PROGRAM ON ECONOMICS & PRIVACY

ANTONIN SCALIA LAW SCHOOL

HOW CONSUMERS VALUE DIGITAL PRIVACY: NEW SURVEY EVIDENCE

Caleb Fuller
Assistant Professor of Economics, Grove City College
Faculty Affiliate, Program on Economics & Privacy

I. Introduction

Regardless of how they define it, few people would deny that they'd like more privacy. The rise of the Internet and "Big Data" have thrust privacy issues to the fore of the public consciousness. Indeed, stories like the one which revealed that Target[1], by analyzing a customer's purchasing habits, determined a teenager was pregnant before her parents knew confirms the worst suspicions of many people that privacy is, in fact, obsolete.[2] It's thus unsurprising that the average American citizen, when surveyed, expresses a desire for less privacy-invasive behavior by both private firms and by government.[3]

Due to the constraints imposed by scarcity, however, there are myriad things which human beings doubtless want more of, but which are simply unobtainable. For example, someone who wants a safer job will often find that while such jobs are available, they pay less than otherwise comparable, but marginally more dangerous options. Employees would prefer jobs that are both safer *and* more remunerative; scarcity dictates that they will be forced to trade off some pay for more safety. Employers aren't willing to pay a worker more than she's worth, and installing safety features—to perhaps lure employees from rivals—and increasing pay are both costly to the firm. More on-the-job safety means the firm won't have to pay as much to attract workers. A prospective employee looking for a less risky job must weigh whether the safer working environment justifies the smaller paycheck.

The logic of tradeoffs applies to privacy, just as it does to the compensation one receives in labor markets. People may routinely express a desire—even a strong one—for additional privacy. But are they willing to bear the costs associated with additional privacy protection?

---

[1] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0

[2] *See* Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, THE GUARDIAN, Jan. 10, 2010, https://www.theguardian.com/technology/2010/jan/11/facebook-privacy (explaining that Mark Zuckerberg has suggested privacy is an outdated social norm).

[3] *See e.g.* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RES. CENTER INTERNET & TECH., May 20, 2015, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Using new survey evidence, I attempt to discover whether there is divergence between the additional privacy consumers demand when it's offered to them as a "free lunch" versus the privacy they demand when privacy is costly, as it is in the real world.

Such research may be helpful for informing debates surrounding digital privacy policy. With the countdown to the "most important change in data privacy regulation in 20 years" well under way, research regarding the importance of privacy to consumers is timely.[4] Related questions—"are consumers really in the dark about who's collecting what?"—and—"why do consumers express a dislike for information collection?" are also important ones for policymakers to consider, and I attempt answers at those via survey.

The case for government intervention in digital markets is made stronger if consumers value privacy highly, if they are highly uninformed, and if market activity, rather than government itself, drives privacy fears. By the same logic, if the average consumer does not value privacy highly, if they are relatively informed, and if government involvement contributes to privacy fears, these facts weaken the case for intervention

II. The Economic Approach to Privacy

In 2015, Google made $67.39 billion in advertising revenue; in 2016, the figure came to $79.38 billion.[5] For digital firms, advertising is virtually synonymous with the surreptitious collection of consumer information by using web bugs and cookies which track consumers' activity across sites. Advertisers are willing to pay Google a handsome sum for the privilege of being permitted access to a consumer's every digital move. Information about consumers is then used to generate personalized advertisements—a practice that many consumers might understandably describe as invasive or "creepy."

Consumer dislike of tracking is confirmed by the empirical evidence. Routine survey and polling data suggest that consumers would prefer digital firms to collect less information or, at the very least, to be more transparent about it. For example, Turow and his coauthors find that 66% of American adults would rather not view advertisements that are tailored based on their search history (so-called "behavioral targeting").[6] Along similar lines, a Pew survey finds that 93% of American adults contend "that being in control of *who* can get information about them is important."[7]

---

[4] On May 25th, 2018, the European Union's "General Data Protection Regulation" (GDPR) goes into effect. The new law promises to unify Europe's fragmented digital privacy law landscape. *See* EUR. UNION, GEN. DATA PROTECTION REG., https://www.eugdpr.org/

[5] *See* Advertising Revenue of Google from 2001 to 2017, STATISTA, https://www.statista.com/statistics/266249/advertising-revenue-of-google/

[6] *See* Joseph Turow et. al., *Americans Reject Tailored Advertising and Three Activities That Enable It*, U. PA. SCHOLARLY COMMONS (Sept. 2009) https://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers

[7] *See* Madden & Rainie, *supra* note 3.

These results are unsurprising, but they are also unsatisfactory from an economic point of view, because they do not tell the full story. They merely demonstrate that, when no cost is involved, consumers prefer more of an economic good to less—a well-accepted tenet of economics 101. Suppose we instead presented consumers with the following query: "Would you prefer more ice cream?" All but the lactose-intolerant would doubtlessly respond that they would prefer more ice cream, especially if they could consume more ice cream without incurring any additional cost. In reality, consuming ice cream *always* incurs a cost: there's the obvious pecuniary cost of acquiring the ice cream, but also a marginally shorter life span, and the foregone alternative to which one's money, time, and ice-cream consuming energy could have been directed.

"These results are unsurprising, but they are also unsatisfactory from an economic point of view, because they do not tell the full story. They merely demonstrate that, when no cost is involved, consumers prefer more of an economic good to less—a well-accepted tenet of economics 101."

To ask consumers whether they want more ice cream, without attaching any cost to that decision, is what might be called an "unconstrained approach" to ascertaining consumers' preferences. The economic approach, by contrast, emphasizes that every choice incurs a cost because we live in a world of scarcity. Whether it's ice cream or privacy, getting more means giving up something else consumers value.

If digital companies did not finance their offerings through the collection of consumer information, they would be looking for some other revenue stream to remain a going concern. One option would be to simply charge consumers a money-price directly, like sellers of bananas do. In this case, consumers would be giving up money to acquire more privacy. Another option would be to stop tracking consumers and show only untargeted ads—ads which have a significantly lower conversation rate than their targeted counterparts.[8] Given that untargeted ads are less effective, advertisers will be willing to pay less for a platform on which to display them. Thus, a switch to purely untargeted ads clearly lowers targeting firms' revenues. In this scenario, consumers would be giving up something else—perhaps some measure of quality associated with the digital firm, fewer digital firms to choose from, or fewer services offered by digital firms.

It's clear that consumers incur a cost by acquiring more of a scarce good, privacy in this case. But what would happen to firms themselves if they decided to charge up front? What if Google began offering annual memberships in return for relinquishing any right to track consumers? Would it lose revenue under this financing scheme?

III. How Much Do Consumers Value Privacy?

[8] *See* Rebecca Walker Reczek, Christopher Summers, & Robert Smith, *Targeted Ads Don't Just Make You More Likely to Buy — They Can Change How You Think About Yourself*, HARV. BUS. REV., Apr. 4, 2016 https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself; Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGMT. SCI. (2011) https://pubsonline.informs.org/doi/abs/10.1287/mnsc.1100.1246

To answer these questions, I conducted one of the largest surveys of consumer privacy valuation to date. Haven Insights LLC, a private data analytics company, generated a random sample of 1,579 Internet users. The composition of respondents, all over age eighteen, mirrored the demographic breakdown of the 2010 U.S. census on the following dimensions: ethnicity, gender, and religious affiliation. Furthermore, all respondents use Google at least occasionally. The primary purpose of the survey was to determine whether there is a significant divergence between "unconstrained" and "constrained" privacy preferences.

The most jarring result of the survey is that many digital consumers view being tracked as a positive economic good in and of itself. When asked: "*Would you prefer that Google collected no information about you when you use Google online products?*", 29% of respondents indicated they would positively *prefer* to be tracked. Evidently the "icky factor" of being watched is insignificant for almost a third of Google users. Presumably these users enjoy the personalized ads, which do in fact, reduce a consumer's search costs.[9] Though a minority of Google users, these respondents indicate that reducing the capability of firms to acquire their information is damaging, rather than beneficial.

The fact remains, however, that 71% of Google users would prefer the same experience sans the tracking. For these users, privacy is an economic good of which they would prefer more, *ceteris paribus*. It turns out that "all other things constant" is the key. When this group is queried further, only 21% are willing to pay *anything* for additional privacy on Google.[10] Put in terms of all Google users, 85% are unwilling to pay anything for privacy on Google.

"It turns out that 'all other things constant' is the key. When this group is queried further, only 21% are willing to pay anything for additional privacy on Google. Put in terms of all Google users, 85% are unwilling to pay anything for privacy on Google."

It is important to note that this is a stated preference, rather than a demonstrated one. To grasp the significance of this fact, it's important to first understand the so-called "privacy paradox."[11] The paradox is the oft-observed finding that consumers routinely state a significant preference for privacy, but just as routinely forgo relatively low-cost methods of protecting their privacy. For example, it is relatively easy to discover the existence of DuckDuckGo, a rival search engine to Google that proudly proclaims it does *not* track consumer searches. How easy is to learn about DuckDuckGo? When I used Google to look for a "search engine that protects privacy,"

---

[9] Hal R. Varian, *Economic Aspects of Personal Privacy*, U.C. BERKELEY I-SCHOOL (Dec. 6, 1996) http://people.ischool.berkeley.edu/~hal/Papers/privacy/privacy.html#SECTION00031000000000000000 (noting that less privacy enables lower search costs).

[10] This group was asked: "*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?*"

[11] *See generally*, Patricia A. Norberg, Daniel R. Horne, & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, 41 J. CONSUMER AFFAIRS 100 (2007) http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2006.00070.x/full

DuckDuckGo was the second result on the page. (The first result was a website listing the 5 best search engines that protect privacy; the first on the list was DuckDuckGo).[12]

Many scholars of privacy argue that the "privacy paradox" demonstrates consumer susceptibility to a host of biases identified by behavioral economists. Stated preference is often viewed as a consumer's "true" preferences; once in the digital environment, however, consumers deviate from perfect rationality, succumbing to a host of biases that generate behavior inconsistent with underlying preferences. Individuals may engage in hyperbolic discounting—discounting the future more heavily than their true preferences would have them. Alternatively, they may systematically underestimate the probability of small risks.

The survey results explored here do not compare "unconstrained" survey questions with subsequent behavior, thus finding that the latter deviates from a consumer's stated intentions. This is the typical method of researchers showing the existence of the "paradox." Instead, this approach compares "stated unconstrained preferences" with "stated constrained preferences." The results show that stated constrained preferences represent a significant deviation from stated unconstrained ones. This suggests that the "privacy paradox" may not be a result of biases causing consumers to act inconsistently with their true preferences. Rather, it's possible that the paradox may be explained on simpler grounds: surveys often take an unconstrained approach; behavior online always incurs a real cost (even if it's a very small opportunity cost).

"… the 'privacy paradox' may not be a result of biases causing consumers to act inconsistently with their true preferences. Rather, it's possible that the paradox may be explained on simpler grounds: surveys often take an unconstrained approach; behavior online always incurs a real cost (even if it's a very small opportunity cost)."

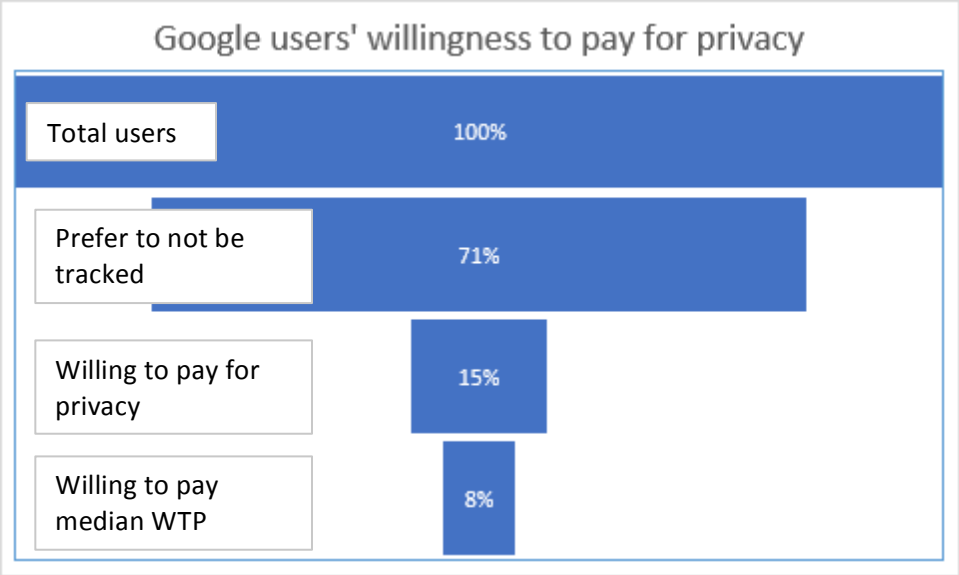
Back to the survey. Only 15% of Google users have a positive willingness to pay (WTP) for privacy. How much is this minority willing to pay? After discarding 4 responses above $10,000, the average annual WTP for complete privacy on Google is $76.78. For a point of reference, the average American household spends $850[13] on soft drinks annually.[14]

At first glance, that average might still seem like a significant sum, especially relative to Google presently being free. Consider, however, that 100% of my respondents indicate they use Google at least once daily.[15] This suggests that respondents would be willing, on average, to pay about 21 cents daily for privacy on Google. A per search measure would clearly be even lower.

Even this relatively small average, however, is itself driven by several outliers, as indicated by a standard deviation of 238. Given this, a better measure would be the median WTP. Once again discarding the four responses above $10,000, the median WTP comes to $20 annually. In sum, only 15% of Google users are willing to pay, and of these, the median WTP is a paltry $20 per

[12] Similarly, when I used to Google to find a "search engine that doesn't track," DuckDuckGo was the first result.
[13] Converted into daily figures, this amounts to over $2.30. Still not much, but far more than consumer WTP for digital privacy.
[14] *See* Brad Tuttle, *How Much You Spend Each Year on Coffee, Gas, Christmas, Pets, Beer, and More*, TIME, Jan 23, 2010 http://business.time.com/2012/01/23/how-much-you-spend-each-year-on-coffee-gas-christmas-pets-beer-and-more
[15] All respondents use Google "once a day," "a few times per day," or "dozens of times per day."

year. In other words, close to 8% of Google users would be willing to pay $20 annually. Since all of the respondents in my sample use Google at least once a day, this annual figure comes to a WTP of somewhere between 5 and 6 cents per day.



Suppose that Google's annual ad revenue comes to somewhere between $67 and $80 billion (these figures are Google's 2015 and 2016 revenue respectively). Google chrome has roughly one billion worldwide users.[16] If the company abandoned all tracking, in favor of simply charging consumers an annual fee, could it possibly hope to maintain revenue neutrality? It's doubtful.

As a check on the results just discussed, the survey next asked those with a positive WTP (again, only 15% of users) if they'd be willing to pay $70 annually to protect privacy while using Google products.[17] Roughly 41% of this 15% said they'd be willing to pay $70. Put in terms of total Google users, only about 6% report they'd be willing to pay $70 annually for privacy while using Google services. Granted, this measure reveals a greater willingness to pay than when consumers are asked to enter in a value on their own. But if the company were to maintain its current revenue stream, virtually 100% of Google users would need to pay $70 annually. And that's a conservative estimate if you take Google's 2016 revenue as the relevant benchmark.

The burden of proof is on regulatory advocates to explain why privacy is sufficiently different from other goods that it requires regulatory intervention. One possible candidate is information asymmetry. Perhaps consumers' WTP is low because they are largely ignorant of the risks they face.

---

[16] *See* Emil Protalinski, *Google Chrome now has over 1 billion users*, VENTUREBEAT, May 28, 2015 https://venturebeat.com/2015/05/28/google-chrome-now-has-over-1-billion-users/.
[17] The exact question: "*Would you be willing to pay $70 per year to ensure your privacy while using all Google online products?*"

IV. How Much Do Consumers Know?

Some scholars might concede the preceding argument if we inhabited a world of perfect information. They contend, however, that consumers are ill-informed regarding firms' information collection practices. They do not always know when information is being collected or what types of information firms are collecting. If consumers knew the full extent of the practice, they'd be willing to pay far more for privacy protection.

It should be noted that there is some degree of information asymmetry between buyers and sellers in *every* transaction. I can't possibly know all the inherent risks in using a smartphone, for instance, though there are doubtless many possible harms. To use a world of perfect information as a benchmark by which to condemn reality commits the Nirvana Fallacy of which economist Harold Demsetz warned.[18]

We must then ask: when consumers are *particularly* ill-informed, why is that the case? Might it be that they have judged the potential privacy harm to be low? That the cost of becoming informed outweighs any potential benefits? After all, I have no idea what the likelihood is that I'll be struck and killed by a falling coconut when I visit my friend in Florida this summer, but I've (rightly or wrongly) evaluated the risk as sufficiently low that I view the benefit of additional research on the topic to be negligible. My time, like every other good, is scarce, and I necessarily sacrifice other valuable goods were I to spend time researching my odds of death-by-coconut.

The economic approach would suggest that when consumers stand to lose more from a potential harm, they are more likely to become informed about it. For example, it stands to reason that women seek to become more informed about pregnancy risks than do; they have more to lose from not being informed. Men, who work disproportionately in coal mines, by the same logic, stand to gain more from learning about coal mining's attendant risks.

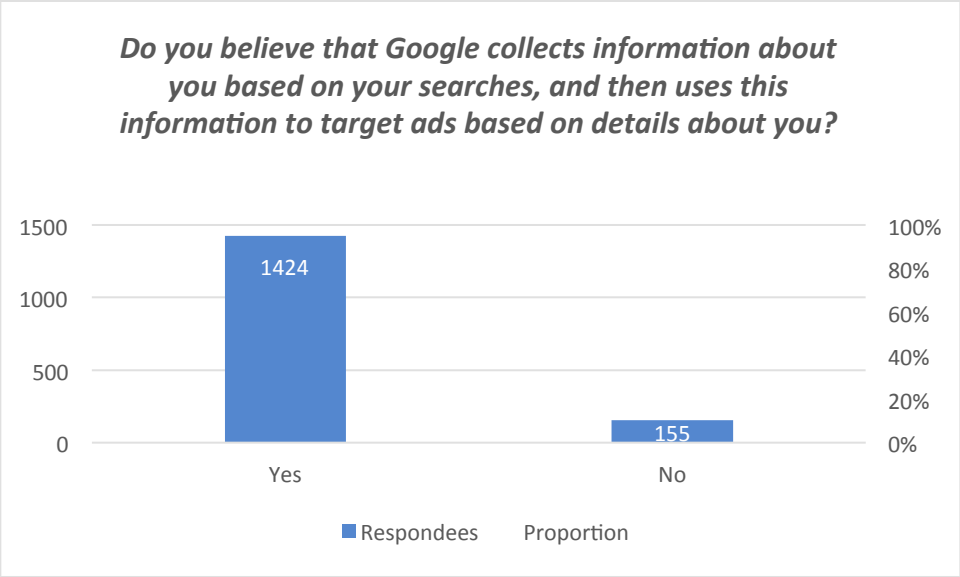
"… among all Google users, 90% respond that they are aware of Google's information collection. This finding suggests that, at least with respect to Google, ignorance regarding the practice of information collection is not widespread."

To test whether the same holds true for privacy harms, I first ask questions to determine how much respondents know about Google's information collection practices. Significantly, among all Google users, 90% respond that they are aware of Google's information collection. This finding suggests that, at least with respect to Google, ignorance regarding the practice of information collection is not widespread.

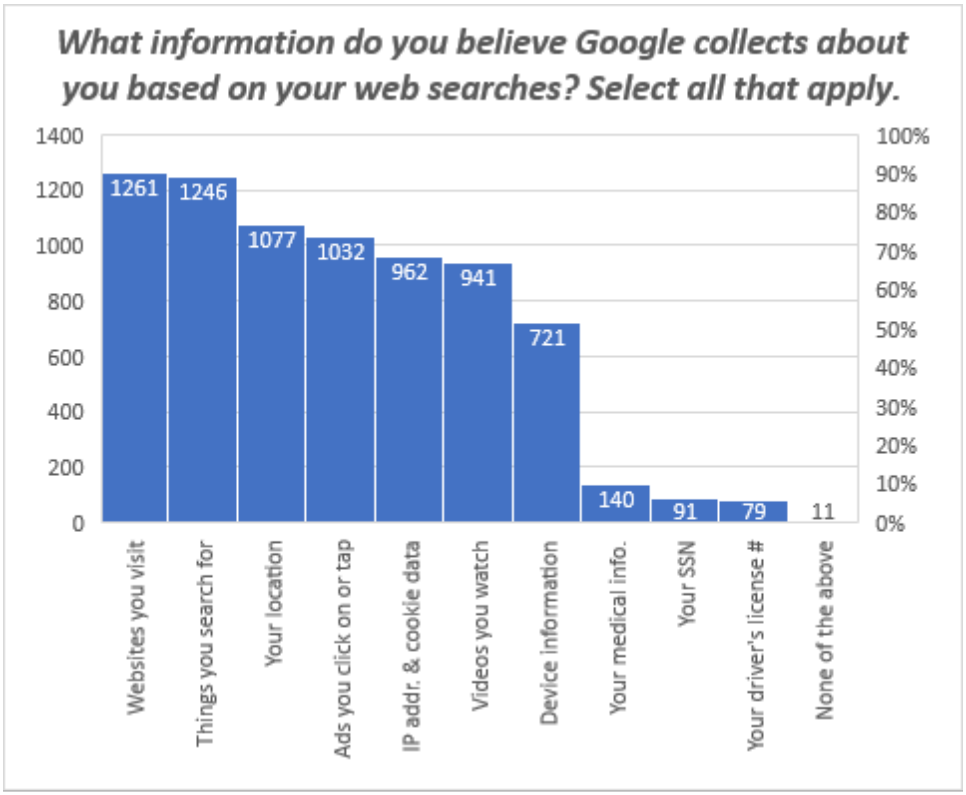
It is one thing to know that Google collects browsers' information. It is quite another to know what sorts of information Google collects. Do consumers merely possess a vague hunch regarding Google's activities or are they better informed?

---

[18] *See generally* Harold Demsetz, *Information and Efficiency: Another Viewpoint*, 12 J. L. & ECON 1 (1969) http://www.journals.uchicago.edu/doi/abs/10.1086/466657?journalCode=jle (outlining Demsetz's famous Nirvana Fallacy argument).



In attempting to answer this question, respondents were presented with 11 possible pieces of data (7 accurate and 4 inaccurate), and asked to select the ones Google collects. Here too, the data reveal that consumers possess a relatively high, albeit imperfect, degree of understanding. How many respondents believe Google collects information it does not? Only 6% believe the company collects driver's license information; 7% believe Google collects social security information; only 10% believe it may collect medical information. Only 1% of respondents indicate that Google collects none of the suggested information. By contrast, 75% know that Google collects information on the browser's location and 88% know the firm keeps a record of whatever the browser searches.



Perhaps the most compelling of these results is that more frequent Google users are better informed than moderate users who are, in turn, more informed than the least frequent users. Among "once a day" Google users, only 78% are aware of information collection, whereas 93% of those who use the site "dozens of times a day or more" are aware of information collection. Moderate users fall in between at 88%. To the extent that browsers suffer privacy harms from using Google, we would expect the most frequent users to be harmed most often. It follows from this that the most frequent users stand to gain the most from becoming informed about what specifically their Google use entails for their privacy.

There is one additional finding consistent with the notion that consumers are guided by relative costs and benefits in their decision to become informed. Respondents indicate the greatest degree of ignorance when asked whether Google collects information about their device. Half respond that they are unaware that this collection occurs. Yet, 88% know that Google saves a record of their searches. Of the two—Google collecting device information vs. saving a record of searches—the latter clearly seems more intrusive. It seems reasonable that the average person is far more likely to care about a permanent record of searches than a permanent record describing her device information. Thus, the benefit to becoming informed about the search record exceeds the benefit to becoming informed about Google's habit of collecting more trivial pieces of information. Consumers similarly demonstrate high levels of awareness regarding Google's practice of collecting information pertaining to "websites visited" and Google searches.

V. Do Governments Contribute to Privacy Hysteria?

Why do consumers express dislike of information collection? As Turow et al. state: "Exactly why they reject behavioral targeting is hard to determine."[19] An excellent survey of the economics of privacy in the *Journal of Economics Perspectives* by Alessandro Acquisti, Curtis Taylor, and Liad Wagman offers a few suggestions.[20] They write: "Use of individual data may subject an individual to a variety of personally costly practices, including price discrimination in retail markets, quantity discrimination in insurance and credit markets, spam, and risk of identity theft, in addition to the disutility inherent in just not knowing who knows what or how they will use it in the future."[21]

My survey empirically examines whether these possibilities are feared by consumers. Additionally, I add another risk to this list: the possibility that governments might force a private firm to relinquish a repository of information. This is an important possibility because other research shows that government activity serves as an important constraint on consumers' digital behavior. Specifically, knowledge of government surveillance activity exerts a "chilling effect" on consumer search habits. Oxford's Jon Penney found that Snowden's NSA revelations caused Wikipedia searches for content that the NSA might find questionable to drop significantly and

[19] *See* Turow, *supra* note 6, at 4.
[20] *See generally* Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442 (2016) https://www.aeaweb.org/articles?id=10.1257/jel.54.2.442.
[21] *Id.* at 483.

lastingly.[22] A working paper by Marthews and Tucker examines the same event and finds similar results: terms that are either "personally-sensitive" or "government-sensitive" were impacted negatively by Snowden's revelations.

On a more theoretical level, even if one grants that government is the solution to supposed privacy harms, one shouldn't rule out the possibility of government failure either. After all, most economists and political scientists would say that government's foundational purpose is to protect private property rights. But that does not stop many governments from engaging in predatory behavior vis-à-vis their own citizen's person and property. Similarly, even if governments are explicitly tasked with the job of protecting consumer privacy, some may use their power to violate, rather than protect, that trust. Apple's 2016 battle with the federal government is a case in point. Some consumers may fear that Google, the largest repository of information in human history, might similarly draw the attention of federal officials looking to connect the dots on a U.S. citizen.

My survey results find support both for Acquisti *et al.*'s observations *and* the possibility that government abuse plays a role in generating dislike for information collection. Identity theft is consumers' biggest fear, with some 70% indicating it is a concern. Unsurprisingly, over half of respondents also expressed a distaste for spam and the uneasiness associated with not knowing who knows what. However, 43% express fear of "a government agency forcing an internet entity that has collected your information to hand over the information." By contrast, only 28% of digital consumers indicate that price discrimination is a concern for them.

My results should be interpreted cautiously. One obvious reason for caution jumps to the fore: consumers may have more information about Google than many other websites they visit. As a result, these results may lack external validity.[23]

VI. Conclusion

Arguments for privacy regulation are weakened by low privacy valuations, well-informed consumers, and the possibility that government itself generates distrust of information collection.

The results of this survey offer reasons to believe that, at least with respect to Google, consumers are willing to give up very little to acquire additional increments of privacy. Furthermore, they're also fairly well-informed. Perhaps even more significantly, respondents seem most informed when the benefits to being informed are higher, suggesting that consumers do not deviate significantly from rationality in digital environments. Lastly, the citizenry's

[22] *See generally* Jon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117 (2016) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.

[23] Trust is also an important factor. Are consumers more likely to trust Google or a smaller firm? Future research might explore whether people are willing to pay less or more to protect their privacy when interacting with entities that are less-established than Google is.

mistrust of government may be a reason to reconsider greater government involvement in privacy.

A regulation like the EU's forthcoming "General Data Protection Regulation" is imposing significant costs on companies as they prepare to become compliant.[24] Resources devoted to compliance mean fewer resources devoted to what markets do best: satisfying ever-changing consumer preferences. Even the most ardent advocates of additional oversight should consider whether the benefits that consumers reap from the new regulation outweigh the costs. This short paper hasn't analyzed the costs of privacy regulation, but it should give one pause before concluding that the benefits are both unambiguously large and positive.

[24] For a discussion on some of the many preparations firms are taking to become compliant, *see* Seb Joseph, *The State of the Ad Industry's Preparations for the GDPR, in 4 Charts*, DIGIDAY, Nov. 14, 2017, https://digiday.com/marketing/state-ad-industrys-preparations-gdpr-4-charts/; Jessica Davies, *Thanks to GDPR, the Chief Data Protection Officer is a New Key Role at Publishers*, DIGIDAY, Jan. 3, 2018, https://digiday.com/media/gdpr-made-chief-data-protection-officer-new-key-role-publishers/