0	8 censored at 0	8 censored at 0	10 censored at 0
	95 censored at 5	82 censored at 5	82 censored at 5	127 censored at 5
	403 uncensored	301 uncensored	301 uncensored	255 uncensored

Robust standard errors in parentheses, †$p \leq 0.10$, *$p \leq 0.05$, **$p \leq 0.01$.
Average marginal effects reported for the coefficients.

[12] We also tested for interaction effects between experimental factors to determine if the increased saliency or the video affected the magnitude of the treatment effects. No interactions were statistically significant.

It is also possible that on average, participants price themselves out of the market (e.g., set WTA close to $5 to decrease the probability of selling their private information), due to increased saliency and heightened awareness of consequences. To test for this possibility, we estimated Logit regressions with a binary dependent variable indicating whether a participant entered a high WTA (i.e., greater than $4.95) or not. Table 4 displays the results. Similar to the pooled analysis in Table 3, we include an indicator variable for each study. Note the baseline study of comparison by the omitted study variable in each model. The results in Model 1 indicate that participation in Study 2 led to an increase in the likelihood of participants pricing themselves out of the market as compared to Study 1 for the student population. Model 2 indicates a significant increase in the likelihood of a WTA greater than $4.95 when comparing Study 3 to Study 1 for the student population, and Model 3 indicates a marginal increase in this likelihood between Studies 2 and 3. Model 4 indicates a significant increase in the likelihood of a WTA greater than $4.95 for the AMT population when comparing Study 3 to Study 2. Thus, these models largely support the finding that increasing the saliency of privacy factors alone (Study 2 compared to Study 1) led to a greater likelihood of a participant pricing themselves out of the market, and heightening awareness using the consequences video (Study 3 compared to Study 2) extended this effect.

Lastly, we implemented manipulation checks in the post-survey to determine if participants believed the privacy factors were risk inducing. Participants only viewed the survey items if assigned to a treatment that had external secondary use for private information or included identifying information in the disclosure. The manipulation checks were measured using a 7-point Likert-type scale ranging from significantly less risk (1) to significantly greater risk (7). We pooled the data and used t-tests to compare mean responses to the risk neutral option (i.e., neither greater nor less risk; value = 4.00). Item (1) asked "How does the inclusion of Name, Date of birth, and Email with other private information affect the risk associated with disclosing your private information?" The results show a perceived a greater risk for external secondary use (students mean = 5.69, $t = 29.32$, $p < 0.001$; AMT mean = 4.58, $t = 6.70$, $p < 0.001$). Item (2) asked "How does the knowledge that Google will provide your private information to a third party affect the risk associated with disclosing your private information?" Again, results show a

perceived greater risk if a requirement of identifying information is present in their disclosure (students mean = 5.73, $t = 30.67$, $p < 0.001$; AMT mean = 4.67, $t = 7.63$, $p < 0.001$). Based upon these results, participants perceived significant manipulation due to these factors but their heightened risk did not consistently translate to higher valuations.

Table 4: Logit Pricing Out of Market

Context	Both		Shopping Only					
Pooled Studies	1, 2		1, 2, 3				2, 3	
Population	Students						AMT	
Variables	(1) AME	(1) OR	(2) AME	(2) OR	(3) AME	(3) OR	(4) AME	(4) OR
Gender	0.038	1.278	0.039	1.266	0.039	1.266	-0.083†	0.668†
	(0.037)	(0.302)	(0.043)	(0.332)	(0.043)	(0.332)	(0.047)	(0.150)
Age							0.039*	1.211*
							(0.020)	(0.118)
Education							0.002	1.012
							(0.018)	(0.088)
False Information	0.014	1.096	0.014	1.090	0.014	1.090	0.046*	1.251*
	(0.019)	(0.133)	(0.022)	(0.151)	(0.024)	(0.150)	(0.022)	(0.134)
Web Usage	-0.014	0.913	-0.011	0.936	-0.011	0.936	0.004	1.018
	(0.022)	(0.126)	(0.024)	(0.135)	(0.024)	(0.135)	(0.019)	(0.094)
Breach History	0.011	1.072	0.010	1.062	0.010	1.062	-0.015	0.930
	(0.012)	(0.084)	(0.014)	(0.092)	(0.014)	(0.092)	(0.016)	(0.073)
Information Context	0.058†	1.452†						
	(0.035)	(0.331)						
Secondary Use	-0.017	0.895	-0.051	0.732	-0.051	0.732	0.014	1.073
	(0.035)	(0.203)	(0.041)	(0.185)	(0.041)	(0.185)	(0.046)	(0.239)
Identifying Information	0.028	1.196	0.046	1.328	0.046	1.328	0.088*	1.533†
	(0.036)	(0.273)	(0.041)	(0.337)	(0.041)	(0.337)	(0.046)	(0.346)
Study 1 Indicator					-0.068	0.658		
					(0.055)	(0.224)		
Study 2 Indicator	0.096**	1.847*	0.068	1.519				
	(0.035)	(0.421)	(0.055)	(0.518)				
Study 3 Indicator			0.151**	2.523**	0.083†	1.661†	0.164**	2.220**
			(0.047)	(0.755)	(0.050)	(0.515)	(0.043)	(0.497)
Constant	-2.185**	0.113**	-2.080**	0.125**	-1.662*	0.190*	-2.078**	0.125**
	(0.609)	(0.069)	(0.669)	(0.142)	(0.672)	(0.128)	(0.658)	(0.082)
Wald x^2	14.060†	14.060†	15.400*	15.400*	15.400*	15.400*	29.090**	29.090**
Log Likelihood	-245.001	-245.001	-197.022	-197.022	-197.022	-197.022	-234.506	-234.506

Robust standard errors in parentheses, †$p \leq 0.10$, *$p \leq 0.05$, **$p \leq 0.01$. AME (Average Marginal Effects). OR (Odds Ratio)

5. Discussion

Overall, the consistent finding of our research is the persistence of null effects of the three common privacy disclosure factors: requiring the disclosure of personally identifying information, external secondary use of personal information, and the context of the information disclosure. With the exception of two, population-specific main effects, we largely observed null effects across multiple studies and populations. This is in contrast to prior research, which has shown that the presence of these three privacy factors can affect consumers' privacy valuations, when they are studied separately and in isolation (e.g.,

Culnan 1993; Hoffman et al. 1999; Solove 2006; Hann et al. 2007; McMillan 2014). So a question arises, why do we observe these consistent null effects? By combining these factors and requesting multiple pieces of personal information, we presented participants with a more realistic disclosure scenario than is typical in prior research. The persistence of the null effects in this scenario suggests that the effects on privacy valuations get complicated when we combine these factors in a disclosure decision. Even when we heightened participant awareness through the increased saliency and the consequences video null effects largely persisted. Thus, the complexity of the realistic scenario may make it difficult for consumers to disentangle the factors affecting the privacy disclosure, demonstrating the resilience of the privacy paradox. This is a significant finding and contribution to privacy valuation research, which poses a need for continuing research on privacy valuations in the context of complex and realistic scenarios that consider the combination of multiple disclosure factors.

Our post hoc analysis provides additional insights on how privacy valuations operate in a scenario with multiple factors. In our replication studies, we introduced increased saliency of the factors and required participants to watch a video on the risks and consequences of disclosing personal information. We used the increased saliency and consequences video as methodological checks to rule out lack of awareness as an explanation for our null effects. Thus, we did not hypothesize direct effects of these checks on overall privacy valuations. Although including these checks did not counter the null effects of the three privacy factors, we did observe average higher valuations and a higher likelihood of participants pricing themselves out of the market (i.e., stating a WTA greater than $4.95 out of $5.00) as a result. This suggests that even though the main privacy disclosure factors did not have consistent significant effects on privacy valuations, participants did react on average when awareness of privacy disclosure risks was heightened. In other words, consumers may make an all or nothing decision: they either accept or reject the disclosure opportunity when awareness is heightened, regardless of the conditions. These results provide a second important contribution to privacy valuation research and offer an opportunity for further research around saliency and awareness.

Beyond the null effects, it is also necessary to address the population-specific main effects

observed in our studies. First, requiring identifying information did have a significant effect on WTA in the AMT sample for Study 2. Prior research has shown that AMT workers in particular place a high degree of importance on the security of their personally identifiable information (Lease et al. 2013), and thus it is not surprising that we observe that main effect to be significant in our study as well. The effect does not persist to the AMT sample for Study 3, however. This is likely because the video further heightened awareness and led to an overall higher WTA and likelihood of pricing out of the market, which overcame the specific main effect of identifying information. Second, we observed a significant effect of information context in the student sample for study 2. One explanation for the result is that the increased saliency of the factors removed the lack of awareness for our participants, resulting in the manifestation of a significant effect of information context, as has been shown in the prior research. The ANCOVA results for study 2 and pooled regression analysis for studies 1 and 2 provide statistical support for this result. However, the lack of evidence in the AMT sample for study 2 and the relatively low model fit for the regression analysis of the student sample in study 2 provide evidence to the contrary. Thus, we have observed only marginal and inconsistent support for the effect of information context on privacy valuation and cannot rule out the possibility that the observed effect is simply due to chance. This inconsistency provides additional evidence that incorporating multiple factors into a privacy disclosure decision complicates effects beyond what prior research has observed by studying factors in isolation.

Legal scholars and policy makers often use the findings from studies on privacy tradeoffs and valuations to inform judicial decisions and aid in the establishment of new precedents (Romanosky and Acquisti 2009). For example, some state courts in the U.S. are considering restricting an organization's ability to gather forms of identifying information and share it with outside parties (Ribeiro 2015). Our results suggest that policy makers may also serve consumers by providing educational services focused on the benefits and consequences of disclosing private information. Policy makers may also consider requiring businesses that collect private information to provide salient descriptions of the private information they capture, their intended uses for that information, and the associated risks involved.

We acknowledge that our research is not without limitations. The consistent use of Google in all

of our studies provides experimental control and suggests the results may be generalizable for large well-known firms but not necessarily new players. It is possible, however, that participants will react differently to unknown or fictitious focal organizations and exhibit differing privacy valuations because of the organization. It is also possible that participants will have mixed reactions or biases about other well-known firms such as Amazon or Apple, Inc. Therefore, future studies should consider investigating the degree to which changing the organization in the disclosure decision affects a privacy valuation.

Another possible limitation of our research is the use of a specified range of $0 - $5 for WTA. We chose this range because it reflects current market prices and our interest in the changes in relative value of a participant's WTA due to the factors we manipulated. We account for any potential censoring of the data due to the range of WTA values by using Tobit regressions. Further, none of our participants reported dissatisfaction with the price range in our post hoc survey. Future work could modify the range of WTA values and consider how the specified price interval affects WTA in privacy valuations. However, we suspect that any observed differences would likely be due to anchoring effects (e.g., Tversky and Kahneman 1974) and not privacy factors.

6. Conclusion

We have demonstrated that participants' privacy valuations are largely unaffected by requiring the disclosure of personally identifying information, the information context, and the intended secondary use of the disclosed information, when these factors are combined in an online disclosure decision. These results contrast with prior research, which has shown these factors to have significant effects on privacy valuations when studied in isolation. Our results were robust across three experiments and used incentive compatible techniques from experimental economics across two separate samples (students and Amazon Mechanical Turk). We did find that increasing the saliency of privacy factors in the disclosure and highlighting the consequences of disclosing private information increases privacy valuations. Our results offer useful implications for consumers, organizations that capture consumer information, and policy makers seeking to improve consumers' privacy protections. Overall, the complexity of dimensions involved in disclosure decisions demonstrates the continued challenges arising from the privacy paradox.

References

Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in *Proceedings of the Fifth ACM Conference on Electronic Commerce,* Breese, J., Feigenbaum, J., and Seltzer, M. (eds.), pp. 21-29.

Acquisti, A., & Gross, R. 2006. "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *Privacy enhancing technologies*, Springer Berlin Heidelberg, pp. 36-58

Acquisti, A. and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security and Privacy* (2), pp. 24-30.

Acquisti, A., Leslie, J. K., and Loewenstein, G. 2013. "What is Privacy Worth?," *The Journal of Legal Studies* (42:2), pp. 249-274.

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), pp. 509-514.

Angst, C. M., and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339-370.

Balebako, R., Schaub, F., Adjerid, I., Acquisti, A., and Cranor, L.F. 2015. "The Impact of Timing on the Salience of Smartphone App Privacy Notices," *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*.

Barnes, S. B. 2006. "A privacy paradox: Social networking in the United States," *First Monday*, 11(9).

Becker, G. M., DeGroot, M. H., and Marschak, J. 1964. "Measuring utility by a single-response sequential method," *Behavioral Science* (9:3), pp. 226-232.

Berendt, B., Gunther, O., and Spiekermann, S. 2005. "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior," *Communications of the ACM* (48:4), pp. 101-106.

Bever, Lindsey. 2018. "Why Apple co-founder Steve Wozniak is joining the #DeleteFacebook movement," Washington Post, published April 9th. Available online: https://www.washingtonpost.com/news/the-switch/wp/2018/04/09/why-apple-co-founder-steve-wozniak-is-joining-the-deletefacebook-movement/?utm_term=.23fd8cffcf64

Burke, A. J. 2015. "Data, Data Everywhere, But Not a Bit Your Own," *Huffington Post,* June 25.

Caudill, E. M., and Murphy, P. E. 2000. "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing* (19:1), pp. 7-19.

Chellappa, R. K., and Sin, R. G. 2005. "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6:2-3), pp. 181-202.

Compeau, D., Marcolin, B., Kelley, H., and Higgins, C. 2012. "Generalizability of Information Systems Research Using Student Subjects – A Reflection on Our Practices and Recommendations for Future

Research," *Information Systems Research* (23:4), pp. 1093-1109.

Coursey, D. L., Hovis, J. L., and Schulze, W. D. 1987. "The Disparity between Willingness to Accept and Willingness to Pay Measures of Value," *The Quarterly Journal of Economics*, pp. 679-690.

Culnan, M. J. 1993. "How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly* (17:3), pp. 341-363.

Culnan, M. J., and Armstrong, P. K. 1999. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science* (10:1), pp. 104-115.

Cvrcek, D., Kumpost, M., Matyas, V., and Danezis, G. 2006. "A Study on the Value of Location Privacy," in *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, pp. 109-118.

Danezis, G., Lewis, S., and Anderson, R. J. 2005. "How Much is Location Privacy Worth?" in *Workshop on the Economics of Information Security* (5).

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Transactions Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Donaldson, C., Jones, M. A., Mapp, J. T., and Olson, A. J. 1998. "Limited Dependent Variables in Willingness to Pay Studies: Applications in Health Care," *Applied Economics* (30:5): pp. 667-677.

Druckman, J., and Kam, C. 2009. "Students as Experimental Participants: A Defense of the "Narrow Data Base"," *Institute for Policy Research Northwestern University Working Paper Series,* WP-09-05 Available at papers.ssrn.com/sol3/papers.cfm?abstract_id=1498843.

Feldman, B. 2017. "The Unroll.me Controversy Is a Good Reminder That Tech Companies and Consumers Don't Understand Each Other," New York Magazine, April 26th, Available online at: http://nymag.com/selectall/2017/04/unroll-mes-lesson-legal-ass-covering-isnt-enough.html. Last Accessed April 27, 2017.

Flaherty, A. 2013. "Americans Growing More Concerned Over Their Online Privacy: Study" *Huffington Post*, November 5.

Hanemann, W. M. 1991. "Willingness to Pay and Willingness to Accept: How Much Can They Differ?," *The American Economic Review* (81:3), pp. 635-647.

Hann, I., Hui, K., Lee, S. T., and Png, I. 2007. "Overcoming Information Privacy Concerns: An Information Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13-42.

Hoffman, D. L., Thomas, P. N., and Marcos, P. 1999. "Building Consumer Trust Online," *Communications of the ACM* (42:4), pp. 80-85.

Huberman, B. A., Adar, E., and Fine, L. 2005. "Valuating Privacy," *IEEE Security and Privacy* (3:5), pp. 22-25.

Hui, K., Teo, H. H., and Lee, S. T. 2007. "The Value of Privacy Assurance: An Exploratory Field

Experiment," *MIS Quarterly* (31:1) pp. 19-33.

Julesz, B. 1995. "Dialogues on Perception," MIT Press.

Kadir, T., and Brady, M. 2001. "Saliency, Scale, and Image Description," *International Journal of Computer Vision* (45:2), pp. 83-105.

Klopfer, P. H., and Rubenstein, D. I. 1977. "The Concept of Privacy and Its Biological Basis," *Journal of Social Issues* (33:3), pp. 52-65.

Kroft, S. 2014. "The Data Brokers: Selling Your Personal Information," *CBS News*, August 24.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Mutlidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22-42.

Lease, M., Hullman, J., Bigham, J. P, Bernstein, M., Kim, J., Lasecki, W. S., Bakhshi, S., Mitra, T., and Miller, R. C. "Mechanical Turk Is Not Anonymous," SSRN. doi: 10.2139/ssrn.2228728.

List, J. A., and Shogren, J. F. 2002. "Calibration of Willingness to Accept," *Journal of Environmental Economics and Management* (43), pp. 219-233.

Madrigal, A.C. 2012 "How much is your data worth? Mmm somewhere between half a cent and $1,200", *The Atlantic*, published March 19, available online at: https://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730/

Malhotra, N., Kim, S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

McCallister, E., T. Grance, and K. Scarfone. 2010. "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-122.

McDonald, J. F., and Moffitt, R. A. 1980. "The Uses of Tobit Analysis," *The Review of Economics and Statistics,* pp. 318-321.

McMillan, R. 2014. "The Hidden Privacy Threat of ... Flashlight Apps," *Wired*, October 20.

Nowak, G. J., and Phelps, J. 1992. "Understanding Privacy Concerns: An Assessment of Consumer's Information-Related Knowledge and Beliefs," *Journal of Direct Marketing* (6:4), pp. 28-39.

Ohm, P. 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* (57), pp. 1701-1777.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing* (19:1), pp. 27-41.

Plott, C. R., and Zeiler, K. 2005. "The Willingness to Pay-Willingness to Accept Gap, the 'Endowment Effect,' Subject Misconceptions, and Procedures for Eliciting Valuations Experimental," *The American Economic Review* (95:3), pp. 530-545.

Posner, R. A., 1981. "The Economics of Privacy," *American Economic Review* (71), pp. 405-409.

Preibusch, S. 2015. "How to Explore Consumer's Privacy Choices with Behavioral Economics," in *Privacy in a Digital, Networked World*, S. Zeadally and M. Badra (eds.), pp. 313-341.

Ribeiro, J. 2015. "Radioshack still plans to sell customer personal data despite state objections," *PCWorld*, April 14.

Rivenbark, D. R. 2011. "Experimentally Elicited Beliefs Explain Privacy Behavior," *Working Paper.*

Romanosky, S., and Acquisti A. 2009. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives," *Berkeley Technology Law Journal* (24), pp. 1061-1102.

Shah, R. 2015. "Do Privacy Concerns Really Change With The Internet of Things?," *Forbes*, July 2.

Sheehan, K. B., and Hoy, M. G. 2000. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy & Marketing* (19:1), pp. 62-73.

Shinal, J. 2017. "Faebook's revenue per user topped $5 for the first time," *CNBC.com*. Published November 2nd, available online at: https://www.cnbc.com/2017/11/02/facebooks-revenue-topped-5-per-user-for-the-first-time.html

Shogren, J. F., Shin, S. Y., Hayes, D. J., and Kliebenstein, J. B. 1994. "Resolving differences in willingness to pay and willingness to accept," *The American Economic Review*, pp. 255-270.

Simonite, T. 2012. "What Facebook Knows" *MIT Technology Review*, June 13.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.

Solove, D. J. 2006. "Taxonomy of Privacy," *Univ. of Pennsylvania Law Review* (154:3), pp. 477-564.

Soojian, C. 2015. "Content Personalization: It's What Consumers Want!," *Social Media Today*, April 4.

Staiano, J., Oliver, N., Lepri, B., de Oliveira, R., Caraviello, M., and Sebe, N. 2014. "Money walks: a human-centric Study on the Economics of Personal Mobile Data," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 583-594.

Steel, E., Locke, C., Cadman, E. and Freese, B. 2013. "How much is your personal data worth?," *Financial Times*, June 12.

Sutanto, J., Palme, E., Tan, C., and Phang, C. W. 2013. "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *MIS Quarterly* (37:4), pp. 1141-1164.

Taylor, S. E., and Fiske, S. T. 1978. "Salience, Attention, and Attribution: Top of the Head Phenomena," *Advances in Experimental Social Psychology* (11), pp. 249-288.

Treisman, A. 1985. "Preattentive Processing in Vision," *Computer, Vision, Graphics, and Image Processing* (31:2), pp. 156-177.

Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on

Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254-268.

Tufekci, Z. 2008. "Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate?". Information, Communication & Society. 11 (4): 544–64.

Tversky, A.; Kahneman, D. 1974. "Judgment under Uncertainty: Heuristics and Biases" *Science* (185:4157): 1124-1131

Xu, H., Teo, H. H., Tan, B. C. Y., and Agarwal, R. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 137-176.

Zetlin, Minda. 2018. "Despite all the #DeleteFacebook talk, data shows we're using it more, not less," Inc. Available online: https://www.inc.com/minda-zetlin/for-all-deletefacebook-talk-data-shows-were-using-it-more-not-less.html

Relative Privacy Valuations under Varying Disclosure Characteristics

Online Appendix

Overview

Contained within this Appendix are an overview of the experiment protocol, relevant figures and tables describing each of the three studies we conducted, and additional details regarding experiment participants and empirical analyses. Figures A1 and A2 provide the experiment protocols participants completed, in order from left to right. All participants followed the same path through the protocols independent of their treatment assignment. With the exception of Study 3, participants began the experiment by reading a series of pages that created a scenario of market research by Google. Participants in Study 3 also went through these scenario pages, but prior to these pages they watched a video presentation on the consequences of disclosing private information and completed a quiz on the topics discussed in the video (viewable at https://goo.gl/X2C5lj). Tables A1, A4, and A6 demonstrate the manipulations found in the scenarios.

As regards the experiment procedure, participants were given instructions on how they may sell their private information by entering a valid WTA. Following the instructions, we quizzed participants to ensure they understood how the selling mechanism (i.e., Becker-DeGroot-Marschak procedure) operates. Participants were then given a list of sample items (Table A2) and told that they may be asked to disclose private information contained in the list or any additional private information Google may require. Following the list of sample items, participants entered their WTA between $0.00 and $5.00. Participants were prevented from continuing if an invalid WTA was entered.

Immediately after submitting their WTA, participants were informed whether their information sold. If participants sold their private information (indicated by dashed arrows), they were directed to a form that contained the list of sample items presented to them earlier. Participants had to disclose private information for each item in the form before continuing the experiment. Participants who did not sell their private information were directed to the post-experiment survey without completing a form. Lastly,

participants answered several questions on a post-experiment survey. At the end of the survey, participants were thanked for their time and informed on how they may receive payment if their private information sold.

We also conducted an a priori power analysis to determine how many participants were required per cell in our factorial design to have sufficient power for detecting at least a medium effect size with an alpha of 0.05. With three factors and two levels of each factor, a minimum participant count per cell is 20 in order to obtain a power of 0.88. The minimum cell count in Study 1 is 34 (37.5 average per cell for students), which is sufficient for a power of 0.98. The minimum cell count in Study 2 is 20 (25.25 average per cell for students; 54.5 average for AMT). Study 3 has two factors with two levels of each factor, so 35 participants are required per cell to obtain a power of 0.84. The minimum cell count in Study 3 is 32 (35 average per cell for students; 45.5 average for AMT). A post hoc power analysis for the student samples show that even with an alpha of 0.10, the power for Study 3 is approaching 0.90. Further, after pooling the studies, the post hoc power achieved is > 0.99 for detecting a medium effect at an alpha of 0.05, and > 0.90 for detecting a small effect. Overall, we are confident that we have sufficient power to detect even small effect sizes, especially given the very high p-values for our null results.

Tables A3, A5, and A7 show the text of each page participants viewed throughout the experiments. Within the text, we indicate the manipulation text from the corresponding manipulations table with brackets and italics (e.g., [*Secondary Use*]). Table A8 includes the items of our post-experiment survey. All items are measured using a 7-point Likert scale unless otherwise specified.

Participation, Opt Outs, and Incomplete Observations

We outline in Table A9 those observations that were removed from each study. As we can see by the Opt Out column, the rates of explicitly opting out are quite low, less than 2% in every case except AMT Study 3 at 3%. It appears the opt out rate does slightly increase as we increase the saliency of consequences in each study, as may be expected. We know that increasing the saliency of consequences does increase the WTA, and that the increase is greatest in Study 3. Next, we discuss the issue of incomplete observations, as that is the source of the bulk of removed observations for the student sample.

Almost all the incomplete observations are driven by limitations of the Qualtrics system used for data collection. Qualtrics records an observation each time a potential participant opens the survey. Therefore, subjects who click on the link to participate, regardless of whether they continue with the study, create a potentially incomplete observation in the data set. Upon inspection, almost all of the unfinished observations were abandoned prior to the request to sell private information. Thus, subjects were assigned to a treatment but did not advance to a point in which they could tease out the purpose of the study. Also, incomplete observations may occur for a multitude of reasons. For example, students may start the study and then become distracted, click on a recruitment link in email using a phone and then later click the link for a second time on a computer, or a participant may have uncertainty if he/she wants to participate at all. In contrast to the student sample, we believe the AMT workers intend to participate in the study once it is started so that their time is used efficiently.

Last, we consider those that failed the attention and/or manipulation checks. We report a bulk rate of ~20-25% removed observations but after removing the incomplete and opt out observations, the percentage of participants that failed attention and/or manipulation checks is less than 9% for students. Regarding AMT, the difference between Study 2 and Study 3 is driven by eight participants that did not play the entire video. Therefore, only 4 of the 12 participants failed the attention or manipulation checks in similar ways for AMT Study 3, putting the rate percentage of observations at 2.00%, which is almost identical to the 1.78% rate for AMT Study 2. Also, instead of implementing attention questions for the AMT workers, we instead used time checking for each page to discover fraudulent workers (e.g., bot workers). If a worker spent a significantly smaller amount of time on the page than the average, we flagged the observation for later review. Any flagged AMT observation was dropped from the study during review if the worker completed the study in an impossibly fast amount of time.

A further breakdown of participants removed from each study is shown by Table A10. There are not any clear indications of differences in participation rates between treatments, and there seems to be no repeatable pattern between the invasiveness of the treatment groups and the incomplete responses and/or failed attention or manipulation checks. For example, in Student Study 1, the group with the highest failed

attention checks has medical context with no secondary use but with identifying information, whereas in Student Study 2, the medical context with secondary use but not identifying information is highest. A similar situation occurs for incompletes, where Student Study 1 has the highest number of incompletes for medical non secondary use non identifying, but Student Study 2 has medical secondary use identifying with the largest number of incompletes. In addition, the overall results are consistent between the Student population and the AMT population, and the AMT population also has fewer dropped observations. The overall breakdown of participants gives us confidence in our random assignment of participants to treatments and effectiveness of experimental manipulation.

Details Regarding Empirical Analysis

To address heteroscedasticity in Study 3 for the AMT sample, we estimated two additional models. The first model estimated is Generalized Method of Moments (GMM) due to its ability to generate efficient parameter estimates in the presence of heteroscedasticity (Baum et al. 2003). We also estimated a Symmetrically Trimmed Least Squares (STLS) model, based upon the ability for STLS estimators to address heteroscedasticity in the Tobit model (Powell 1986). Results are shown in Table A11 and are qualitatively consistent with the Tobit regressions already presented in the paper.

Tables and Figures

Figure A1: Study 1 and Study 2 Experiment Protocol

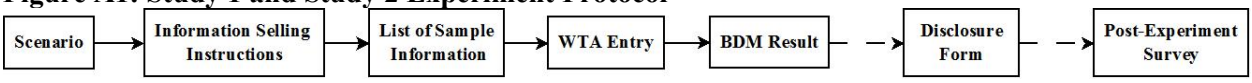

Figure A2: Study 3 Experiment Protocol

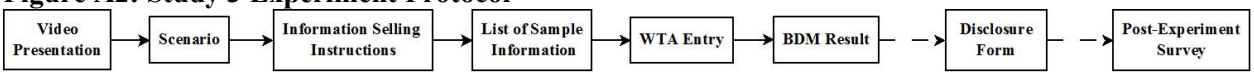

Table A1: Study 1 Manipulations

Information Context	
Medical	medical history
Shopping	shopping preferences
Secondary Use	
Secondary Use	will distribute the information you provide to outside marketing and advertising agencies for various purposes

No Secondary Use	will not distribute information to any third parties. The information will be for internal application use only
Identifying Information	
Identifying Information	will store identifying information, such as name, email, and phone number, with the medical information you provide
No Identifying Information	will not store identifying information, such as name, email, and phone number, with the medical information you provide

Table A2: List of Sample Information Items

Medical	Shopping
Allergies	Frequent Retail Stores
Illnesses	Frequent Purchases
Diseases	Recent Purchase History
Family History	Preferred Shipping Method
Sexual Activity	Product Attributes
Smoking Habits	Preferred Method of Payment
Drug Use	Frequent E-commerce Websites
Alcohol Use	Common Grocery Purchases
Blood Type	Mobile App Purchases

Table A3: Study 1 Outline

Page 1

Welcome

The following is a study on the valuation of information. Google Inc. is currently developing a new [*Information Context*] application. **Google Inc. wishes to begin paying users** for the information they provide when registering for the application. However, Google Inc. does not know how much to compensate users for their information. In order to capture an appropriate compensation value, we will ask you to enter your selling value for **ALL** of your medical information. **The value entered must be between $0.00 and $5.00.** Throughout the study, we will refer to this value as your selling price.

It is important to note that Google Inc. [*Secondary Use*].

The application Google Inc. is developing will require users to enter [*Information Context*] information about themselves. A sample of the information Google Inc. may request appears later. Due to a nondisclosure agreement with Google Inc., we cannot disclose the specifics of the new application. However, the application will provide a quality service for its users.

You may opt out of this study at any time.

Page 2

Information Selling Instructions

After viewing the list of information Google Inc. may request, you have two options.

1. You may enter your selling price for the information Google Inc. requests. **Remember that the value entered is your selling price for all of your information, not individual pieces.**
2. You may opt out if you do not wish to participate or if your selling price is greater than $5.00. A opt

out option is available on the selling price page. If you choose to opt out, you must provide a reason for doing so.

If you choose to participate and enter a selling price then you will type your selling value into a text box. The value must be between $0.00 and $5.00 and in the format X.XX. The following occurs after you submit your selling price:

Google Inc.'s information buying algorithm calculates a buying price between $0.00 and $5.00.

If Google Inc.'s buying price is greater than or equal to your selling price, you will sell your information to Google Inc. for the buying price and must provide the information Google Inc. requests. If Google Inc.'s buying price is less than your selling price, you will not sell your information and do not provide your information to Google Inc.

Example 1:
Your selling value is $1.00, Google Inc. buying price is $2.50 ⇒ You will sell your information for $2.50.

Example 2:
Your selling value is $3.00, Google Inc. buying price is $2.00 ⇒ You will **NOT** sell your information.

Example 3:
Your selling value is $2.50, Google Inc. buying price is $2.50 ⇒ You will sell your information for $2.50.

You will receive course credit for participating in this experiment and finishing the survey at the end. If you sell your information to Google Inc., you will receive the course credit and the buying price. If you do not sell your information to Google Inc. or choose to opt out, you will only receive the course credit.

****IMPORTANT****
Before you receive your payment from Google Inc., Google Inc. will verify the information you provide for truthfulness.

Page 3

Information Selling Instructions

We will now demonstrate how pricing works. It is in your best interest to accurately state your true valuation as your selling price for your information. The following are two examples of why:

Example 1: What happens if your stated selling price is HIGHER than your true value:
Imagine you value your information at $3.00, but you enter a selling value of $4.50. We will say that the Google Inc. buying price is $4.25.

Since the buying price, $4.25, is less than your selling price, $4.50, you will not sell the information to Google Inc. and will not earn the $4.25. Therefore, you will miss the opportunity to sell your information for a price you deem as reasonable.

Example 2: What happens if your stated selling price is LOWER than your true value:

Imagine you value your information at $1.75, but you enter a selling value of $0.75. We will say that the Google Inc. buying price is $1.00.

Due to your selling price being lower than the Google Inc. buying price, you must sell your information to Google Inc., even though you value the information much more than the $1.00 you will receive. You will forfeit your information for less than what you think it is worth.

Page 4

Information Selling Instructions Quiz

Before proceeding, we wish to ensure you understand all of the instructions clearly. Below are four example scenarios, please choose the best answers to the questions:
Scenario 1: Your stated selling value is $1.50. The Google Inc. buying price is $2.50. What will happen next?

- You will not sell your information or complete the form
- You will sell your information for $1.50 and complete the form
- You will sell your information for $2.50 and complete the form

Scenario 2: Your stated selling value is $1.50. The Google Inc. buying price is $1.00. What will happen next?

- You will not sell your information or complete the form
- You will sell the information for 0.50 and complete the form
- You will sell the information for 1.50 and complete the form

Scenario 3: Google Inc.'s buying price is $0.75 and your selling value is $0.25. What must you do after winning?

- Do not complete the information form
- The information sells so you must complete the information form

Is the Google Inc. buying price (and your selling value) based on each individual piece of information or all information on the form?

- Each individual piece of information
- All information on the form

Page 5

Thank you for completing the tutorial.

The following page will request your selling value for your medical information. Below, we provide a brief list of possible information items Google Inc. will request. This list is not comprehensive and Google Inc. reserves the right to request [*Information Context*] that is not shown below.

Please be aware that Google Inc. [*Identifying Information]*

[*List of Medical/Shopping Information Items]*

Page 6

Enter a selling value between $0.00 and $5.00, in the format X.XX, for the information presented in the sample form.

If you wish to opt out of the study, you may do so. To opt out please select the Opt Out option and click >>.

Opt Out

Page 7 (if information was sold)

SOLD!

Your value, $[*participant's WTA*], is less than the randomly drawn value, $[*system generated WTA*]. Therefore, you will earn an additional $[*Random WTA minus the WTA entered*] at the end of this experiment. Please proceed to the next page and enter the requested information.

Page 7 (if information was not sold)

NO SALE

Unfortunately your selling price, $[*participant's WTA*] was greater than the randomly drawn value, $[*system generated WTA*]. You are not required to enter your information. Please proceed to the next page.

Table A4: Study 2 Manipulations

Information Context	
Medical	***medical history***
Shopping	***shopping history***
Secondary Use	
Secondary Use	***will distribute the information you provide to outside marketing and advertising agencies for various purposes***
No Secondary Use	***will not distribute information to any third parties. The information will be for internal application use only***
Identifying Information	
Identifying Information	***will store identifying information, such as name, email, and phone number, with the medical information you provide***
No Identifying Information	***will not store identifying information, such as name, email, and phone number, with the medical information you provide***

Table A5: Study 2 Outline

Page 1
Welcome

Google Inc. is currently developing a new [Information Context] application and wishes to pay its users for the information they provide when registering for the application. However, Google Inc. does not know how much to compensate users for their information. In order to capture an appropriate compensation value, we will ask you to enter your selling value for ***your [Information Context]***. The value entered must be between $0.00 and $5.00. This value will be referred to as your selling price.

The application Google is developing will require users to enter [*Information Context*] about themselves. A sample of the information Google Inc. may request appears later. Due to a nondisclosure agreement with Google Inc., we cannot disclose the specifics of the new application. However, the application will provide a quality service for its users.

You may opt out of participation at any time.

Page 2

Welcome

We must inform you that ***Google Inc. [Secondary Use]*** Disclosing your information represents consent for Google Inc. to share the information with other [*medical/advertising*] companies.

Page 3

Welcome

Shown below is a brief list of possible information items you will provide when registering for an account. In addition to [*Information Context*], ***you [Identifying Information]***. This list is not comprehensive and Google Inc. reserves the right to request [*Information Context*] that is not shown below.

[*List of Medical/Shopping Information Items*]

Page 4

Welcome

In summary, Google Inc. is creating a new application in which
Users *provide* [*Information Context*]
Google [*Secondary Use*]
Users provide [*Identifying Information*]

Compensation for your information can fall between $0.00 and $5.00. You may opt out at any time by closing your web browser.

Page 5

Information Selling Instructions

****IMPORTANT**** Before you receive your payment from Google Inc., Google Inc. will verify the information you provide for truthfulness.

After viewing the list of information Google Inc. may request, you have two options.

1. You may enter your selling price for the information Google Inc. requests. **Remember that the value entered is your selling price for all of your information, not individual pieces.**
2. You may opt out if you do not wish to participate or if your selling price is greater than $5.00. A opt out option is available on the selling price page. If you choose to opt out, you must provide a reason for doing so.

If you choose to participate and enter a selling price then you will type your selling value into a text box. The value must be between $0.00 and $5.00 and in the format X.XX. The following occurs after you submit your selling price:

Google Inc.'s information buying algorithm calculates a buying price between $0.00 and $5.00.

If Google Inc.'s buying price is greater than or equal to your selling price, you will sell your information to Google Inc. for the buying price and must provide the information Google Inc. requests. If Google Inc.'s buying price is less than your selling price, you will not sell your information and do not provide your information to Google Inc.

Example 1:
Your selling value is $1.00, Google Inc. buying price is $2.50 ⇒ You will sell your information for $2.50.

Example 2:
Your selling value is $3.00, Google Inc. buying price is $2.00 ⇒ You will **NOT** sell your information.

Example 3:
Your selling value is $2.50, Google Inc. buying price is $2.50 ⇒ You will sell your information for $2.50.

You will receive course credit for participating in this experiment and finishing the survey at the end. If you sell your information to Google Inc., you will receive the course credit and the buying price. If you do not sell your information to Google Inc. or choose to opt out, you will only receive the course credit.

Page 6

Information Selling Instructions

We will now demonstrate how pricing works. It is in your best interest to accurately state your true valuation as your selling price for your information. The following are two examples of why:

Example 1: What happens if your stated selling price is HIGHER than your true value:
Imagine you value your information at $3.00, but you enter a selling value of $4.50. We will say that the Google Inc. buying price is $4.25.

Since the buying price, $4.25, is less than your selling price, $4.50, you will not sell the information to Google Inc. and will not earn the $4.25. Therefore, you will miss the opportunity to sell your information for a price you deem as reasonable.

Example 2: What happens if your stated selling price is LOWER than your true value:

Imagine you value your information at $1.75, but you enter a selling value of $0.75. We will say that the Google Inc. buying price is $1.00.

Due to your selling price being lower than the Google Inc. buying price, you must sell your information to Google Inc., even though you value the information much more than the $1.00 you will receive. You will forfeit your information for less than what you think it is worth.

Page 7

Information Selling Instructions Quiz

Before proceeding, we wish to ensure you understand all of the instructions clearly. Below are four example scenarios, please choose the best answers to the questions:
Scenario 1: Your stated selling value is $1.50. The Google Inc. buying price is $2.50. What will happen next?

- You will not sell your information or complete the form
- You will sell your information for $1.50 and complete the form
- You will sell your information for $2.50 and complete the form

Scenario 2: Your stated selling value is $1.50. The Google Inc. buying price is $1.00. What will happen next?

- You will not sell your information or complete the form
- You will sell the information for 0.50 and complete the form
- You will sell the information for 1.50 and complete the form

Scenario 3: Google Inc.'s buying price is $0.75 and your selling value is $0.25. What must you do after winning?

- Do not complete the information form
- The information sells so you must complete the information form

Is the Google Inc. buying price (and your selling value) based on each individual piece of information or all information on the form?

- Each individual piece of information
- All information on the form

Page 8

Enter a selling value between $0.00 and $5.00, in the format X.XX, for the information presented in the sample form.

If you wish to opt out of the study, you may do so. To opt out please select the Opt Out option and click >>.

○ Opt Out

Page 9 (if information was sold)
SOLD! Your value, $[*participant's WTA*], is less than the randomly drawn value, $[*system generated WTA*]. Therefore, you will earn an additional $[*Random WTA minus the WTA entered*] at the end of this experiment. Please proceed to the next page and enter the requested information.

Page 9 (if information was not sold)
NO SALE Unfortunately your selling price, $[*participant's WTA*] was greater than the randomly drawn value, $[*system generated WTA*]. You are not required to enter your information. Please proceed to the next page.

Table A6: Study 3 Manipulations

Secondary Use	
Secondary Use	will distribute the information you provide to outside marketing and advertising agencies for various purposes
No Secondary Use	will not distribute information to any third parties. The information will be for internal application use only
Identifying Information	
Identifying Information	will store identifying information, such as name, email, and phone number, with the shopping information you provide
No Identifying Information	will not store identifying information, such as name, email, and phone number, with the shopping information you provide

Table A7: Study 3 Outline

Page 1
Before you begin, please watch the brief video below. Following the video, you will be asked several questions regarding its content. [*Embedded video*]

Page 2 (Video quiz)
Online businesses are able to perform _____ (varying the price of a product according to who the buyer is), with the information they obtain from consumers. ○ Price matching ○ Price equity ○ Price discrimination ○ Fair pricing

Advertising agencies are capable of targeting unwanted advertisements with the information they are able to obtain.

- True
- False

With the distribution of private information to third parties, there are more targets for hackers and identity thieves to attack. Thus, people experience an increased chance of experiencing _____.

- Harm
- Inconvenience
- Both harm and inconvenience

Sharing private information over the Internet leads to greater vulnerability to which of the following events?

- Identity theft
- Hacked online accounts
- Data loss
- All of the above

Which of the following is considered identifying information and can magnify the effects of a security breach?

- Full name
- Shopping habits
- Hobbies
- Special interests

Page 3

Welcome

Google Inc. is currently developing a new shopping application and wishes to pay its users for the information they provide when registering for the application. However, Google Inc. does not know how much to compensate users for their information. In order to capture an appropriate compensation value, we will ask you to enter your selling value for ***your shopping information***. The value entered must be between $0.00 and $5.00. This value will be referred to as your selling price.

The application Google is developing will require users to enter shopping information about themselves. A sample of the information Google Inc. may request appears later. Due to a nondisclosure agreement with Google Inc., we cannot disclose the specifics of the new application. However, the application will provide a quality service for its users.

You may opt out of participation at any time.

Page 4

Welcome

We must inform you that ***Google Inc. [Secondary Use]*** Disclosing your information represents consent for Google Inc. to share the information with other advertising and marketing companies.

Page 5

Welcome

Shown below is a brief list of possible information items you will provide when registering for an account. In addition to the shopping information, ***you [Identifying Information]***. This list is not comprehensive and Google Inc. reserves the right to request shopping information that is not shown below.

[*List of Shopping Information Items*]

Page 6

Welcome

In summary, Google Inc. is creating a new application in which
Users *provide shopping information*
Google *[Secondary Use]*
Users provide [*Identifying Information*]

Compensation for your information can fall between $0.00 and $5.00. You may opt out at any time by closing your web browser.

Page 7

Information Selling Instructions

****IMPORTANT**** Before you receive your payment from Google Inc., Google Inc. will verify the information you provide for truthfulness.

After viewing the list of information Google Inc. may request, you have two options.

1. You may enter your selling price for the information Google Inc. requests. **Remember that the value entered is your selling price for all of your information, not individual pieces.**
2. You may opt out if you do not wish to participate or if your selling price is greater than $5.00. A opt out option is available on the selling price page. If you choose to opt out, you must provide a reason for doing so.

If you choose to participate and enter a selling price then you will type your selling value into a text box. The value must be between $0.00 and $5.00 and in the format X.XX. The following occurs after you submit your selling price:

Google Inc.'s information buying algorithm calculates a buying price between $0.00 and $5.00.

If Google Inc.'s buying price is greater than or equal to your selling price, you will sell your information to Google Inc. for the buying price and must provide the information Google Inc. requests. If Google Inc.'s buying price is less than your selling price, you will not sell your information and do not provide your information to Google Inc.

Example 1:
Your selling value is $1.00, Google Inc. buying price is $2.50 ⇒ You will sell your information for $2.50.

Example 2:
Your selling value is $3.00, Google Inc. buying price is $2.00 ⇒ You will **NOT** sell your information.

Example 3:
Your selling value is $2.50, Google Inc. buying price is $2.50 ⇒ You will sell your information for $2.50.

You will receive course credit for participating in this experiment and finishing the survey at the end. If you sell your information to Google Inc., you will receive the course credit and the buying price. If you do not sell your information to Google Inc. or choose to opt out, you will only receive the course credit.

Page 8

Information Selling Instructions

We will now demonstrate how pricing works. It is in your best interest to accurately state your true valuation as your selling price for your information. The following are two examples of why:

Example 1: What happens if your stated selling price is HIGHER than your true value:
Imagine you value your information at $3.00, but you enter a selling value of $4.50. We will say that the Google Inc. buying price is $4.25.

Since the buying price, $4.25, is less than your selling price, $4.50, you will not sell the information to Google Inc. and will not earn the $4.25. Therefore, you will miss the opportunity to sell your information for a price you deem as reasonable.

Example 2: What happens if your stated selling price is LOWER than your true value:
Imagine you value your information at $1.75, but you enter a selling value of $0.75. We will say that the Google Inc. buying price is $1.00.

Due to your selling price being lower than the Google Inc. buying price, you must sell your information to Google Inc., even though you value the information much more than the $1.00 you will receive. You will forfeit your information for less than what you think it is worth.

Page 9

Information Selling Instructions Quiz

Before proceeding, we wish to ensure you understand all of the instructions clearly. Below are four example scenarios, please choose the best answers to the questions:

Scenario 1: Your stated selling value is $1.50. The Google Inc. buying price is $2.50. What will happen next?

- You will not sell your information or complete the form
- You will sell your information for $1.50 and complete the form
- You will sell your information for $2.50 and complete the form

Scenario 2: Your stated selling value is $1.50. The Google Inc. buying price is $1.00. What will happen next?

- You will not sell your information or complete the form
- You will sell the information for 0.50 and complete the form
- You will sell the information for 1.50 and complete the form

Scenario 3: Google Inc.'s buying price is $0.75 and your selling value is $0.25. What must you do after winning?

- Do not complete the information form
- The information sells so you must complete the information form

Is the Google Inc. buying price (and your selling value) based on each individual piece of information or all information on the form?

- Each individual piece of information
- All information on the form

Page 10

Enter a selling value between $0.00 and $5.00, in the format X.XX, for the information presented in the sample form.

If you wish to opt out of the study, you may do so. To opt out please select the Opt Out option and click >>.

- Opt Out

Page 11 (if information was sold)

SOLD!

Your value, $[*participant's WTA*], is less than the randomly drawn value, $[*system generated WTA*]. Therefore, you will earn an additional $[*Random WTA minus the WTA entered*] at the end of this experiment. Please proceed to the next page and enter the requested information.

Page 11 (if information was not sold)

NO SALE

Unfortunately your selling price, $[*participant's WTA*] was greater than the randomly drawn value, $[*system generated WTA*]. You are not required to enter your information. Please proceed to the next page.

Table A8: Post-Experiment Survey Items

Demographics
Sex
Age
Highest level of education
Average daily Internet usage
Some websites ask you to register with the website by providing personal information. When asked for such information, how often do you falsify the information? (5-point Likert scale)
How frequently have you personally been the victim of what you felt was an improper invasion of privacy?
Additional Measures
Do you trust Google Inc. to follow through with what they tell consumers?
How does the inclusion of Name, Date of birth, and Email with other private information affect the risk associated with disclosing your private information?
How does the knowledge that Google Inc. will provide your private information to a third party affect the risk associated with disclosing your private information?

**All items use a 7-point Likert-type scale unless otherwise specified.

Table A9: Breakdown of participants removed from each study (percentage of total observations are shown in parentheses)

Population	Study	Total Obs	Failed Attention or Manipulation Checks	Incomplete	Opt Out	Usable Obs
Student	1	394	26 (6.60%)	66 (16.75%)	2 (0.51%)	300 (76.14%)
Student	2	270	23 (8.52%)	41 (15.19%)	4 (1.48%)	202 (74.81%)
Student	3	175	12 (6.86%)	20 (11.43%)	3 (1.71%)	140 (80.00%)
AMT	2	450	8 (1.78%)	0	6 (1.33%)	436 (96.89%)
AMT	3	200	12 (6.00%)	0	6 (3.00%)	182 (91.00%)

Table A10: Breakdown of participants removed from each study by treatment

Population	Study	Total Obs	Failed Attention or Manipulation Checks	Incomplete	Opt Out	Usable Obs
Student	**1**	**394**	**26**	**66**	**2**	**300**
Med-SU-Id		47	4	8	2	33
Med-No SU-Id		57	7	7	0	43
Med-SU-No Id		52	3	9	0	40
Med-No SU- No Id		46	1	10	0	35
Shop-SU-Id		50	3	8	0	39
Shop-No SU-Id		48	1	9	0	38
Shop-SU-No Id		47	5	7	0	35
Shop-No SU-No Id		47	2	8	0	37

Student	**2**	**270**	**23**	**41**	**4**	**202**
Med-SU-Id		33	3	7	2	21
Med-No SU-Id		36	1	8	0	27
Med-SU-No Id		39	5	6	1	27
Med-No SU- No Id		36	4	6	1	25
Shop-SU-Id		33	4	4	0	25
Shop-No SU-Id		29	2	3	0	24
Shop-SU-No Id		32	3	5	0	24
Shop-No SU-No Id		32	1	2	0	29
Student	**3**	**175**	**12**	**20**	**3**	**140**
Shop-SU-Id		44	7	3	2	32
Shop-No SU-Id		44	2	6	0	36
Shop-SU-No Id		41	1	5	1	34
Shop-No SU-No Id		46	2	6	0	38
AMT	**2**	**450**	**8**	**0**	**6**	**436**
Med-SU-Id		61	0	0	3	58
Med-No SU-Id		52	2	0	1	49
Med-SU-No Id		65	0	0	0	65
Med-No SU- No Id		55	1	0	0	54
Shop-SU-Id		53	2	0	2	49
Shop-No SU-Id		58	0	0	0	58
Shop-SU-No Id		55	1	0	0	54
Shop-No SU-No Id		51	2	0	0	49
AMT	**3**	**200**	**12**	**0**	**6**	**182**
Shop-SU-Id		50	2	0	2	46
Shop-No SU-Id		51	2	0	3	46
Shop-SU-No Id		51	5	0	1	45
Shop-No SU-No Id		48	3	0	0	45

Note: Med = Medical Context; Shop = Shopping Context; SU = Secondary Use; Id = Identifying Information

Table A11: AMT Study 3 Heteroscedasticity Robustness Models

	GMM		Symmetric LS	
Variables	(1)	(2)	(3)	(4)
Gender	-0.086	-0.107	-0.086	-0.107
	(0.216)	(0.216)	(0.229)	(0.229)
Age	0.081	0.089	0.081	0.089
	(0.091)	(0.096)	(0.095)	(0.100)
Education	-0.027	-0.008	-0.027	-0.008
	(0.079)	(0.080)	(0.082)	(0.084)
False Information	0.063	0.051	0.063	0.051
	(0.118)	(0.117)	(0.129)	(0.129)
Web Usage	-0.147	-0.144	-0.147	-0.144
	(0.089)	(0.088)	(0.093)	(0.092)
Breach History	-0.063	-0.082	-0.063	-0.082
	(0.076)	(0.078)	(0.081)	(0.083)
Secondary Use		-0.119		-0.119
		(0.212)		(0.226)
Identifying Information		0.318		0.318
		(0.221)		(0.233)
Constant	4.223**	4.109**	4.223**	4.109**
	(0.544)	(0.554)	(0.571)	(0.579)
Observations	182	182	182	182

Robust standard errors in parentheses, †$p \leq 0.10$, * $p \leq 0.05$, ** $p \leq 0.01$.

References

Baum, C. F., Schaffer, M. E., and Stillman, S. 2003. "Instrumental Variables and GMM: Estimation and Testing," *Stata Journal* (3:1), pp. 1-31.

Powell, J. L. 1986. "Symmetrically Trimmed Least Squares Estimation for Tobit Models," *Econometrica* (54:6), pp. 1435-1460.