Caleb S. Fuller

Is the Market for Digital Privacy a Failure?

Assistant Professor of Economics, Grove City College

Acknowledgements: I wish to thank William H.J. Hubbard, Alessandro Acquisti, Peter Leeson, Chris Coyne, Peter Boettke, David Lucas, Noah Gould, and Nicholas Freiling for helpful suggestions. All errors are my own. I am also indebted to the Mercatus Center at George Mason for providing funding for the survey conducted by Haven Insights LLC.

Conflict of Interest: Caleb S. Fuller has received funding from the Mercatus Center at George Mason University to conduct this survey. He is also a faculty affiliate at George Mason University Law School's "Program on Economics and Privacy."

Abstract

Why do many digital firms rely on collecting consumer information–a practice that survey evidence shows is widely disliked? Why don't they, instead, charge a fee that would protect privacy? This paper empirically adjudicates between two competing hypotheses. The first holds that firms pursue this strategy because consumers are ill-informed and thus susceptible to exploitation. The second holds that this strategy reasonably approximates consumer preferences. By means of survey, I test a.) the extent of information asymmetry in digital markets, b.) consumers' valuation of privacy, and c.) whether government failure contributes to consumer mistrust of information collection. My results indicate that a.) the extent of information asymmetry is minimal, b.) there is significant divergence between "notional" and "real" demand for privacy and c.) that government contributes to consumer distrust of information collection by private firms. Significantly, almost 85% of Google users are unwilling to pay anything for increased digital privacy.

Keywords: privacy paradox, digital privacy, survey, market failure

JEL-Classification: D23, K24, Z18

1 INTRODUCTION

Google's motto is "Don't Be Evil." But the fact that the company surreptitiously collects personal information from more than one billion individuals annually leads some to question whether the firm's business model runs afoul of its dictum (Hoofnagle 2009). Does information collection align with consumer preference, as argued by some (Cooper 2012), or is there a disconnect between the two, as argued by others (Strandburg 2013)?

Survey evidence reveals that consumers usually express dislike of digital information collection (Turow et al. 2009; Madden and Rainie 2015). Why then do so many firms rely on this monetization technique when they could charge visiting consumers a fee instead? One hypothesis is that companies benefit from information asymmetry and behavioral biases which enable more data collection than consumers prefer (Hoofnagle and Whittington 2013: 639). This perspective sees the relationship between information-collecting companies and consumers as exploitative (Calo 2013; Hoofnagle and Whittington 2013). Calo (2013) refers to "the exploitation of cognitive bias." Collecting personal information permits greater "personalization" of the interaction between firms and consumers which, in turn, enables firms to identify "the specific ways each individual consumer deviates from rational decision-making...and leverage that bias to the firm's advantage," (p. 1003). Acquisti (2004) agrees that consumer biases help explain the prevalence of the practice: "individuals who...would like to protect their privacy may not do so because of psychological distortions well-documented in the behavioral economics literature," (p. 7).[1]

By offering an alternative answer to the question of why so many firms collect information, I shed light on an empirical puzzle known as the "privacy paradox"–the finding that consumers often state a high privacy-valuation but subsequently forgo low-cost methods of protecting it. My resolution to the paradox does not rely on consumers being poorly informed or behaving inconsistently with their true preferences. I argue there may be no paradox at all–simply a positive preference for more of an economic good, *ceteris paribus.*

Many scholars view privacy concerns as stemming from asymmetric information (Hirsch 2010). Consumers are alleged to be ignorant of when a firm is collecting information, what information it is collecting, or to what specific uses the information will be put. Some then conclude from this that there is information over-collection relative to the ideal of perfectly-informed market participants (Hoofnagle 2005; Hirsch 2010). The market for privacy is thus a

[1] "Privacy" is difficult to define, but the complementary definitions offered by Posner (1978) and Stigler (1980) are the most amenable to economic analysis. Posner argues that privacy is the "withholding...or concealment of information," while Stigler states that privacy "...connotes the restriction of the collection or use of information about a person..." Acquisti et al. (2016) note, specifically with respect to the digital context, that: "Privacy is not the opposite of sharing–rather, it is control over sharing" (p. 445), a conception of privacy that echoes Posner's.

failure (Newman 2014).[2] Gertz (2002) also considers the digital marketplace a "classic example of a market failure" to be regulated, a position advanced by many other scholars (Solove 2004; Vila et al. 2004; Hui and Png 2005; Hermalin and Katz 2006; Sachs 2009; Turow et al. 2009; Ohm 2010; Hoofnagle et al. 2012; Strandburg 2013; Acquisti et al. 2016).[3] Solove (2004) adds that though consumers would prefer a greater level of privacy, bargaining inequity between corporations and individual consumers prevents Coasean solutions. Perhaps as a result of the market-failure perspective, some governments, most notably the EU (beginning in 1995 with an important update set to take effect in mid-2018), have enacted legislation aimed at curtailing privacy-invasive practices.[4]

Such legislation is aims to place additional parameters on the ways firms collect consumer information. Web platforms collect "non-sensitive" information directly from consumers or allow third parties (advertisers) to use the site for surreptitious information collection (Goldfarb and Tucker 2011; de Corniere and de Nijs 2016). Humorously referred to as "mouse droppings" (Berman and Mulligan 1998), non-sensitive information usually consists of device information, geographic location, browsing history, click-trail, and the like.

Probably no website collects more "mouse-droppings" than Google. In fact, most of Google's revenue (over $70 billion in 2015) is earned from third-party advertisers who pay to use the platform to track consumer behavior. While some scholars argue that personal information is merely the "price" that consumers pay in return for accessing a service that charges a zero money price (Farrell 2012; Fuller 2017), others complain that this price is difficult to observe due to lack of transparency in the exchange between consumers and firms–evidence, once again, of market failure (Strandburg 2013).

The strongest piece of evidence raised by those who see the privacy market as characterized by failure is survey evidence indicating that consumers value their privacy highly. Both non-academic research, such as Pew surveys, and academic studies suggest that most consumers prefer greater privacy in their digital interactions than they currently experience (Acquisti and Gross 2006; Turow et al. 2009; Madden and Rainie 2015; Acquisti et al. 2016: 476-478). For instance, Turow et al. (2009) show that 66% of Americans do not prefer marketers to target their offerings–but that most respondents use search engines that do just that, which suggests deception to the authors.

[2]Brown (2013) argues that there are two categories of "failure" in the digital privacy market. The first consists of "individual failures," as consumers fall prey to behavioral biases that cause them to act in ways that do not accord with their long-run preferences. The second consists of "market failures" that can be broken into two broad categories. The first is information asymmetry between firms and consumers, whereas the second is the negative externality associated with the possibility of reselling data to third parties.

[3]There is much less consensus regarding what policy interventions should look like.

[4]Japan, Canada, Singapore, and South Africa have all passed comprehensive digital privacy legislation.

Furthermore, the same study shows that 86% of "young adults" do not want to be shown ads that are a result of them being tracked across websites.[5]

One possible conclusion to draw from these findings is that markets fail to satisfy consumer preference. This conclusion would be unwarranted, however. Scholars have identified a simple, if not puzzling, "privacy paradox": consumers frequently state their preference for increased privacy, but just as frequently forgo low-cost methods of protecting the privacy that they claim to value highly (Berendt et al. 2001; Norberg et al. 2007; Acquisti et al. 2016).[6]

A potential resolution to this paradox is that consumers are making the mental trade-offs necessary to calculate the value of an additional "unit" of privacy (Acquisti et al. 2016: 476). Some scholars, however, reject this view, claiming that consumers are incapable of navigating the trade-offs inherent in digital privacy. It follows that markets may not be satisfying consumers' true preferences. For example, one states that "...issues associated with individuals' awareness of privacy challenges, solutions, and trade-offs cast doubts over the ability of market outcomes to accurately capture and reveal, by themselves, individuals' true privacy valuations," (Acquisti et al. 2016: 448). Immediate-gratification and status-quo biases may cause even well-informed individuals to allow more information collection than is in their ultimate, long-run interests (Acquisti 2004; John et al. 2011). In this view, the quantity of information collection results from some combination of information asymmetry and behavioral biases that cause behavior to deviate from true preferences to the benefit of firms and the detriment of consumers.

Using unique data from one of the largest privacy surveys in the literature, I question the perspective that the market for digital privacy is a failure. Specifically, my findings demonstrate that the extent of information asymmetry between firms and consumers has been overstated, that consumers have a high "notional" but low "real" demand for privacy, and that government action contributes to consumer dislike of private data collection policies.

Section 2 identifies specific claims in the privacy literature which lack empirical support and which are used to build the case for market failure. Section 3 discusses the need for a "constrained approach" to privacy valuation. Section 4 advances a series of related hypotheses. Section 5 details my survey design and its limitations. Section 6 discusses the empirical support for the hypotheses offered in Section 4. Section 7 concludes with a few implications.

[5]Lenard and Rubin (2009) argue that consumers derive significant benefits, such as lower search costs, from information collection.

[6]For example, consumers demonstrate a preference for the privacy-intrusive Google over the also-free search engine, DuckDuckGo, that refrains from collecting consumer information.

2 PRIVACY LITERATURE CLAIMS

To make the case that the market for digital privacy is a failure, advocates of this position advance three related claims. By empirically examining these claims, my paper contributes to a debate in the economics of digital privacy literature: is the digital marketplace a failure? While there is a longstanding tradition in economics that sees markets as primarily coordinative (Boettke 2007), this perspective contrasts with a popular view in the economics of privacy literature: that firms and consumers are fundamentally at odds (Hoofnagle et al. 2012). In what follows, I describe three claims from the economics of privacy literature, which, if true, lend weight to the argument that the digital privacy market is a failure.

Claim 1: There is widespread information asymmetry between firms and consumers. Consider the following representative statements. "Information asymmetries regarding the usage and subsequent consequences of shared information raise questions regarding individuals' abilities, as rational consumers, to optimally navigate privacy trade-offs," (Acquisti et al. 2016: 448). Hirsch (2010) states, "Those who object to a market solution [to privacy] focus on information asymmetries," (p. 455). "Privacy choices are affected by...*asymmetric information*," (Acquisti and Grossklags, 2007, p. 364, emphasis in original). Tucker (2012) concludes that, "...there is a need for empirical work that attempts to understand the extent of informational asymmetry between consumers and firms...about how much data are being collected..." (p. 328).

Claim 2: Consumers value their privacy highly. Evidence for this claim comes primarily via survey (Turow et al. 2009). For example, Turow et al. (2009) state that, "several studies...show a strong concern for internet privacy among Americans and a desire for firms not to collect information about them online," thus concluding "it seems clear...that Americans value the right to opt out from this sort of collection," (p. 10). As Turow et al. (2009) further argue: "It is hard to escape the conclusion that our survey is tapping into a deep concern by Americans that marketers' tailoring of ads for them and various forms of tracking that informs those personalizations are wrong," (p. 4). Yet, we know little regarding what the modal consumer would be willing to *sacrifice* to get additional privacy (FTC 2010).[7]

Claim 3: Consumers dislike information collection for one of four reasons, all of which are inherent features of unhampered markets. Acquisti et al. (2016) summarize these four reasons: "...price

[7]As the report states: "...consumer surveys have shown that a majority of consumers are uncomfortable with being tracked online, although the surveys provide little or no information about the degree of such discomfort or the proportion of consumers who would be willing to forego the benefits of targeted advertising to avoid being tracked," (p. 42).

discrimination...spam...risk of identity theft...[and] the disutility inherent in just not knowing who knows what," (483).[8]

This paper evaluates all three of these claims by way of new survey evidence. To date, there are few studies of consumer privacy-valuation. Notably, Acquisti et al.'s (2013) survey distinguishes between willingness to accept (WTA) payment in exchange for disclosure of information and willingness to pay (WTP) to protect otherwise publicly available information, and in so doing identify a "privacy endowment effect." As Acquisti et al. (2013) note, most empirical studies of the value of privacy focus on consumers' reservation price to disclose some piece of otherwise private information (WTA), while only Rose (2005) and Tsai et al. (2011) investigate what consumers are willing to give up in order to get privacy over otherwise public information (WTP).[9] Tsai et al. (2011) do find that, when a company makes its privacy-protective policies prominent, consumers are willing to pay a small premium for those features.

Rose (2005) finds that 47% of respondents were willing to pay to protect their privacy, but my approach differs in important ways. First, that study examined a change in the privacy legal regime, whereas mine attempts to determine WTP with respect to a company with which consumers interact frequently. Second, that study took place in New Zealand, but privacy attitudes vary across cultures (Milberg et al., 2000). Most importantly, that study was conducted over a decade ago, but privacy attitudes shift in response to changing constraints (Goldfarb and Tucker 2012; Penney 2016).

3 BACKGROUND

Privacy is an economic good in most contexts (Farrell 2012). That consumers express a preference for more of an economic good (privacy) or less of an economic bad (privacy invasion) is unsurprising. One might similarly expect that individuals would express a preference for higher incomes, lower buying prices, higher selling prices, better working conditions, and more friends, *ceteris paribus*.

Thus, it is unsurprising that consumers express this preference in surveys of privacy valuation. Consider a few representative digital privacy survey questions. Turow et al.'s (2009) survey asks questions such as: "Please tell me

[8]For the purposes of this paper, I ignore two issues with claiming that price discrimination is problematic. For one, price discrimination implies not only that some buyer faces a *higher* price, but also that some other buyer faces a *lower* price. Second, traditional economic theory demonstrates that price discrimination increases market efficiency.

[9]"...studies in which consumers are...asked to consider paying...to protect their privacy are...scarcer," (Acquisti et al. 2013: 254).

whether or not you want the websites you visit to show you ads that are tailored to your interests." Finding that a significant percentage of those polled respond negatively to queries like this one, the authors conclude that an opt-in default or time limits on data preservation should be imposed on privacy-invasive firms by governments.[10] Turow et al. (2009) also cite a survey by Westin that finds 59% of Americans were made "very uncomfortable" when posed with the following question: "How comfortable are you when...websites use information about your online activity to tailor advertisements or content to your hobbies or interests?"

A query that reveals consumers' preferences for a greater quantity of privacy protection, *ceteris paribus*, is an "unconstrained approach" to privacy valuation.[11] Unconstrained survey questions fail to remind consumers that acquiring an additional "unit" of privacy (or any scarce good) comes with an opportunity cost that they necessarily bear, and thus such an approach is not "economic" in the strictest sense, as there are no trade-offs.[12] Thus, the approach reveals the "notional" demand of individuals for privacy, but not their "real" demand.[13]

The economic approach, by contrast, necessarily asks "constrained questions."[14] This approach is superior because, for individuals choosing in the face of constraints, there are no solutions, only trade-offs. For example, a seller asking a low money-price is enabled to ask for a greater quantity of non-money equalizing differentials (Alchian 1967). In the case of Google, the firm asks a zero money-price, enabling them to collect a positive quantity of information.[15]

Because many internet platforms earn revenue (in some cases, all their revenue) by collecting information about

[10]Tucker and Goldfarb (2011) examine the economic impact of the EU's switch to an opt-in rather than an opt-out default. They find that the switch decreased the effectiveness of the average digital ad dramatically, due to the inability to target advertisements. Lerner (2012) finds that the EU rules have decreased business investment in European, ad-supported firms.

[11]Sowell (1987) describes the difference between a "constrained" and an "unconstrained" worldview.

[12]Clark and Powell (2013) confront "non-economic" approaches in the sweatshop literature. Activists often ask sweatshop workers "unconstrained questions" regarding the nature of their working conditions–conditions which are undesirable relative to average working conditions in developed nations. Unconstrained questions ask sweatshop employees whether they would prefer "better" working conditions, to which nearly 100% of respondents answer in the affirmative. Clark and Powell conduct a survey of sweatshop workers that forces respondents to consider the opportunity cost of working condition improvements. For example, they ask respondents whether they would be willing to accept reduced pay in order to be assigned more predictable hours, to which the majority respond they would not. Viscusi (1993) is also illustrative of the economic approach in that the value of life may be inferred from an individual's behavior toward risk.

[13]Note that one flaw of a survey is that it does not ascertain an individual's demonstrated preference. There may still be divergence between stated WTP and what an individual demonstrates in action. Nonetheless, the point of this investigation is determine whether there is divergence between "constrained" and "unconstrained" survey approaches.

[14]Acquisti (2005) affirms that there are both costs and benefits to disclosure of personal information.

[15]Non-money differentials may include preferences for beauty, love, discrimination and so on (Boettke and Candela 2016), but they are comprised of personal information in the case I explore.

the consumers visiting their site, such firms would be forced to rely on some alternative way of earning revenue–most likely by charging a money fee–absent the ability to collect information.[16] It follows that the economic approach would ask consumers how much they would be willing to pay to visit Google–and receive the same quality of services from Google–but without surrendering any personal information.[17]

4 HYPOTHESES

Should consumers prefer a greater level of privacy than markets currently afford, there is a profitable opportunity in exposing Google's practices and establishing alternative business models, as has been done by DuckDuckGo, a search engine that does not track browsers. Founded in 2008, DuckDuckGo advertised via a billboard in San Francisco that boldly proclaimed: "Google tracks you. We don't." Though DuckDuckGo has grown steadily, it currently averages only 10 million queries daily, far less than 1% of Google's daily traffic.[18] The fact that consumers continue to use Google indicates they have demonstrated a preference for it over more privacy-protective alternatives, such as DuckDuckGo. Of course, consumers could also refrain from all digital activity if information collection troubled them sufficiently. Physical encyclopedias are a substitute for Google search.

Perhaps in a world of fully-informed individuals, DuckDuckGo's traffic would dwarf Google's. Once again, however, we would expect this information gap to manifest as a profitable opportunity. Hence, I test individuals' level of knowledge regarding Google's information collection practices. If consumers are well-aware of the information collection, but *persist* in their demonstrated preference for services that rely on this method of monetization, it is unclear why the market for privacy is problematic or in need of a regulatory fix. Accordingly, I offer Hypothesis 1 and Corollary 1a:

Hypothesis 1: *Digital consumers are aware that digital producers collect their information.*

Corollary 1a: *Digital consumers are aware of the type of information collected.*

We would also expect relatively more frequent Google users to possess a greater awareness of the company's information collection policies. The reason is straightforward. Awareness increases positively with the cost of ignorance regarding Google's practices, a prediction in line with Becker and Rubinstein (2011). Frequent Google

[16] Another alternative is that firms are financed by non-targeted advertising, but given that these are less effective, a website earns less revenue by hosting them relative to targeted ads.

[17] As Hui and Png (2006) rightly state: "...the key issue is not whether individuals value privacy. It is obvious that people value privacy. What is not known is *how much* people value privacy," (p. 19, emphasis in original).

[18] See https://duckduckgo.com/traffic.html for statistics on DuckDuckGo's traffic over time. See http://www.internetlivestats.com/google-search-statistics/ for a daily count of Google searches.

users stand to lose more from being uninformed relative to infrequent users. This prediction stems from a rational choice framework—that costs and benefits are dictating browsers' choices—but in the digital context this framework has been repeatedly challenged by behavioral economics. Support for this prediction is thus additional support for the relevance of the rational choice framework, even in contexts where behavioral economists have argued that individuals are particularly prone to biases. Accordingly, I offer Corollary 1b:

Corollary 1b: *The responses of frequent users evince less information asymmetry.*

Though Turow et al. (2009) find that 66% of consumers are "uncomfortable" with targeted ads, I hypothesize that far fewer than 66% will be willing to pay to avoid them. This is reasonable because a "constrained" approach should elicit a lower quantity demanded for privacy than should the "unconstrained" approach. Consumers may express a (notional) demand for increased privacy when confronted with an "unconstrained" question, but may value it relatively little as measured by WTP. Though we would expect individuals to demand positive quantities of an economic good (in this case, privacy), that fact tells us nothing about the size of the opportunity cost individuals are willing to incur to acquire that good. It is likely that many individuals are unwilling to incur a significant cost to acquire more privacy. After all, billions of individuals voluntarily post pieces of personal information to social media sites, such as Facebook and Google. As an FTC (2010) report indicates, consumers are uncomfortable with data collection, but knowing that tells us little about how much they would be willing to pay to avoid that discomfort. Upon finding a divergence between "notional" and "real" demands for privacy, it is natural to investigate the size of this disparity, which my survey also addresses.

Many scholars have argued that individuals volunteering information online is no indication of a person's true preferences–that biases are causing behavior to deviate from expressed preferences. As a result, these scholars contend that consumers' demonstrated preference for privacy-invasive technologies is not sufficient evidence that they truly prefer such technologies. If this is the case, my survey should reveal that the average consumer has a large *expressed* WTP. Such a large expressed WTP would suggest divergence between behavior and "true" preferences. By contrast, if the modal Google user expresses a low WTP, this suggests "true" preferences and demonstrated preference are aligned. Accordingly, I offer Hypothesis 2:

Hypothesis 2: *A constrained approach to eliciting responses will reveal that many consumers prefer sacrificing some level of privacy to paying a pecuniary fee to digital producers.*

Several recent empirical studies find that government surveillance programs have a "chilling" effect on internet

search activity (Marthews and Tucker 2013; Penney 2016). If the threat of government surveillance constrains consumers' digital behavior, this suggests that government failure, rather than (or, at least in addition to) market failure is to blame for distrust of information collection. The business practice, by itself, may be insufficient to generate the level of discomfort expressed by consumers. Potential for government over-reach may be required to generate this level of mistrust. Accordingly, I offer Hypothesis 3:

Hypothesis 3: *A source of discomfort with digital information collection is the risk of government privacy intrusion.*

Taken together, insight into these three basic questions–the extent of information asymmetry, valuation of privacy, and the role governments play in shaping privacy expectations–can play an important role in informing digital privacy policy.

5 METHODOLOGY AND LIMITATIONS

To test these hypotheses, I conducted a survey of 1,579 randomly-selected internet users. The pool of respondents, all over age eighteen, mirrored the 2010 U.S. census on the following dimensions: ethnicity, gender, and religious affiliation. The survey was administered online intermittently between December 27, 2016 and January 11, 2017 to respondents across the U.S. (the survey's complete text can be found in the Appendix). The data are available on request. The questionnaire was programmed and administered by Haven Insights LLC and hosted at SurveyGizmo.com (Widgix, LLC). Respondents were directed to the survey by several online panel providers. Standard data quality controls were implemented, and data was cleaned post-survey to include only high-quality responses in accordance with market research industry best-practices.

It should be noted that this approach is not without limitations. First, the value of privacy differs across both cultures and contexts (Milberg et al. 2000; Rose 2005). My results generate insight into a particular context (interactions with Google) in a particular time and place (the U.S. in the year 2017). Consumers may possess different appraisals of other digital firms that collect information. Thus, my results may lack external validity. In a sense, my results represent a snapshot since individuals' views on privacy may evolve, especially in response to events with direct bearing on the privacy of one's online activities (Marthews and Tucker 2013; Penney 2016). Nonetheless, these results are sufficient to caution policymakers who assume that the market for digital privacy is necessarily a failure, and that policy measures are thus necessarily warranted.

Second, privacy is a somewhat slippery concept (Thompson 1975; Posner 1978; Berman and Mulligan 1998; Solove 2006). Survey respondents surely answer according to their own subjective interpretation of what privacy means. It is possible that survey respondents would be more (or less) sensitive to privacy concerns if an alternative conception of privacy was offered them. This also relates to the idea that privacy is contextual. A high (or low) valuation of privacy when interacting with Google does not necessarily translate to other contexts.

Third, establishing the randomness of the sample is not without difficulties. As Turow et al. (2009) have noted, those who respond to an online survey may be less privacy-sensitive than those who do not. This is a potential weakness of any privacy survey, as those volunteering responses may tend to place a lower value on excluding others from their personal information.

Fourth, it is possible that there is a significant divergence between consumers' *ex ante* and *ex post* WTP with respect to an event that alters their evaluation of privacy threats. Individuals may express a low WTP before they believe their privacy has been invaded; that WTP may increase dramatically in the wake of an event that forces them to update their expectation of privacy threats. In other words, consumers may experience regret that over not taking measures to protect privacy. As Acquisti (2014) has argued, sacrificing one's privacy may be analogous to writing a blank check insofar as it is difficult to anticipate the consequences of others accessing one's personal information. My survey does not distinguish between those who feel they have had their privacy violated and those who do not. It is possible that such a delineation would reveal different WTP between the two groups.

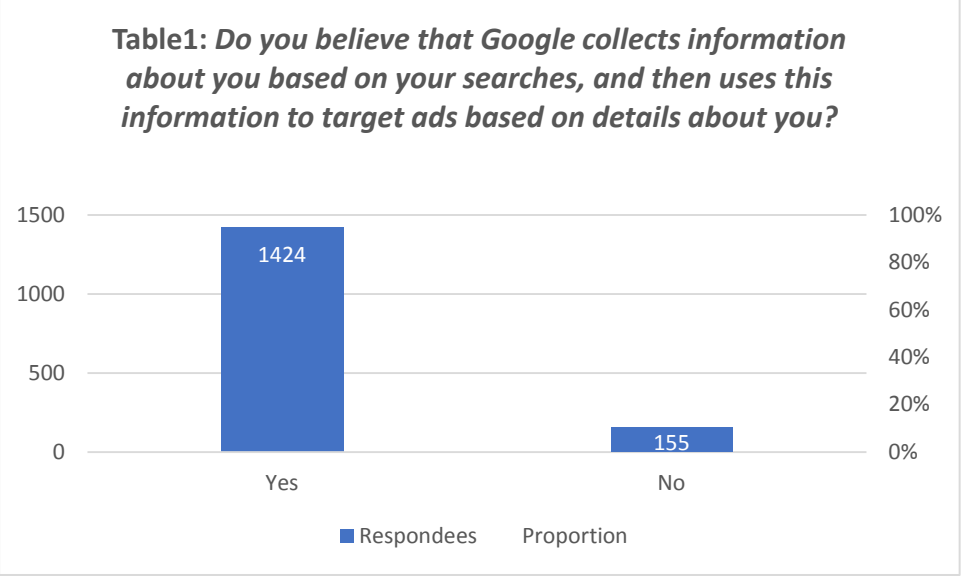
6 RESULTS AND DISCUSSION

My survey results largely confirm the hypotheses offered in Section 3. In what follows, I discuss the results in relation to each hypothesis.

Hypothesis 1: *Digital consumers are aware that digital producers collect their information.*

The survey evidence supports Hypothesis 1. Google users are overwhelmingly aware that the company collects personal information about them as they use the service. After ensuring by way of a "screener question" ("Do you make searches on Google.com") that all respondents were Google users, they were queried about their level of knowledge of Google's information-collection practices. Nine out of ten Google users are aware that the search engine collects their personal information, indicating a low degree of information asymmetry, at least regarding the *existence* of the practice. In sum, 90% of those voluntarily using Google are aware of its business practice–a practice

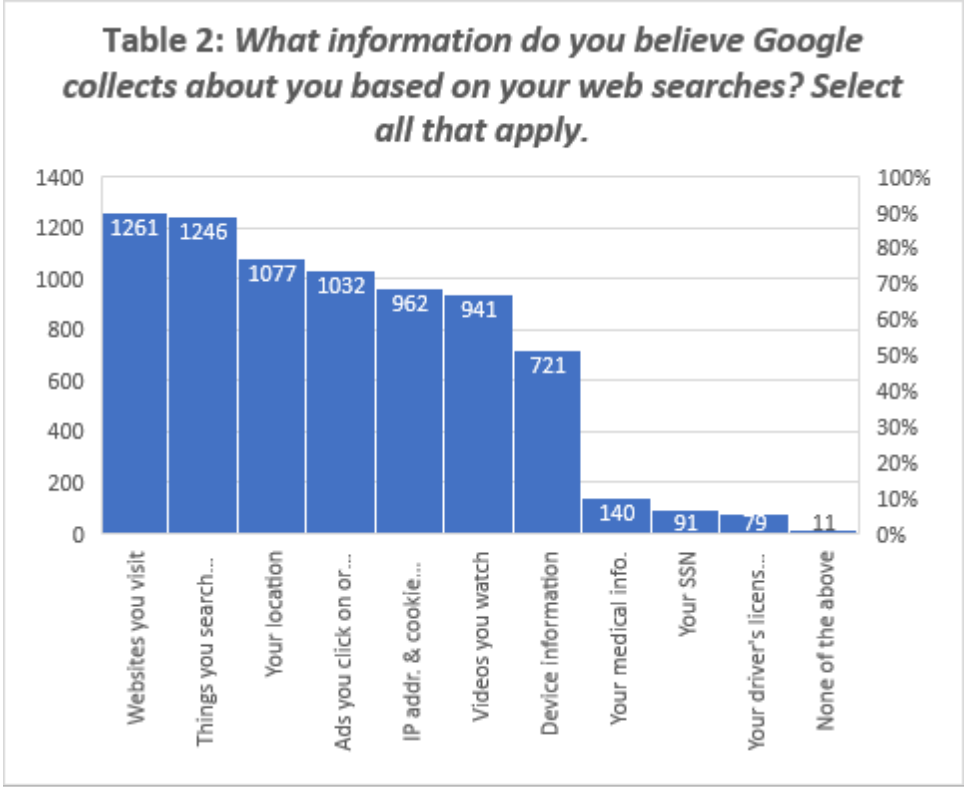
that is oft-criticized by scholars (Hoofnagle and Whittington 2013).



Corollary 1a: *Digital consumers are aware of the type of information collected.*

Following the initial question regarding consumers' awareness of data collection, respondents were presented with 11 possible pieces of data (7 accurate and 4 inaccurate), and asked to select all that Google collects. It is one thing for a respondent to be aware that some information is collected; it is quite another to possess accurate knowledge of that information. Here too, however, the data largely reveal that consumers possess a relatively high degree of understanding. Only 1% of consumers believe that Google collects "none" of the suggested pieces of information, 6% believe the company collects driver's license information, 7% believe Google collects social security information, while only 10% believe it may collect medical information. By contrast, 75% know that Google collects information on the browser's location and 88% know the firm keeps a record of what the browser searches.[19] Table 2 depicts these results.

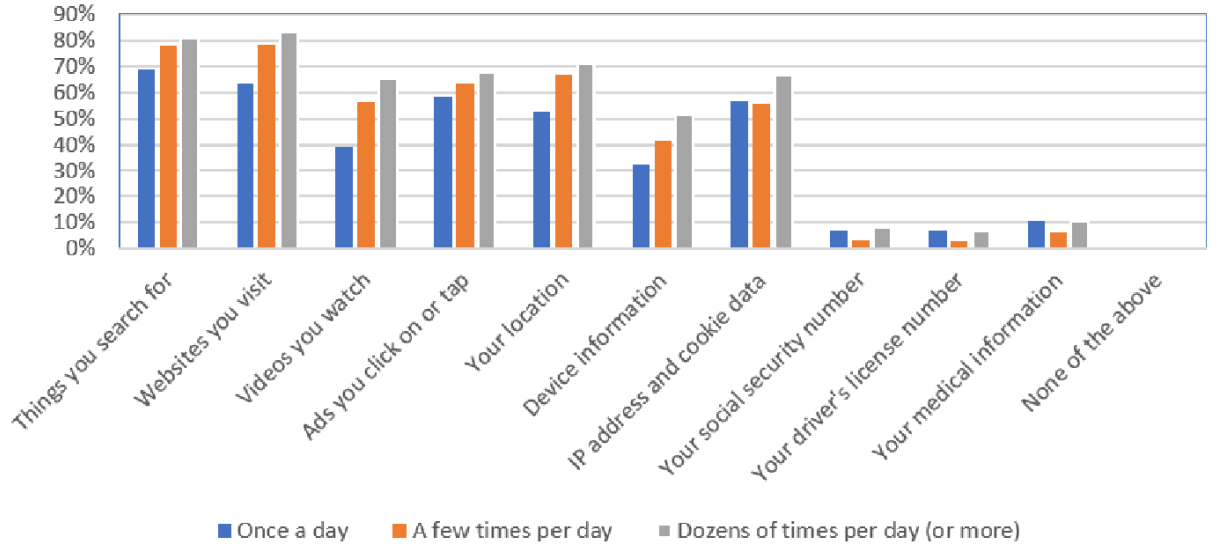
[19]My results show that the greatest amount of information asymmetry concerns consumers being unaware that information about their device is being collected. Still, even here, 50% of consumers are aware that device information is collected. And arguably, device information is probably the least "sensitive" or "important" (to most users) piece of information collected. It is also possible that consumers are unaware of what is meant by "device information." This could contribute to a low level of information.



Corollary 1b: *The responses of frequent users evince less information asymmetry.*

The prediction of Corollary 1b is also supported by the data. The more frequent users of Google's services are more aware of the information collection practices, a finding that follows directly from the idea that the cost of being uninformed is greater for them than relatively less frequent users. Among "once a day" Google users, only 78% are aware of information collection, whereas among those who use the site "dozens of times a day or more," 93% are aware of the collection, with moderate users falling in between at 88%.

Table 3: *Do you believe that Google collects information about you based on your searches, and then uses this information to target ads based on details about you?*



[b]Total Respondents for the three groups were as follows: Once a day: 75. A few times per day: 755. Dozens of times per day (or more): 760.

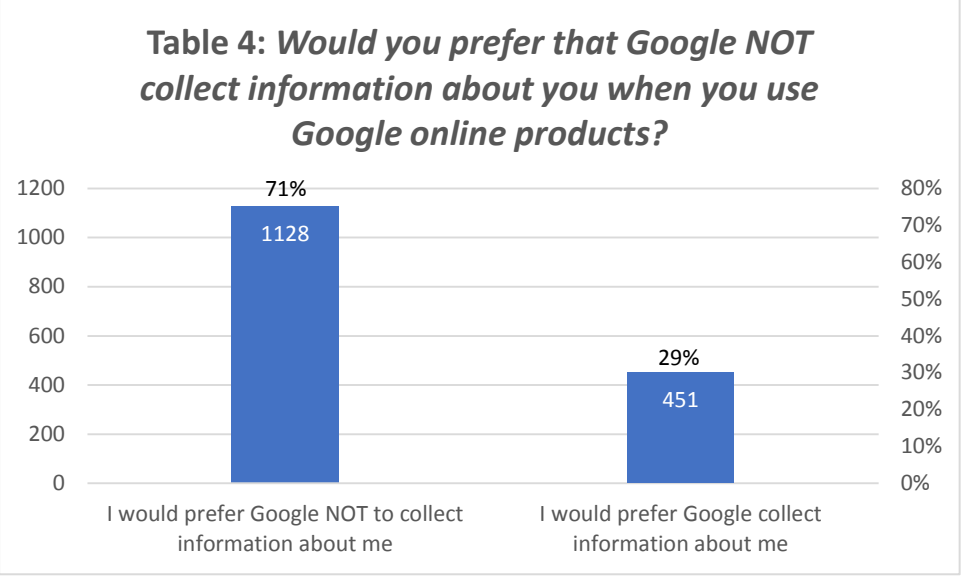
Hypothesis 2: *A constrained approach to eliciting responses will reveal that many consumers prefer sacrificing some level of privacy to paying a pecuniary fee to digital producers.*

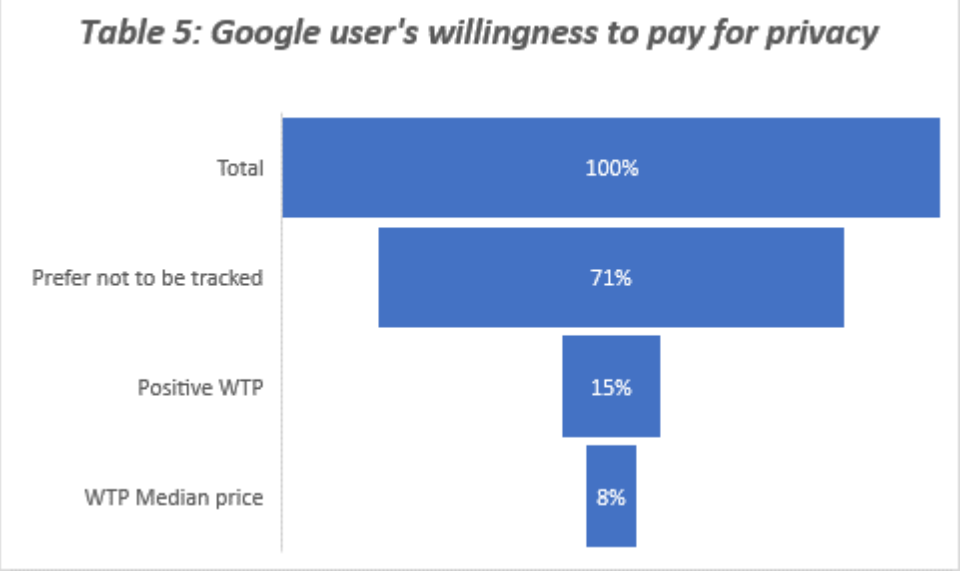
The evidence also overwhelmingly supports Hypothesis 2. Of particular note, and perhaps most surprising, is that 29% of Google users state that they have a *positive* preference for Google to collect their personal information. This may be due to an implicit understanding that such collection enables them to avoid a pecuniary fee. It might also be because it lowers consumers' search costs for products (via targeted advertising), a benefit of information collection noted by Varian (2009). This possibility is further supported by my finding that 24% of consumers express that they "like seeing the ads customized to my preferences."

Still, my survey shows that 71% of Google users say they would prefer for Google not to collect their information, a finding consistent with most other surveys of privacy and consistent with the idea that privacy is a "price" to many consumers. Such a result is also consistent with the notion that, for a majority of individuals, privacy is an economic good of which they would prefer more, *ceteris paribus*.

However, individuals expressing a preference for more of something that markets provide does not indicate that markets are failing by under-providing the good. Tellingly, of the 71% of all respondents who said they would prefer

not to be tracked, only 22% are willing to pay anything to retain their privacy. This finding is the strongest counter-argument against privacy market failure: of those who both voluntarily use Google and also prefer not to be tracked the overwhelming majority are not willing to sacrifice *anything* to achieve that privacy. Combining these figures, 85% of all Google users are unwilling to pay anything for marginal improvements to privacy. This leaves a scant 15% who are willing to pay for increased privacy.





How much is this minority willing to pay? Among those with a positive WTP to conceal information from

Google–between 15% and 16% of all Google users–the WTP is consistently small. Before beginning this analysis, I discarded all entries with a value greater than $10,000 (a total of only four entries) on the grounds that these were likely errors.[20] Among those indicating a positive WTP, the average annual WTP equals $76.78. Recall that all respondents in my sample report that they use Google at least once daily. Converted into daily terms, this annual WTP amounts to roughly 21 cents per day. After having removed the four values above $10,000, however, even this mean is driven by several outliers, as evidenced by a standard deviation of 238. Google has about one billion users annually and earns roughly $70 billion annually from information collection. How much revenue would the firm generate if it charged users a fee, rather than collecting their private information? Even under the most generous assumptions, my data suggest it could hope to make about 11.5 billion dollars (that is, multiplying the number of those with a positive WTP by the average WTP). This figure would amount to roughly 15% of Google's current annual information-collection revenue–its most significant revenue source.

Such a large standard deviation suggests that the median is better suited than the mean to provide an accurate picture of WTP. Were Google to use the mean to calculate a money price for increased privacy on its browser, it would effectively "price out" most of its customers. The median provides a better picture of the amount Google could hope to collect from charging consumers directly. In the dataset in which all responses of $10,000 or above have been omitted, the median annual WTP equals $20. In other words, of the roughly 15% of Google users willing to pay to protect their information, half are not willing to pay more than $20 annually. Converted into daily terms, this annual WTP amounts to roughly five and a half cents per day. Only about 8% of Google users would be willing to pay the minimum of $20 annually for increased privacy while using Google. For perspective, the National Soft Drinks Association estimates that the average American household spent about $850 on soft drinks in 2012.[21] Such a low WTP suggests that, even if a problem, digital privacy may not be worthy of being addressed via policy tools. The costs of such interventions may outweigh the benefits.

Because individuals might have difficulty calculating what a year of privacy is worth to them, these same respondents were also asked about their "per-search" willingness to purchase privacy. This time, respondents were asked to select one of the following for per-search measures of WTP: "less than 1 cent," "1 cent to 99 cents," "$1 to $5," or "more than $5." To this question, 59% responded that their per-search WTP was "less than 1 cent," 26% chose between 1 and 99 cents, with the remaining 15% choosing the final two options. These low per-search

[20]Three of the four were $100,000 or greater.
[21]See here: http://peopleof.oureverydaylife.com/much-americans-spend-soft-drinks-11124.html

valuations are consistent with the low annual privacy valuations.[22]

As stated above, Google serves roughly one billion users annually and earns roughly $70 billion annually in targeted advertising revenue. In order to earn $70 billion from directly charging consumers, Google must charge a $70 money price annually from every user. Thus, as a final measure of consumers' WTP, respondents with a positive WTP were simply asked a "yes or no" query regarding their willingness to pay $70 annually to protect their privacy when interacting with Google. Recalling that only 26% of those preferring not to be tracked have any positive WTP for privacy, this question revealed that 41% of these would be willing to pay the $70 fee that would be required of 100% of users if Google was to recoup its total revenue via charging a money price, rather than by collecting information. Thus, roughly 6.1% of all Google users would be willing to pay the $70 fee.

While average WTP is higher than median WTP, it is the latter that is more relevant for the question of charging for privacy. Were a company, such as Google, to collect data on the average WTP, and then set the price at that average, they would immediately price the majority of their users out of the market. Only those with a WTP above the average would then purchase the services. Of course, were the company to perennially evaluate the WTP of its current user base, this approach would generate a "lemons problem" in which every user is eventually priced out of the market (Akerlof 1970).

These results may be construed as even more significant given Acquisti et al.'s (2013) findings that there is a large endowment effect with respect to privacy. After all, my results show that consumers place a low valuation on privacy, *despite* the fact that they possess a property right in their information prior to accessing Google's services. By the logic of the endowment effect, consumers should place a greater value on their privacy relative to the benchmark of Google being the default personal-information owner. Consider the fact that Google does not gain access to consumer information unless a consumer uses a Google product, implying that the initial property right to personal information belong to consumers.

Furthermore, a low valuation of privacy is significant given that my other results indicate there is little information asymmetry between consumers and Google (see Hypothesis 1 and the attendant discussion). If consumers were highly uninformed while placing a low value on their privacy, this might simply suggest a higher valuation for informed consumers. Nonetheless, my results indicate well-informed consumers who, despite

[22]Given the nature of the question, it is impossible to determine if consumers are perfectly consistent between their annual and "per-search" evaluations. For example, one respondent selecting "$1 to $5" may have $1 in mind, whereas another has $5 in mind. Nonetheless, the answers are "generally" consistent in that both the annual and "per-search" prompts elicit relatively low WTP.

possessing a property right in their information, have a low WTP to prevent the transfer of that right to Google.

There is a possibility for terminological confusion here. What is the default? It depends on whether one's starting point is a consumer already using Google, in which case the default is that Google has rights to the information, or whether the starting point is a consumer *considering* using Google, in which case the default is that the consumer possesses the rights. The latter default is the one relevant to my survey design because I explicitly ask consumers their WTP to use Google, while retaining all the rights to their information. The starting point for my survey is personal ownership of information, which by Acquisti et al.'s (2013) results suggests that expressed valuation of privacy would be even higher than if personal ownership was not the default.

Hypothesis 3: *A source of discomfort with digital information collection is the risk of government privacy intrusion.*

The survey asked respondents about six possible threats to privacy and also included an option for "other" (an option selected by only 3%, indicating that these capture individuals' primary concerns). The evidence supports Hypothesis 3, suggesting that the literature has largely ignored an important reason for why individuals express dislike of digital information collection. My findings also provide support for the reasons offered by Acquisti et al. (2016). For example, about 70% of consumers indicated concern with respect to "the risk of identity theft," a threat noted by Acquisti et al. (2016) and one not necessarily tied to government failure.

Of those who dislike their privacy being compromised, however, 43% indicate that "a government agency forcing an internet entity that has collected your information to hand over the information" is a concern. By contrast, only 28% expressed any distaste for the common practice of price discrimination, which is frequently blamed for generating consumer dislike of information collection.[23] This suggests that, at the very least, concern over government intrusion should be included alongside dislike of practices such as price discrimination.

Respondents were then asked to ordinally rank their concerns. Fear of government intrusion earned a mean rank of 2.6 out of a possible seven options, suggesting that though it is not the most important concern for most users, it contributes significantly to consumer fear of information collection. These data suggest that government failure–in this case, the possibility of governments violating private property rights by forcing companies to relinquish data–is an important driver of consumer distrust of information collection.

The finding that consumers are suspicious of government access to information (for whatever reason) suggests

[23]An online vendor may price discriminate based on purchase history or location.

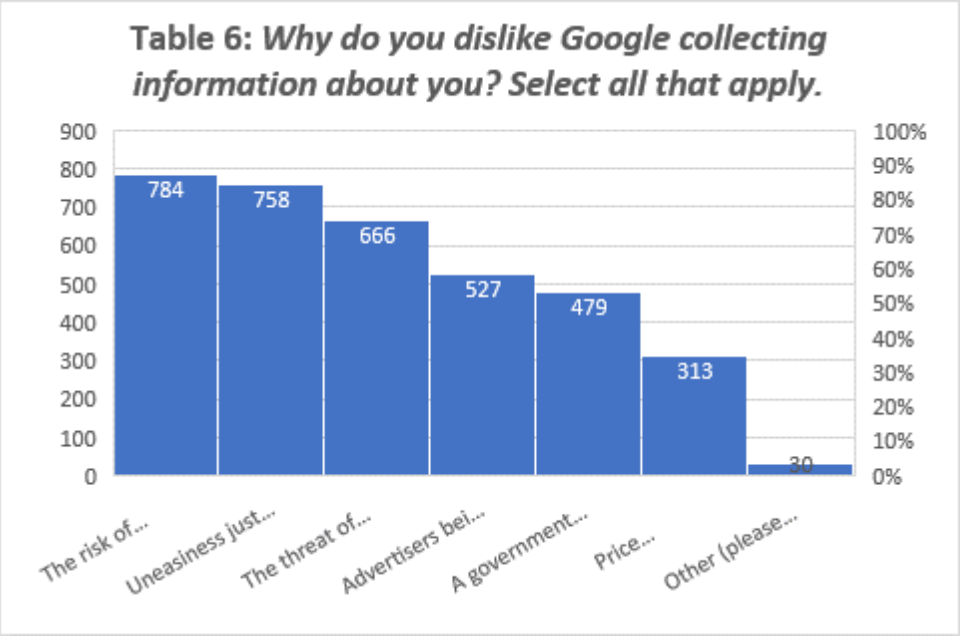
that, rather than systematic "over-collection" of information by firms, there may be systematic "under-collection" relative to the benchmark in which governments are "perfectly constrained." Hirsch (2010) argues that over-collection of consumer information occurs due to ill-informed consumers. With perfectly-informed consumers, less information would be collected. But if a world of perfect information and perfectly enforced property rights is the relevant benchmark, this suggests that the real world–in which governments may over-step their bounds–may suffer from information *under-collection.*

Consumers' concern about government over-reach serves as a constraint on the quantity of information firms may collect. This constraint may operate through two possible channels. First, individuals engage in less internet search activity. Secondly, firms are incentivized to collect less (and less sensitive) information given that consumers fear the governmental threat. In other words, the existence of uninformed consumers may, indeed, push toward over-collection as Hirsch (2010) contends. But the existence of predatory government pushes toward under-collection, and it is not clear which effect dominates, though my results (see Hypothesis 1 and attendant discussion) suggest that the extent of information asymmetry is minimal. Low levels of information asymmetry coupled with fear regarding government intrusion suggests that the net effect may be to push toward an information under-collection equilibrium.

At least with respect to Google, there is little evidence of widespread information asymmetry. There is no expressed WTP to protect privacy by over 4 out of 5 Google users[24] and a low average WTP among the remaining 1 out 5.[25] Lastly, there is some evidence that the threat of government collection should also be recognized as a factor in generating consumer distaste for information collection by private firms. Table 6 depicts these results.

[24]This increases to 6 out of 7, when accounting for those who initially indicated a WTP, but then entered a value of $0.

[25]It is low relative to the $70 which would be required from every Google user were it to substitute a fee for information collection.



[a] The original wording of the questions are: A) The risk of identity theft B) Uneasiness just not knowing who knows what about you C) The threat of spam D) Advertisers being able to target you directly E) A government agency forcing an internet entity that has collected your information to hand over the information F) Price discrimination (advertisers might show you a higher or lower price based on yourpersonal characteristics) G) Other (please specify)

7 CONCLUSION

My paper has three primary implications. First, it is possible to explain the so-called "privacy paradox" by showing that individuals only express a significant demand for digital privacy when they are not forced to consider the opportunity cost of making that choice. The question has never been whether consumers value privacy at all but rather how strongly they value it. The question is not whether individuals prefer more privacy but rather how much of other goods individuals are willing to exchange for greater privacy. At least in the context of interacting with Google, my results suggest that individuals place a low valuation on privacy. This explains why so many digital firms engage in information collection rather than alternative methods of earning revenue: consumers prefer this method to the alternatives. Put differently, there is little paradox at all–simply a positive preference, *ceteris paribus*, for more, rather than less, of an economic good.

Second, my results are particularly relevant given that there is little consensus regarding the best way for governments to protect consumer privacy (Hirsch 2010). This lack of consensus, coupled with my findings, should temper the impulse to regulate digital privacy with a significant dose of humility. The justification for regulating

privacy in a digital environment rests on the pillars that consumers are highly uninformed, value their privacy highly, and dislike information collection due to features of unhampered markets (price discrimination, etc...) My results cast doubt on all three of these claims. Yet, updates to the EU's Privacy Directive are set to take effect in 2018. And in the U.S., policymakers continue to debate the merits of implementing comprehensive, EU-style regulation. As a recent FTC (2012) report states, "...companies use this information to deliver better products and services to consumers, but they should not do so at the expense of consumer privacy," (p. 7). Such a value judgment is not supported by the results of my paper.

Third, continued collection of consumer information in the face of stated dislike for such activity has been called a market failure, but my results suggest government failure is also to blame. Governments, especially those possessing the technological capabilities of the modern era, play a significant role in shaping citizens' expectations of the interaction between firm and state. Citizens are concerned about governmental attempts to access information collected by Google–a reasonable concern in light of recent revelations of mass surveillance programs and government attempts to force private companies to surrender information. The fact that internet-users harbor this fear does not mean that other concerns are unwarranted; rather, it simply indicates that researchers should acknowledge that failure by governments to respect private property rights also plays a role in citizen mistrust of firms' data collection practices.

In sum, there is little evidence here to suggest that the digital marketplace fails, at least with respect to one of its biggest players: Google. Such a result should inspire humility on the part of policymakers who believe themselves capable of improving on the choices of informed individuals interacting within a regime of property, contract, and consent.

8 APPENDIX

The survey contained the following questions, which appeared to the respondent in the order they are listed below:

1. *Do you make web searches on Google.com?*

If the respondent indicated they did not, they were disqualified from further questions. After this "screener question" was performed, the sample was reduced to 1,599 respondents.

2. *How often do you make searches on Google.com?*

Possible responses included: "once a day," "a few times per day," and "dozens of times per day (or more)."

3. *Do you believe that Google collects information about you based on your searches, and then uses this information to target ads based on details about you?*

Possible responses included: "Yes" and "No."

4. *What information do you believe Google collects about you? Select all that apply.*

Possible responses included: "Your driver's license number," "Your social security number," "Videos you watch," "Device information," "Ads you click on or tap," "Websites you visit," "Your location," "Things you search for," "Your medical information," "IP address and cookie data," and "None of the above." Google may collect any of this information except for "Your driver's license," "Your social security number," and "Your medical information."

5. *Do you trust Google to keep this information private?*

Possible responses included: "Yes," "No," and "Somewhat."

Note: This question was not analyzed in the paper, but was collected to contextualize the other questions.

6. *Would you prefer that Google collected no information about you when you use Google online products?*

Possible responses included: "I would prefer Google collect information about me" or "I would prefer Google NOT collect information about me." Those responding that they would prefer Google to collect personal information were disqualified from answering additional questions so that the remaining sample was only comprised of individuals with a demand for additional digital privacy.

7. *Why do you dislike Google collecting information about you? Select all that apply.*

Possible responses included: "A government agency forcing an internet entity that has collected your information to hand over the information," "Price discrimination (advertisers might show you a higher or lower price based on your personal characteristics)," "Uneasiness just not knowing who knows what about you," "The risk of identity theft," "The threat of spam," "Advertisers being able to target you directly," and "Other (please specify)."

8. *Please rank the following items in terms of which concerns you the most, where 1 is the most concerning.*

Question eight asked respondents to provide an ordinal ranking of the responses they had provided in question seven, in order of decreasing perceived severity.

9. *What do you think about the ads targeted to you based on the information Google collects about you?*

Possible responses included: "I like seeing the ads customized to my preferences" and "I don't like the ads and would rather not seem them."

Note: This question was not analyzed in the paper, but was collected to contextualize the other questions.

10. *Would you prefer to pay to use Google.com in exchange for a guarantee that Google will NOT collect any private information about you, and therefore show you no targeted ads?*[26]

Possible responses included: "Yes" and "No." Those answering "No" to this question were disqualified from further queries.

11. *How much would you be willing to pay per year to use Google.com without Google collecting any personal information about you? Enter a whole number in US dollars.*

12. *How much would you be willing to pay per search to use Google.com without Google collecting any personal information about you?*

Possible responses included: "Less than 1 cent," "1 cent to ninety-nine cents," "$1 to $5" or "More than $5."

13. *Would you be willing to pay $70 per year to ensure your privacy while using all Google online products?*

Possible responses included: "Yes" and "No."

[26] Twenty-four respondents failed to answer this question.

REFERENCES

Acquisti, Alessandro. 2014. “From the economics of privacy to the economics of big data”.

— . 2004. “Privacy in electronic commerce and the economics of immediate gratification”. In *Proceedings of the 5th ACM conference on Electronic commerce*, 21–29. ACM.

Acquisti, Alessandro, and Ralph Gross. 2006. “Imagined communities: Awareness, information sharing, and privacy on the Facebook”. In *International workshop on privacy enhancing technologies*, 36–58. Springer.

Acquisti, Alessandro, and Jens Grossklags. 2005. “Privacy and rationality in individual decision making”. *IEEE Security & Privacy* 2 (2005): 24–30.

— . 2007. “What can behavioral economics teach us about privacy”. *Digital Privacy: Theory, Technologies and Practices* 18:363–377.

Acquisti, Alessandro, Leslie K John, and George Loewenstein. 2013. “What is privacy worth?” *The Journal of Legal Studies* 42 (2): 249–274.

Acquisti, Alessandro, Curtis R Taylor, and Liad Wagman. 2016. “The economics of privacy”. *Available at SSRN 2580411*.

Akerlof, George A. 1970. “The market for” lemons”: Quality uncertainty and the market mechanism”. *The quarterly journal of economics*: 488–500.

Alchian, Armen A. 1967. *Pricing and society*. Institute of Economic Affairs.

“American’s Attitudes About Privacy, Security, and Surveillance”. 2015.

Ayenson, M, et al. 2012. “Behavioral Advertising: The Offer You Cannot Refuse”. *Harvard Law and Policy Review* 273.

Becker, Gary S, Yona Rubinstein, et al. 2004. “Fear and the response to terrorism: an economic analysis”. *University of Chicago mimeo*.

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. 2005. “Privacy in e-commerce: stated preferences vs.

actual behavior". *Communications of the ACM* 48 (4): 101–106.

Berman, Jerry, and Deirdre Mulligan. 1998. "Privacy in the digital age: Work in progress". *Nova L. Rev.* 23:551.

Boettke, Peter J. 2007. "Liberty vs. Power in Economic Policy in the 20th and 21st Centuries". *The Journal of Private Enterprise* 22 (2): 7–36.

Boettke, Peter J, and Rosolino Antonio Candela. 2015. "Price Theory as Prophylactic against Popular Fallacies". *Available at SSRN 2710201*.

Brown, Ian. 2016. "12. The economics of privacy, data protection and surveillance". *Handbook on the Economics of the Internet*: 247.

Calo, Ryan. 2013. "Digital Market Manipulation". *Geo. Wash. L. Rev.* 82:995.

Clark, Jeff R, and Benjamin Powell. 2013. "Sweatshop working conditions and employee welfare: Say it ain't sew". *Comparative Economic Studies* 55 (2): 343–357.

Cooper, James C. 2012. "Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity". *Geo. Mason L. Rev.* 20:1129.

— . 2013. "Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity". *George Mason Law Review, Forthcoming*: 13–39.

De Corniere, Alexandre, and Romain De Nijs. 2016. "Online advertising and privacy". *The RAND Journal of Economics* 47 (1): 48–72.

Farrell, Joseph. 2012. "Can privacy be just another good". *J. on Telecomm. & High Tech. L.* 10:251.

Federal Trade Commission. 2010. "Protecting Consumer Privacy in an Era of Rapid Change." Preliminary FTC Staff Report, 1-122. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

Federal Trade Commission. 2012. "Protecting Consumer Privacy in an Era of Rapid Change." FTC Report, 1-112. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Fuller, Caleb S. 2017. "Privacy law as price control". *European Journal of Law and Economics*: 1–26.

Gertz, Janet Dean. 2002. "Purloined Personality: Consumer Profiling in Financial Services, The". *San Diego L. Rev.* 39:943.

Goldfarb, Avi, and Catherine Tucker. 2012. "Shifts in privacy concerns". *The American Economic Review: Papers*

and Proceedings 102 (3): 349–353.

Hermalin, Benjamin E, and Michael L Katz. 2006. “Privacy, property rights and efficiency: The economics of privacy as secrecy”. *Quantitative Marketing and Economics* 4 (3): 209–239.

Hermstrüwer, Yoan. 2017. “Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data”. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC)* 8:9–26.

Hoofnagle, Chris Jay. 2003. “Reflections on the NC JOLT Symposium: The Privacy Self-Regulation Race to the Bottom”. *NCJL & Tech.* 5:213.

Hoofnagle, Chris Jay. 2009. “Beyond Google and evil: How policy makers, journalists and consumers should talk differently about Google and privacy”. *First Monday* 14 (4-6).

Hoofnagle, Chris Jay, and Jan Whittington. 2013. “Free: Accounting for the costs of the internet’s most popular price”. *UCLA L. Rev.* 61:606.

Hoofnagle, Chris Jay, et al. 2012. “Behavioral Advertising: The Offer You Can’t Refuse”. *Harv. L. & Pol’y Rev.* 6:273.

Hui, Kai Lung, and Ivan PL Png. 2006. “Economics of Privacy”. *HANDBOOK OF INFORMATION SYSTEMS AND ECONOMICS*.

John, Leslie K, Alessandro Acquisti, and George Loewenstein. 2011. “Strangers on a plane: Context-dependent willingness to divulge sensitive information”. *Journal of consumer research* 37 (5): 858–873.

Lenard, Thomas M, and Paul H Rubin. 2009. “In defense of data: Information and the costs of privacy”. *Technology Policy Institute Working Paper*: 9–44.

Lerner, Josh. 2012. “The Impact of Privacy Policy Changes on Venture Capital Investment in Online Advertising Companies”. *Analysis Group*: 1–2.

Marthews, Alex, and Catherine Tucker. 2015. “Government surveillance and internet search behavior”. *Available at SSRN 2412564*.

Milberg, Sandra J, H Jeff Smith, and Sandra J Burke. 2000. “Information privacy: Corporate management and national regulation”. *Organization science* 11 (1): 35–57.

Newman, Nathan. 2013. “Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google, The”. *Wm. Mitchell L. Rev.* 40:849.

Norberg, Patricia A, Daniel R Horne, and David A Horne. 2007. “The privacy paradox: Personal information disclosure intentions versus behaviors”. *Journal of Consumer Affairs* 41 (1): 100–126.

Penney, Jon. 2016. “Chilling Effects: Online Surveillance and Wikipedia Use”. *Berkeley Technology Law Journal*.

Posner, Richard A. 1978. “Economic theory of privacy”. *Regulation* 2:19.

Rose, E. 2005. “Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?” In *System Sciences, 2005. HICSS’05. Proceedings of the 38th Annual Hawaii International Conference on*, 180c–180c. IEEE.

Sachs, Benjamin R. 2009. “Consumerism and information privacy: How Upton Sinclair can again save us from ourselves”. *Virginia Law Review*: 205–252.

Solove, Daniel J. 2006. “A taxonomy of privacy”. *University of Pennsylvania law review*: 477–564.

— . 2004. *The digital person: Technology and privacy in the information age*. NyU Press.

Sowell, Thomas. 1987. “A conflict of visions”. *New York: Morrow*.

Stigler, George J. 1980. “An introduction to privacy in economics and politics”. *The Journal of Legal Studies* 9 (4): 623–644.

Strandburg, Katherine J. 2013. “Free Fall: the Online Market’s Consumer Preference Disconnect”. *U. Chi. Legal F.* 95.

Thomson, Judith Jarvis. 1975. “The right to privacy”. *Philosophy & Public Affairs*: 295–314.

Tsai, Janice Y, et al. 2011. “The effect of online privacy information on purchasing behavior: An experimental study”. *Information Systems Research* 22 (2): 254–268.

Tucker, Catherine E. 2012. “The economics of advertising and privacy”. *International journal of Industrial organization* 30 (3): 326–329.

Turow, Joseph, et al. 2009. “Americans reject tailored advertising and three activities that enable it”. *Available at SSRN 1478214*.

Varian, Hal R. 2009. “Economic aspects of personal privacy”. In *Internet policy and economics*, 101–109. Springer.

Vila, Tony, Rachel Greenstadt, and David Molnar. 2004. “Why we can’t be bothered to read privacy policies”. In *Economics of Information Security*, 143–153. Springer.