THREE ESSAYS ON THE ECONOMICS OF DIGITAL PRIVACY

By

Caleb S. Fuller
A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
The Requirements for the Degree
of
Doctor of Philosophy
Economics

Committee:

_____ Director

_____

_____

_____ Department Chairperson

_____ Program Director

_____ Dean, College of Humanities and Social Sciences

Date: _____ Summer Semester 2017
George Mason University
Fairfax, VA

Three Essays on the Economics of Digital Privacy

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at George Mason University.

By

Caleb S. Fuller
Master of Arts
George Mason University, 2015
Bachelor of Arts
Grove City College, 2013

Director: Christopher J. Coyne, Associate Professor
Department of Economics

Summer Semester 2017
George Mason University
Fairfax, VA

ACKNOWLEDGEMENTS

I would like to acknowledge the generous financial assistance of the Mercatus Center, without which graduate school would not have been possible for me.

To all my past teachers, particularly those who instilled a love of learning and of economics: thank you! In particular, I am indebted to Jeff Herbener and Shawn Ritenour of Grove City College for showing by their example that devoting my life to studying and teaching economics is a worthy calling.

I would like to thank my insightful classmates at George Mason University who have been a constant source of inspiration, encouragement, and insight. In particular, thank you to David Lucas, Nicholas Pusateri, and Ennio Piano who have refined many of my good ideas and have corrected many of my bad ones. I am also extremely grateful for the friendship of Nicholas Freiling who has been not only a constant source of encouragement since freshman year of college, but also played a significant role in bringing chapter four of this dissertation to fruition.

A big "thank you" goes to my fantastic committee members who are indispensable sources of inspiration and model scholars. As my scholarly career begins, I realize how much I've learned from Chris Coyne's tireless mentorship, Peter Boettke's unparalleled ability to synthesize ideas, and Peter Leeson's razor-sharp logic.

Lastly, I wish to acknowledge the loving support of my family members without whom I certainly would not have made it this far in my academic journey. Specifically, I want to recognize the personal sacrifices that my parents (Steve and Kelly Fuller) and grandparents (Ed and Lynn Schisler) made to invest in my educational and personal development. Doubtless there are many others who have guided, encouraged, taught, and strengthened me through the years. Thank you all!

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

1. European Union (EU)
2. General Data Protection Regulation (GDPR)
3. Children's Online Privacy Protection Act (COPPA)
4. Department of Health, Education, and Welfare (HEW)
5. Health Insurance Portability and Accountability Act (HIPAA)
6. Fair Information Practice Principles (FIPPS)
7. Personally Identifiable Information (PII)

ABSTRACT

THREE ESSAYS ON THE ECONOMICS OF DIGITAL PRIVACY

Caleb S. Fuller, Ph.D

George Mason University, 2017

Dissertation Director: Christopher J. Coyne

Is the market for digital privacy a failure? If so, can governments improve on the unhampered outcome? This dissertation explores these related questions. The commercialization of the Internet—in addition to a host of other digital technologies—has pushed the issue of digital privacy to the fore. Surveys show that the modal individual is made uncomfortable by the common practice of Internet companies "tracking" their digital behavior. As a result of this, many scholars argue that the digital marketplace is a "classic market failure" due to information over-collection, and governments worldwide have initiated legislation to regulate the interaction between digital firms and consumers.

My first essay engages in a broad sweep of both the literature and existing digital privacy laws. In so doing, I find evidence for Kirzner's (1985) "perils of regulation." Such a finding suggests that regulation cannot always be costlessly and effectively implemented. The second essay argues that certain forms of digital privacy law, namely a mandated opt-

in, mimic a traditional price ceiling and thus generate the unintended consequences that accompany such interventions. Taken together, essays 1 and 2 suggest that governmental attempts to rectify the alleged market failure may generate a host of additional problems. Essay 3 marshals new survey data to suggest that the market is not a failure in the first instance. By way of survey analysis, I argue that there is little information asymmetry between firms and consumers, that consumers possess low willingness to pay for privacy, and that fear of government abuse contributes to consumer dislike of information collection.

CHAPTER 1: Introduction

This dissertation explores a small but growing topic in the law and economics literature: the economics of privacy. As Acquisti et al. (2016) note, the economics of privacy is best conceived of as a subfield of information economics with its roots in Hayek (1945), Stigler (1961), Akerlof (1970) and others. Specifically, this dissertation sheds light on issues within the economics of *digital* privacy, an area of investigation that promises to becoming increasingly relevant with technological innovation (Tabarrok and Cowen 2015). The economics of digital privacy traces its roots to theoretical explorations by Posner (1978, 1981) and Stigler (1980) of privacy in non-digital contexts (for example, an employer screening her applicants' histories or an individual examining and correcting information regarding his credit history).

Today's digital privacy scholars explore the concealment of non-sensitive information (an Internet browser's geographical location, search history, device information, and so on) in digital contexts.[1] Collection of non-sensitive consumer information—so-called "mouse droppings" (Berman and Mulligan 1998)—by web platforms is usually performed via use of cookies and web bugs, placed by advertisers who

[1] "Concealment of information" was the definition of privacy offered by Posner and Stigler. However, others like Hirshleifer (1980) dissented, preferring a more expansive, but perhaps less tractable definition: "autonomy within society."

are awarded "slots" on a platform in a real-time auction (Goldfarb and Tucker 2011; de Cornière and de Nijs 2016). These advertisers supply most or all of the revenue for many online platforms. But as Acquisti et al. (2016) argue, "…consumers have good reason to be concerned about unauthorized commercial application of their private information. 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," (483). Tucker (2012) echoes the latter concern.

In light of these concerns, many scholars advance two related propositions with respect to digital privacy. The first claim is that, due largely to information asymmetry between consumers and companies, the digital environment constitutes a market failure in which firms "over-collect" consumer information.[2] As Hirsch (2010) puts it, "Because the market for online privacy is characterized by highly imperfect and asymmetrical information, firms can collect and use far more personal data than they could in a hypothetical perfect market," (455). Claims like this one are often bolstered by appeal to survey evidence suggesting that consumers value their privacy highly, but that digital firms fail to respect it—that they "over-collect" personal information (Acquisti and Grossklags 2007; Turow et al. 2009; Acquisti et al. 2013; Acquisti et al. 2016). For example, Turow

[2] Brown (2013) sees two broad categories of "failure" with respect to privacy in digital markets. The first is the "individual failure" of consumers succumbing to a host of biases that cause their behavior to deviate from their best interests. The second category consists of more traditional "market failures"—in this case, information asymmetry and the negative externality of re-selling personal information to third parties.

et al. (2009) claims that 86% of young adults do not want targeted advertising if it results from tracking websites other than the one they are currently visiting.

The second claim is that governments can effectively correct the unhampered market's outcome (Hoofnagle 2005; Hermalin and Katz 2006; Hui and Png 2006; Acquisti 2012; Hoofnagle et al. 2012).[3] For example, Newman (2014) argues that the market's failure to provide sufficient digital privacy is analogous to the market failure in food and product safety that he believes characterized 20th century markets. In the same way that government is alleged to have corrected that failure, it should also correct this one. Sachs (2009) concurs, stating that "…these market failures must be addressed on more than one front" and that the past century of consumer protection laws "can be our guide to the next century, providing a valuable framework for evaluating and drafting laws that catalyze, rather than trivialize, the market for information," (251). Hoofnagle (2005) likewise states, "It is imperative that the Federal Trade Commission (FTC) act now to correct these market failures" and that "The FTC is capable of creating reasonable and effective privacy protections for American consumers."

Together, my three essays investigate the popular, twin notions that the digital marketplace is a failure with respect to privacy and, relatedly, that government can effectively correct this failure. Essays one and two address the latter claim, whereas essay three offers reasons to question the very premise that the market for online privacy is characterized by failure in the first place. The first two chapters advance the relatively

[3] Hoofnagle (2012) even goes so far as to say, "Government interventions in the direct marketing field have been choice enabling…Market interventions, on the other hand, often force choices on the consumer," (294).

modest claim that government solutions are imperfect and costly, thus suggesting that future research should admit the flaws of government solutions and shift focus to a comparative institutional analysis. The final chapter makes the much bolder claim that there is currently little problem in digital markets in the first place and thus little need for the *deus ex machina* of government to correct alleged deviations from perfection.

Essay one, "The Perils of Privacy Regulation," uses Kirzner's (1985) "perils of regulation" framework to illuminate several unintended consequences generated by digital privacy law. This paper argues that the optimism regarding government ability to address digital privacy concerns is unwarranted. The regulatory process has no access to the profit and loss feedbacks that guide and correct market participants, it often stifles entrepreneurial discovery, and also creates opportunities for unproductive entrepreneurial discovery. The second paper, "Privacy Law as Price Control," offers an alternative way to conceptualize digital privacy law. Taking the EU Privacy Directive as an example, this paper argues that a mandated "opt-in" is a price ceiling. As a result, we should expect to see the effects generated by a price control, albeit contingent on the particulars of the digital environment. My third essay empirically examines three oft-made claims in the economics of privacy literature that are harnessed to make the case for market failure. These claims are that consumers are ill-informed, that they value privacy highly, and that market phenomena alone are responsible for consumer dislike of information collection. By way of newly generated survey data, I challenge all three claims, thereby providing evidence that digital markets are not, as some (Hoofnagle 2003) have alleged, a "race to the bottom," but instead serve to reasonably approximate consumer demand.

CHAPTER 2: The Perils of Privacy Regulation[4]

I. Introduction

In a society where digital technologies are pervasive, few issues excite as much concern as does digital privacy. Governments' own track records of digital privacy intrusion notwithstanding, a significant fraction of individuals believe that government regulation is the necessary solution to privacy risks. A "post-Snowden era" Pew Report (2014) finds that 80% of American adults "agree" or "strongly agree" that "Americans should be concerned about the government's monitoring of phone calls and Internet communications." The same survey, however, finds that 64% of respondents indicate government should do more to regulate digital advertisers. This reveals a tension: the median American is fearful of government surveillance, but also tasks that institution with protecting him or her from unwanted digital privacy intrusion. Even in the early days of the Internet, Bibas (1994) reports that the legal status quo protected data privacy poorly and that the "predictable" American response was for a "law" and a "federal government agency" to assume the protective role.

Laypeople are not alone in these opinions. Hoofnagle, a law professor and outspoken

[4] I wish to thank Chris Coyne, Nicholas Pusateri, participants in George Mason University's Hayek Program's weekly graduate student paper seminar, and an anonymous referee for their helpful remarks on this paper. Any remaining errors are my own.

commentator on digital privacy topics, argues (2005) that the "[Federal Trade Commission] has to move into the 21st century and meaningfully address Internet privacy," that "the FTC should abandon its faith in self-regulation," and that "the FTC is certainly capable of protecting privacy online." Similarly, Solove, a law professor and digital privacy expert, remarks that, "the market in privacy is not a well-functioning market..." (2004: 87). He, along with Hirsch (2010), concludes that regulation is necessary to correct the deficiencies inherent in the unhampered market.

Using insights from the market process tradition in economics, I argue that calls for top-down regulatory solutions should be tempered by a full accounting of the costs which these regulations may impose. Other examinations of the costs of digital privacy regulation (Lenard and Rubin, 2009) have focused extensively on the ways that these laws constrict the free flow of information. As Lenard and Rubin (2009) indicate, this focus is due to the economist's preoccupation with the perfect competition model in which perfectly informed agents are the ideal. Though I also discuss the constriction of valuable information flows, I take a slightly different tact than authors such as Lenard and Rubin (2009) who have focused so extensively on that consequence of regulation.

Kirzner's conception of the entrepreneur and his extension of that type to analyze the effects of regulation provide the framework for my analysis. Market process theory has a tradition that emphasizes the "dynamics of interventionism" (Mises [1949] 1998; Rothbard 1962; Kirzner 1985; Ikeda 1997; 2005). As such, this analysis does not stop with the immediate effects of intervention, but seeks to trace its long-run, spillover impacts on other markets, industries, and actors. As this paper shows, digital privacy law generates perils by

failing to provide an analogue to the market's disciplinary corrective of profit-loss accounting, by stifling the market's discovery process, and by creating superfluous avenues of discovery.

Following Lenard and Rubin (2009), I examine regulations which curtail the collection and use of "nonsensitive information"–data which might be used to profile or identify an individual, but not information that could be used to gain access to the individual's assets (credit card or social security information). Neither do I deal with laws restricting the use of personal information for the purposes of false representation. This would include, for example, obtaining an individual's photo in order to impersonate them online. Privacy concerns that regulators commonly address and which are the focus of this paper include: the surreptitious collection of information by Internet vendors from visitors to their sites and the sale of that information to third parties. The justifications for this data collection are numerous, but common ones include the ability to target advertising directly toward interested consumers, to sell to third party data brokers, or to conduct market research on one's customer base.

Visions of a world where Internet merchants can accurately predict a consumer's reservation price or where employers can discriminate based on health risks surmised by culling data from an applicant's social media activity (two examples raised by Acquisti et al. 2016) may admittedly frighten the average Internet user.[5] Buchanan (2004) notes that many are "afraid to be free," and this appears notably so on the Internet. Some prefer

[5]See Hirsch (2010) for a more comprehensive accounting of the ways that websites may collect information and of the parties who have a vested interest in information collected on the Internet.

Buchanan's "parental socialism," desiring the state to impose privacy rules.

Government-mandated digital privacy rules are not neutral, however, with respect to the workings of the market; as Kirzner (1985) argues, all intervention stifles and redirects the market process. As such, this paper suggests that digital privacy law represents an opportunity for economists who have traditionally focused their attention on more prominent examples of intervention–antitrust, tariffs, taxation, and the like. Opportunity-cost reasoning suggests that it is impossible to precisely quantify the impact of digital privacy laws; if anything, this makes a thorough examination of these costs all the more important.

The paper proceeds in Section 2 with a literature review of the economics of digital privacy as well as a brief overview of the market process framework. Section 3 applies that framework to illuminate the perils of digital privacy law. Section 4 concludes with implications.

II. Literature Review

Posner (1978, 1981) and Stigler (1980) were among the first to provide an economic examination of privacy, defining it as the "concealment of information" or "secrecy" (Posner, 1981). Stigler (1980) writes that, "privacy connotes the restriction or use of information about a person..."[6] Posner (1981) argues that legislation which protects personal data results in efficiency losses due to information asymmetries, since employers

[6]Hirshleifer (1980) took issue with the Posnerian focus on "privacy" as "secrecy," arguing that "privacy" should be defined more expansively, likening "privacy" to "autonomy." For Hirshleifer, privacy as autonomy entails freedom from observation. I stick to the Posnerian conception.

can no longer gain access to applicant information. Personal information is an economic good in markets prone to adverse selection and moral hazard (Pavlou 2011). It follows that constricting the availability of such information reduces the efficiency of these markets.

Those advocating digital privacy regulation, however, often advance one of two closely-related arguments, the second of which is also based on appeals to asymmetric information. The first is that privacy is a fundamental human right that Internet companies often disregard. The second is that the market for digital privacy fails; consequently, regulation must correct the deficiencies inherent in the unhampered market.

Legal experts such as Solove (2004), appealing to privacy as a human right, assert that "law must intervene to protect privacy." Budnitz (1997) concurs that, "Regulation should interfere with the free market only to the extent necessary," but that, "consumers need a statute that grants government agencies the power to enforce privacy rights violations." Swire (2003) contends that economists favor a regime that permits open access to information because of their undue concentration on perfectly competitive markets and efficiency; this analysis "leaves out much of what people actually fear in the area of privacy protection," (2).

Government agencies also frequently appeal to rights-based language when addressing digital privacy concerns. "Big Data and Privacy: A Technological Perspective" (2014) refers to "privacy rights" throughout, stating that: "Collisions between new technologies and privacy rights should be expected to continue...," (4). Furthermore, "new privacy rights" emerge when technologies begin encroaching on "widely shared values" about which there is "consensus." One might reasonably question whether there is consensus on

a topic with as many gray areas as "privacy" (for discussions of what constitutes privacy, see: Warren and Brandeis (1890), Hirshleifer (1980), Posner (1981), and Henry-Scholz (2015)). As Solove (2006: 477) asserts: "Privacy is a concept in disarray."

Others appeal to market failure arguments. Hirsch (2010) argues that the market for digital information is rife with information asymmetry; thus, firms collect more information than they would in a "perfect market." For Hirsch, a "perfect market" is one in which users perfectly understand every reason–present or future–why a firm would collect personal information. As such, unregulated firms "significantly damage the privacy of Internet users," (449), and the "secondary use" of information collected online is "particularly vexing," (451), constituting a "serious invasion of personal privacy," (451). For this reason, he advocates a "co-regulatory" approach. Solove (2004) also complains of asymmetric information, concluding that "the market currently fails to provide mechanisms to enable individuals to exercise informed meaningful choices," (91). Milberg et al. (2000) argue that countries high in "uncertainty avoidance" are likely to embrace regulatory solutions to digital privacy problems. These authors find that discontent among the citizenry regarding corporate handling of citizen information is predictive of when governments will supply regulatory solutions to the perceived market failure (Milberg et al. 2000).

Though commentators advocating for some form of regulatory oversight probably represent the majority viewpoint, there are other voices that are more skeptical. Thierer (2014), for instance, notes that privacy legislation is characterized by the precautionary principle, a norm forbidding new innovations until they are proven "safe." Thus, "new

forms of digital innovation [are] guilty until proven innocent," (468). A few others have also raised concerns about the impact of digital privacy law on both innovation and consumer welfare (Varian 2009; Lenard and Rubin 2009; Goldfarb and Tucker 2011; Lerner 2012; Campbell et al. 2015). Varian (2009) notes that privacy regulation may raise search costs to buyers and sellers. Lenard and Rubin (2009) provide a helpful overview of the digital privacy landscape. They identify several costs of digital privacy legislation: reduced ability to match between consumers and producers as well as a likely reduction in innovation by Internet firms. Furthermore, they dispel several myths surrounding the collection of consumer data, noting for instance, that most firms anonymize it. Lastly, they also point out emerging, entrepreneurial solutions for the privacy-conscious consumer. Goldfarb and Tucker (2011) show a fall in advertising effectiveness in the wake of EU privacy legislation. Lerner (2012) demonstrates empirically that the passage of the EU Privacy Directive precipitated a decline in investment in advertising-supported Internet firms. Campbell et al. (2015) show that privacy regulation may serve as a barrier to entry for small firms.

The preceding papers are important; nonetheless, no market process analysis of digital privacy law has yet been offered. Previous analyses have not always rooted regulatory failure in the fundamentally different institutional context that guides market participants as compared to regulators. Furthermore, past analyses have not always taken the entrepreneur–whom Mises calls the "driving force of the market" ([1949] 1998: 325)–to be the primary unit of analysis. This paper attempts to fill that gap by focusing on the market's discovery process, facilitated by the entrepreneur. Thus, this analysis points out

that to the extent digital privacy law raises barriers to entry (to take just one example of many), it impedes the ceaseless churning of the market as entrepreneurs continually discover the prices, quantities, and qualities that satisfy consumer demands.

Before turning to a brief summary of the market process perspective, it should be noted that pronouncements of market failure in digital privacy rest on less than solid footing. Digital privacy legislation is a form of consumer protection. In the same way that regulatory agencies purport to ensure consumers' best interests by imposing food safety mandates,[7] groups like the FTC maintain they are correcting market deficiencies by passing digital privacy law. Such market-failure reasoning appears dubious, however. First, imperfect information does not imply that consumers are necessarily unable to act in accordance with their preferences. The information compelling every action is necessarily incomplete, but individuals still act with *ex ante* expectations of achieving their ends in an efficient manner. Second, some appeal to an artificial standard–for example, Hirsch's "perfect market"–in order to criticize real-world markets. This is a variant of the "Nirvana Fallacy" that condemns the real world to failure via comparison to an inherently unobtainable model (Demsetz 1969). Third, some express puzzlement at the lack of privacy protection that contracts provide. Yet, might the absence of such protection be evidence that consumers do not value it highly? Fourth, even if it were granted that markets under-provide a good, it would not follow that governments provide the optimal quantity (Kirzner

[7]Hirsch (2010) advocates a "co-regulatory" approach to protecting privacy in which governments and firms work cooperatively to set regulations. Incidentally, one of the most cited papers on the economics of co-regulation is an examination of its operation in the context of food safety economics (see Martinez et al., 2007).

1985).

Regardless of the soundness of market failure claims, market process theory illuminates several regulatory dangers that advocates of digital privacy law overlook. Identifying these perils is not a shut case against regulation since advocates might contend that the benefits outweigh attendant costs. Cataloging such costs allows us to evaluate the debate holistically, however. Kirzner (1985) examines three perils associated with any regulatory solution. First, he explains the *"unsimulated discovery process*."[8] Because there are no market prices providing feedback, government officials cannot know the appropriate price, quantity, or quality of a good to supply. Technology only heightens the complexity of the economic system, rendering it less knowable, a point that is highly applicable to discussions of digital privacy (Klein and Foldvary 2002). As I demonstrate in Sections 3.1, this lack of knowledge manifests itself, on the one hand, by the potential for regulators to *over-supply* privacy protection by constricting valuable information flows, and on the other hand, by the potential for regulators to increase security risks.[9]

Second, Kirzner explains "the most serious effect" of intervention, the *"stifled discovery process*." "Regulated restraints and requirements...block activities that have not yet been foreseen by anyone," (1985: 142). Because interventions into the market process impose

[8]Kirzner begins his discussion by exploring the "undiscovered discovery process." He uses this terminology to highlight that what has been labeled a "market failure" is, in fact, an opportunity for entrepreneurial profit. Calls for regulation frequently follow from the belief that entrepreneurs are incapable of solving alleged market failures. The focus of this paper is not on how entrepreneurs may solve digital privacy problems (though such research is worthwhile). Rather, the focus of this paper is on the ways that digital privacy law distorts the entrepreneurial market process, and thus I begin my analysis by discussing the "unsimulated" rather than the "undiscovered" discovery process.

[9]Note that a "security" risk differs from a "privacy" risk. The latter refers to the types of information I deal with in this paper: personal, but nonsensitive information. The former refers to sensitive information such as an individual's credit card number.

opportunity costs, they are impossible to measure. In Section 3.2, I demonstrate the myriad ways that digital privacy law stifles the entrepreneurial discovery process by erecting barriers to entry. Complementary to Kirzner's insight, Higgs (1997) argues that uncertainty about policy changes dampens investment activity. Higgs' insights complement Kirzner's– ever-shifting legal rules create an environment in which entrepreneurs experience heightened difficulty forecasting a project's rate of return. This concern is particularly applicable to digital technologies because they transcend rule-making boundaries. Questions concerning which rules will take precedence, which rules are more likely to be enforced, and which rules will impose a greater penalty for violations increase entrepreneurial uncertainty.

Finally, Kirzner notes that regulation generates "entirely new, and not necessarily desirable opportunities for entrepreneurial discovery," (1985: 144), the *"superfluous discovery process*." In the language of Baumol (1996), laws create the opportunity for "destructive entrepreneurship." Political actors may garner support by enacting legislation that favors domestic companies or industries at the expense of foreign competition. Because of the Internet's inherently "borderless" nature, however, it is difficult to prevent consumers from buying products or using services of foreign firms. To the extent that political actors seek to regulate, ban, or tax such practices, they risk the displeasure of their citizenry. At the same time, domestic Internet-based companies may look to the state for protection from foreign competition. In Section 3.3, I show how digital privacy legislation is one way that political entrepreneurs may balance these competing demands. Note lastly that Kirzner's perils are not mutually exclusive, and one can reasonably quibble that the

empirical examples I have provided for one peril might be categorized differently. For instance, Section 3.1 explains that regulators may impose solutions that do not jive with consumer preferences because the former lack access to market price signals. Such regulations have the potential to stifle the market's discovery process, a theme that Section 3.2 explores in greater depth.

III. Some Overlooked Perils of Digital Privacy Regulation

3.1 The Unsimulated Discovery Process

Consumers may, indeed, incur costs–as privacy law advocates contend–when they do not possess a protection right in their personal information. For example, individuals might prefer to visit websites without the "risk" of their data being collected and analyzed. There are, however, significant benefits that consumers reap from unrestricted information flow. I do not intend to argue that individuals bear no costs when others gain access to their personal information; the question, for every user, is whether attendant benefits outweigh the costs. Only demonstrated preference, expressed in the institutional context of private property and consent, can reveal the appropriate mix of privacy and the benefits that come from sacrificing that privacy.

Furthermore, as Acquisti and Grossklags (2005) have shown via survey evidence, consumers possess disparate tastes for privacy. Accordingly, consumers view privacy along a spectrum, acknowledging that additional privacy reduces other benefits they desire (Bergkamp 2003). Markets–and the price signals generated by them–provide the fine-grained solutions that balance these competing demands. By contrast, government plans to

restrict information flows often focus exclusively on the costs of accessing personal information, while understating the benefits. As such, regulation can persist in imposing "solutions" that do not accord with consumer preference for the reasons that Kirzner highlights in his discussion of the "unsimulated discovery process." Regulators are unfettered by the discipline imposed by losses that the market forces on failing entrepreneurs. Each consumer confronts both costs and benefits of unrestricted information flow, but only entrepreneurs possessing access to the price system can provide a service that balances these costs and benefits according to demonstrated preference. By contrast, government officials have no mechanism by which to discover appropriate prices or product quality. Furthermore, they cannot discover when they have erred in a previous regulatory decision (Kirzner, 1985).

The 2012 FTC report, "Protecting Consumer Privacy in an Era of Rapid Change," is one example of a government agency advocating a paternalistic approach that would seek to deny customers the ability to make the benefits-privacy tradeoff according to their own valuations. It states, "...companies are collecting, storing, and sharing more information about consumers than ever before...they should not do so at the expense of consumer privacy." The EU's Data Protection Directive, however, is a piece of already-existing regulation that focuses on the costs to the exclusion (of many) of the benefits of information flow.[10] It prohibits the collection and processing of personal data, except for in a few instances where the collector must shoulder an extensive burden of proof that the collection

[10]The Directive also contains provisions for protecting against true invasions of property, such as credit card theft.

meets stringent requirements. The restriction covers information collected by personal or automated means and extends to anonymized data.

The EU Directive further specifies a few exceptions to the general ban, but mandates that these exceptions be governed by "opt-in" (that is, individuals must consent to the collection). The Directive also mandates a "right to be forgotten." Individuals may force an organization to delete personal data when its "legitimate use" has expired. This rule inhibits the ability of firms to store information for opportunities which may not be foreseeable in the present, but could emerge in the future. In an unfettered market, each firm would be free to calculate whether the cost of continuing to store data is outweighed by possible future benefits. The proposed EU General Data Protection Regulation (GDPR) would intensify and unify the already-existing mandates contained in the Directive. Among many other strictures, the new law would raise the bar for an organization's ability to claim it has a legitimate reason for accessing and using consumer data (EU press release, 2012).

Varian (2009) and Lenard and Rubin (2009) have noted that a privacy regime that bans information collection or surveillance may increase search costs to both buyers and sellers. Targeted advertising saves firms' resources and time by increasing the probability of making a sale, even while reducing the total quantity of advertisements needed to achieve that sale (Lenard and Rubin, 2009). In the same way, consumers may learn of new products that are similar to others they have purchased in the past in a price range that is likely to fit their budget (Lenard and Rubin, 2009). Regulations that would ban the collection of this information prevent both buyers and sellers from discovering mutually beneficial matches or a new product that fits the consumer's preferences.

The lowering of search costs is not the only benefit from the unrestricted flow of information. Many of the most popular services on the Internet depend on unrestricted information flow. As of the first quarter of 2015, Facebook claimed over 1.44 billion users (Statista 2015) of their free application, supported by targeted advertising that depends on the collection of user information. Free social media services, such as Facebook, allow for a near-costless exchange of information. They also allow for a dramatic increase in the average person's number of "weak ties," Granovetter's (1973) term for socially distant acquaintances, who serve disproportionately as "bridges" to opportunities like jobs. LinkedIn is arguably the most prominent example of a site, dependent at least in part on collecting user information, that extends the reach of weak ties. As of the first quarter of 2015, the notable networking site had 364 million users (Statista 2015).

Free social media platforms have also enabled coordinated resistance to unpopular government action (Shirky 2011), notably in toppling Egyptian president, Hosni Mubarak in 2011 (Gaudin, 2011). This does not provide a complete account of all the benefits of free information flow or deny potential costs (such as the possibility of terrorists using free social media sites to coordinate activity), but it demonstrates the wide spectrum of potential benefits, all reliant on business models that utilize personal information.

Though over a billion users have demonstrated their preference for Facebook's service, the forthcoming EU regulation could spell the end of ad-based services, such as Gmail and Facebook, in Europe. Alternatively, those popular services may still operate in the European environment, albeit with a fee-based model (Heath 2013). Some commentators, nonetheless, see applications (like Facebook) that collect user data as incontrovertible

proof of market failure because they "place the burden of privacy protection on the individual," (Report to the President 2014).[11] Leaving privacy solutions to the market, however, allows individuals to evaluate the privacy-benefits trade-off according to their own, personal valuations, as opposed to regulatory approaches that impose a "one-size-fits all" solution. It also allows entrepreneurs to discover that level of privacy that best satisfies consumer demands. Because the regulatory process does not simulate the market's discovery process, it is impossible to determine whether new regulations accord with consumers' preferences.

Like social media platforms, the free provision of search engines also relies on the ability to customize advertising based on consumer browsing habits, location, and other collectible information. Besides the obvious benefit of providing free access to information, Google's search algorithm also bestows less apparent gains. Notably, this includes the generation of dispersed, local, knowledge that no individual mind could access. As one example, consider the new "ARGO," an algorithm based on the now-defunct Google "Flu Trends" model. This program detects search terms that indicate the presence of influenza, and even corrects for changes in the ways that individuals search (Yang et al. 2015). No single individual–not even a doctor who treats influenza patients–has access to the dispersed data that could convey information about the relative severity of the flu in a given locale. Though it is possible to collect such information by more traditional methods (hospital records, for instance), the analysis and dispersion of such

[11] An early study (Gross and Acquisti 2005) of Facebook and other social media sites revealed that young users, on average, did not express a high desire for digital privacy or anonymity, suggesting that the aims of privacy legislators become quickly outdated.

information would likely be time-consuming, costly, and irrelevant by the time it was analyzed. ARGO aggregates local knowledge, allowing researchers to quickly identify influenza "hot-spots." Consequently, in the future, it may facilitate the faster containment of epidemics as individuals are able to easily avoid hard-hit areas.[12] Researchers are optimistic that the algorithm will soon be able to incorporate data gleaned from social network sites like Twitter and Facebook (Mole 2015). Thus, in this case, the restriction of information flows would reduce the ability of search engines to solve problems on a scale never-before-seen. These examples indicate that policymakers–without access to profit and loss accounting–may provide more privacy protection than consumers demand. After all, if consumers are troubled by Google tracking their searches, they are free to switch to a more privacy-conscious search engine.[13]

Finally, because the regulatory process does not simulate either the local, specialized knowledge, or the profit incentives inherent in the market process, privacy regulation also has the potential to accomplish the opposite of its stated intentions–it may, in fact, increase security threats.[14] This fact is additional evidence for the "unsimulated discovery process" that governs decision-making falling outside the purview of profit-and-loss discipline.

One common practice for many online companies is to "anonymize" the information that they collect from consumers, making it difficult, if not impossible, to use this

[12]The knowledge that ARGO aggregates is Hayekian in the sense that it is localized and dispersed, though not tacit.

[13]For example, DuckDuckGo is a rapidly growing search engine that does not track individual's queries.

[14]Note that this paper focuses primarily on "privacy" risks, that is access to "nonsensitive" information, rather than on threats to "sensitive" information such as credit card theft. The latter fits more properly under the category of "cybersecurity." What this section demosntrates, however, is the ironic fact that bureaucratic efforts to shield privacy may, in fact, result in graver threats to one's own cybsersecurity.

information to identify specific individuals. The proposed 2015 "Consumer Privacy Bill of Rights Act"[15] would force firms to abandon such anonymization practices. The legislation states that, "Each covered entity shall, upon the request of an individual, provide that individual with reasonable access to, or an accurate representation of, personal data that both pertains to such an individual and is under the control of such covered entity."

This provision requires the explicit linkage of consumer identity with collected data in order to afford consumers' the "right" to the information collected about them. The EU's proposed regulation (the GDPR) would mandate similarly: it states the consumers must have access to their own data as well as the ability to transfer data between service providers (EU press release, 2012). As a result, these laws consolidate consumer identities and data in one place (say, a company's server), thus making this information less costly for identity thieves to acquire.[16] Consequently, legislation crafted with the intent to protect so-called privacy rights may enable serious property rights violations.[17] In a market-setting, entrepreneurs who selected for an arrangement that exposed their clients to higher levels of security risk would see either a decrease in their number of clients or would be forced to compensate them through the provision of some other beneficial service. The institutional environment of regulation, however, without access to the market's corrective feedback, does not incentivize the corrective adjustment that would closer align with

[15]This piece of legislation is based on the Obama Administration's 2012 "Consumer Privacy Bill of Rights."

[16]I am indebted to a 2015 blog post entitled "Innovation Death Panels and Other Shortcomings" by Geoffrey Manne at the blog "Truth on the Market" for the idea that the "Consumer Privacy Bill of Rights" exposes consumers to greater privacy risks.

[17]As Hirsch (2010) documents, providing consumers with "access" to their information–what this bill would do–is a cornerstone of the 1973 Fair Information Practice Principles (FIPPs) proposed by the Department of Health, Education, and Welfare (HEW).

consumer demands.

3.2 The Stifled Discovery Process

It is appropriate that what Kirzner identifies as the most "serious" peril–the stifling of the discovery process–should comprise the bulk of my examples. Though it is tempting to overlook relatively more innocuous interventions, such as digital privacy law, Kirzner emphasizes that the costs of stifling the market's discovery process are inherently unknowable. As he argues, "regulation...may discourage, hamper, and even completely stifle the discovery process of the unregulated market," (141).

Because regulation has dynamic and spillover effects, not every case of stifling necessarily occurs in the market being regulated. There is evidence to suggest that digital privacy law, for instance, has stifled the discovery process in industries ancillary to those that collect consumer data directly. Evidence for this claim comes from a case-study comparing the privacy practices of e-commerce companies in the U.S. and the U.K. Market process theory suggests that the market is comprised of rivalrous competitors, jostling on a variety of margins, not limited exclusively to price competition. For Internet firms, one such competitive margin is the provision of enhanced privacy protection, either through the company's own technology, or via services furnished by third-party quality ensurers. The existence of digital privacy law then may reduce the incentive for firms to compete on the margin of supplying privacy-conscious services.

Jamal et al. (2005) note that the relative absence of over-arching federal privacy law in the U.S. provides a natural experiment with which to compare the strict EU regulation that governs U.K. privacy practices. The authors examine practices and outcomes for 100 high-

traffic U.S. e-commerce firms and 56 similar companies in the U.K. First, they find no significant difference between the number of U.S. and U.K. firms which failed to honor their "opt-out" policy concerning email. Similarly, they find that consumers in both countries are vulnerable to a comparably small number of firms which "misbehave" with consumer data, indicating that the EU regulation does little to curtail so-called privacy violations.

They find, however, that U.S. firms are overwhelmingly more likely to engage in behavior that signals quality assurance in the form of privacy protection. First, the U.S. firms displayed their privacy policies much more prominently, making them easier to find. Second, of the 100 U.S. firms, 34 signaled their intentions by paying a fee to become certified by a third-party firm that conducts regular audits of e-commerce companies' privacy policies and allows their seal to be displayed on the audited firm's website. In the U.K., no firms had undertaken such measures, and the authors were able to identify only one U.K. company that even offered such a service (it served only 41 clients) (Jamal et al. 2005).

The results of this study suggest that it is easier for U.S. consumers to identify websites that value consumer privacy. Without regulation stifling the emergence of the quality assurance market, higher quality firms can signal their privacy practices by incurring a fee. Presumably, higher-quality firms find it more profitable to incur the cost of this signal, and thus consumers can infer the quality of a firm's privacy policies by the presence or absence of such seals. In the U.K., by contrast, consumers have fewer means to differentiate between the privacy practices of rival firms. Despite the public interest rhetoric of privacy

legislation, the actual consequence of privacy law can be to create an environment where it is difficult to ascertain which firms value privacy highly. As Section 3.3 shows, public interest rhetoric is not sufficient to guarantee public interest outcomes.

Regulation's stifling effect on ancillary industries notwithstanding, its impact is probably most keenly felt in the very industries at which the regulation is targeted. Regulatory impositions often directly stifle the entrepreneurial discovery process by the imposition of fixed costs. This is particularly relevant in an environment where firms frequently enjoy large economies of scale, as in the digital arena.[18] When economies of scale are widespread, fixed costs fall disproportionately on smaller, entrant firms. As an example, consider the Federal Data Protection Act that has governed German privacy issues since 1977. This legislation imposes significant fixed costs on even the smallest of firms. As Geiger (2003) details, the law applies to "private sector companies that process or use personal data from non-automated filing systems. Companies that collect or process personal data are required to appoint a data collection official within a month of beginning operations; the law states that this stipulation applies to all firms with four or more employees" (Geiger 2003). Such an imposition doubtlessly benefits large, incumbent firms at the expense of small, rival startups.

Campbell et al. (2015) discuss the EU's Directive which mandates that the use of tracking cookies be treated as an "opt-in" rather than an "opt-out" default. Under the Directive, if a website's owners wish to customize ads–to place ads based on a user's

[18]Once an Internet merchant has established a digital storefront, the marginal cost of acquiring and serving an additional customer is often very low.

browsing patterns–opt-in requires obtaining the user's explicit consent. Though not the focus of their analysis, these authors note that firms may use TrustE, a software provider that ensures compliance with the opt-in directives as handed down by the EU. As these authors describe, installing the TrustE software imposes a fixed cost on all firms seeking the ability to support customized advertising (Campbell et al. 2015).

One conclusion of this analysis is that firms with large economies of scale will not suffer as disproportionately by opt-in legislation as will entrant firms that must incur this cost prior to acquiring a customer-base. To the extent that digital privacy law has this effect, it stifles the discovery process undertaken by small or entrant firms. Further, the "opt-in" regime would benefit larger firms because it would require smaller firms to obtain a solicitation list on their own, a time and resource-intensive project that favors large firms. Under "opt-out" regimes, most small startups are able to simply purchase such lists (Litan 1999). As such, a shift to an opt-in regime would benefit firms that are first-movers, those having already developed a solicitation list prior to the change in the law. Furthermore, Pasquale (2013) notes that an increase in merger activity is one likely consequence of banning the third-party resale of personal information. Applying the same reasoning to a legally mandated "opt-in" regime indicates that firms struggling to build consumer solicitation lists may be incentivized to merge with larger, more successful rivals, thus reducing the number of competitors.

Ensuring legal compliance imposes other, subtler fixed costs due to the complexity of many digital privacy laws. Consider the EU Directive's "Principle of Accountability" as outlined in the 2014 "Handbook on European Data Protection Law." It states that

controllers must be able, at all times, to demonstrate compliance with EU digital privacy law to data subjects, the general public, and to regulators. The Handbook further specifies that documentation specifying what measures have been taken to ensure compliance must be made readily available. Presumably, large firms more easily absorb the costs of this compliance, as simply having more customers or data may not increase the quantity of documentation a firm needs in order to demonstrate compliance.

In the United States, the Children's Online Privacy Protection Act (COPPA), amended in late 2012, expanded the obligations of Internet companies beginning in 2013. These enlarged obligations require firms to provide direct notice of any company changes regarding collection or use of data from individuals under age thirteen. The amendments also stipulate that firms only retain information collected from a child for as long as necessary for the purpose collected (Federal Register, 2013). Due to the extent of such obligations, some commentators have labeled COPPA a "complex" law (Consumercal.com 2015). Describing how COPPA's complexity has influenced startups for which he has worked, technology executive Tom Sands[19] (email correspondence 2015) states, "COPPA has constrained my teams' past efforts to deliver solutions to those under thirteen years of age. The combination of significant development efforts required to meet the standards, necessary legal consultation to follow changes in the laws, and periodic certification reviews rendered it prohibitively costly to pursue that age group. Larger companies, with significant development and legal resources, are at an obvious advantage in these

[19]Sands is a technology executive who has experience with large companies as well as several startups, including several directly involved in providing digital privacy solutions.

scenarios."

Sands is referring to the economies of scale which allow large firms to absorb the legal compliance costs associated with COPPA in a way that is not available to startups with more limited resources. In Sands' experience, the costs of complying with COPPA proved to be so significant that it prevented entry into the market for those under age thirteen. Consequently, this regulation imposed a cost on the startup owners and employees, but it also imposed a subsequent cost in the form of restricting the total quantity of discovery that firms in the economy were undertaking.

Digital privacy consultant, Daragh O'Brien, writing in a popular outlet (PrivacyAssociation.com 2014), further discusses the stifling consequences of digital privacy law. In O'Brien's experience, entrant firms often undertake substantial investments before they consider the obligations that digital privacy law requires of them. Ignorant of these laws, entrepreneurs may have acquired a customer list by illegal means; regulators then force them to surrender that list, perhaps the primary or only asset that the firm owns. He notes that the penalties for violation of digital privacy law are increasing, such that they will soon "bury" even the most well-funded startups. O'Brien's advice to entrant firms is that they take measures to protect themselves, but all such measures are inherently costly, thus favoring larger, entrenched competitors. He suggests, for example, that firms hire a "chief privacy officer" or a "data protection officer" to ensure compliance with privacy law. He also suggests that firms should only enter certain markets, such as the EU, after extensive due diligence.

Relatedly, a market process perspective also suggests that the EU mandate to discreetly

dispose of data after the purpose for which it was collected has been fulfilled stifles the potential for entrepreneurial innovation. It is impossible for any individual or firm to perfectly foresee future market opportunities because the market process continually reveals new information. As such, it is strictly impossible to know when any given piece of information has outlived its "usefulness." Because entrepreneurs are constantly alert to localized knowledge that is specifically relevant to their own industries or firms, they are both the most knowledgeable and most interested decision-makers concerning the costs and benefits of continuing to store data after its initial utility has expired. They can calculate whether they are willing to incur the cost of additional storage in return for an uncertain future use of the data that has not yet been discovered.

The laws discussed above directly stifle discovery by imposing fixed costs via technological, staffing, legal compliance requirements, and the stricture to promptly dispose of data. The opportunity costs of such regulations are the small up-start firms that never emerge as a result of these additional hurdles. From the entrepreneurial market process perspective, fewer entrepreneurs means fewer discoveries of the most consumer-satisfying resource allocations.

Direct stifling is not the only possible consequence of regulation, however; indirect stifling of the discovery process is also possible. Higgs (1997) notably identifies the uncertainty induced by capricious law-makers as the explanation for depressed levels of private fixed investment during the 1930's; this paper's analysis extends his insights to pre-existing laws that contravene each other. With regards to digital privacy legislation, this effect has been almost completely (if not entirely) ignored in the existing literature. Higher

levels of uncertainty raise the cost to potential firms from entering the market. Thus, uncertainty has a "stifling" quality that resembles the barriers to entry that compliance costs and other strictures raise. Higgs' argument conflicts with those, such as Milberg et al. (2000), who argue that privacy legislation reduces uncertainty.

The EU's proposed GDPR echoes Milberg et al. (2000) by stating that its measures will improve consumer confidence online, thus providing a boost to European growth (EU press release, 2012). The regulatory approach, however, while potentially reducing the uncertainty of Internet users, actually *increases* the regime uncertainty of Internet entrepreneurs. It does so by two primary channels. These include a.) the contradictory patchwork of digital privacy laws and b.) the notably "open-ended" wording of privacy legislation, which permits bureaucratic, discretionary enforcement.

The patchwork characteristics of U.S. privacy law have led some to call it a "sectoral model." That is, law-makers pass rules reactively[20] to address privacy concerns that are peculiar to specific industries. The result is that "new legislation is introduced whenever new technology raises privacy concerns," (Craig and Ludloff 2011: 28). This approach raises uncertainty for all firms that are innovating new digital technologies. When viewed from a global perspective, the situation is similar. As Neef (2014: 212) states, "data privacy laws are being altered day-to-day in nations all over the world." The outcome of such shifting goal-posts is inevitable entrepreneurial uncertainty, an unseen cost, largely ignored in the literature. As innovators observe this pattern of reactive legislation, they may become

[20]Note that Milberg et al. (2000) argue that one benefit of digital privacy law is that it would *correct* the "reactive" failures of private firms.

increasingly cautious about investment opportunities.

Commentators refer to U.S. privacy law as "piecemeal" and "bottom-up" as compared with the stricter, "top-down" approach favored in the EU (Craig and Ludloff 2011). In the U.S., federal, digital privacy law primarily regulates two industries–health care (via HIPPA) and financial services (via the Gramm-Leach-Bliley Act)–as well as one population demographic–children under the age of 13 (via COPPA) (Craig and Ludloff 2011).

The reason, then, that U.S. privacy law is "piecemeal" is due to the contradictory nature of the state laws. An informal publication by the law firm of Oliver and Grimsley (2013) states that, "privacy law is a mess–a hodge podge of state laws..." Furthermore, digital privacy law at the state level is outright contradictory (Jolly 2014). Though the Commerce Clause limits a state's legislative power to its borders, the "borderless" nature of the Internet permits state-enacted privacy legislation to be enforced in other states (Ezor 2012). Consequently, the contradictory nature of state digital law is likely to be more impactful than other areas of state law which, though contradictory, are limited, in jurisdiction, to the state border.

One such example of state-enacted privacy law, which has the potential for far-reaching consequences, is California's 2003 Online Privacy Protection Act. This law stipulates how businesses which serve California residents must post their privacy policies, what such policies must contain, and even the font size and color by which the privacy policy must be displayed. Though the legislation only extends to California customers, it binds all companies who serve them, thus encompassing any U.S.-based Internet company.

Consequently, the technological nature of the Internet has rendered the rule constraining state power to state borders a meaningless one. From a Higgsian perspective, the result can only be greater uncertainty on the part of entrepreneurs who must account for state law other than that of the state in which they operate.

The aforementioned publication by Oliver and Grimsley concludes that a landscape of disparate state laws is best addressed by "some national, preemptive legislation...for businesses so they do not have to worry that they are violating some esoteric rule buried in some regulation, or some arcane state law," (Oliver and Grimsley 2013). In short, this proposed solution promises to "standardize" privacy law in the U.S., reducing the costs to small and entrant firms of understanding and complying with privacy law.

This proposed solution is likely a shortsighted one. Due to the inherently "boundless" nature of digital technology, it is difficult for nation-states to effectively regulate it, as it transcends geopolitical borders. Even if the U.S. adopted standardized privacy laws, it is doubtful that these laws would coincide perfectly with legislation passed in the EU or other parts of the world that regulate digital activities. Questions concerning the application and enforcement of digital privacy law in other countries would presumably still encourage a regime of uncertainty on the part of U.S.-based firms that anticipate an international customer base.[21]

Finally, to propose a standardized, international privacy law, while possibly serving as a corrective to consumers' uncertainty, would likely only exacerbate the knowledge

[21]Obviously, the same conclusion holds for entrepreneurs in any country.

problems explored earlier. To take one potential problem, consider that different societies possess differing norms concerning privacy, or that the privacy demands of those in emerging markets likely differ from those in developed countries. A globally unified privacy standard would be ill-suited to address such diverse, localized concerns. A standardized approach to U.S. digital privacy law also fails to take into account that the global trend is for less, not more, standardization of regulatory approaches to privacy issues (Neef 2014).

Overlapping and conflicting digital privacy laws are not the only impediment to investment. Bergkamp (2003: 123), describing the EU Data Protection Directive writes, "...privacy in Europe is like pornography in the U.S.: the government will know a privacy violation when it sees one." Nebulous and "open-ended" legislative rhetoric also heightens uncertainty. Technology executive, Sands, has stated that, "Uncertainty regarding implementation and enforcement of digital privacy law has delayed my teams' entry into certain foreign markets," (email correspondence 2016). This insight further militates against Milberg et al. (2000) who argue that legislators enact privacy law to satisfy citizens' "uncertainty avoidance." Even if privacy legislation reduces the uncertainty faced by the consumer, it likely increases the uncertainty faced by the innovator. Thus, the impact on overall innovation and growth is indeterminant at best.

Such a case-by-case understanding of privacy law imposes uncertainty on entrepreneurs who can never be certain–even after examining previous case law–whether they are in compliance. One hypothesis to explain the prevalence of open-ended privacy legislation is the rapidly-evolving nature of digital technology. Because regulators are unable to forecast

what the market's discovery process will reveal, they may purposefully craft legislation that encompasses a wide range of possibilities. Such open-ended legislation reduces the costs of having to continually craft new legislation or amend prior law. Instead, sufficiently vague law can be applied to novel situations. Thus, the speed at which digital technology evolves may be the impetus for a regulatory response that heightens the level of entrepreneurial uncertainty.

As an example, consider the EU Data Protection Directive that grants consumers a right to their personal data, and uses words such as "reasonable," "fair," and "justified" to describe the benchmark that Internet companies must meet in order to comply while collecting, accessing, storing, or distributing personal information. As another example, Singapore's 2012 Personal Data Protection Act also applies a "reasonableness" test to how organizations collect, use, and disclose personal information. Not only is there uncertainty surrounding what constitutes an "unreasonable" breach of the law (courts have developed competing interpretations), there is also uncertainty about the jurisdictional scope of the law, whether it extends, for example, to foreign companies who might collect information from native Singaporeans (Olswang 2012).

While Bergkamp (2003) notes the loss of civil liberty that attends the use of vague legislative rhetoric, market process reasoning informs that legislation which grants rule-making to bureaucratic decision-makers also decouples these actions from the discipline of profit and loss. As such, bureaucrats are more likely to make decisions in accord with their unique preferences. Because market participants are not privy to these bureaucratic preferences, they face increased uncertainty concerning the scope of the law, and encounter

disincentives to invest in technologies or business processes that may come under scrutiny. It is impossible to quantify the cost of such uncertainty, as it consists of potential firms that never enter or existing firms that refrain from innovation.

Uncertainty about judicial interpretation of privacy law is particularly disincentivizing toward long-term investments. Entrepreneurs can only know how the law has been applied in the past and whether such application has been inconsistent. Coupled with the fact that digital technologies change quickly, thus rendering digital privacy law quickly obsolete, entrepreneurs face a highly uncertain investment environment. With judges inconsistently interpreting ever-evolving legislation, entrepreneurs may be incentivized to avoid technologies or innovations that might be seen as privacy-intrusive, but which confer other benefits on consumers.

Section 3.2 has offered evidence for Kirzner's "stifled discovery process." In some cases, the stifling potential of these laws is more obvious than others. Directly imposing fixed costs is relatively easier to identify than is the fact that these strictures may impede the market's discovery process in ancillary industries, such as firms that specialize in third-party certification of other companies' privacy practices. In Section 3.3, the paper turns to the closely related "superfluous discovery process." Though one side effect of the "superfluous discovery process" is to stifle entrepreneurial discovery, it also generates the added harm of creating opportunities for entrepreneurs to engage in wealth-destroying discovery. Rather than investing resources in discovering the most profitable avenues by which to serve consumers, entrepreneurs may turn to digital privacy laws as a way to protect their own economic interests at the expense of their competition.

3.3 The Superfluous Discovery Process

Not all entrepreneurship is productive; it can, in fact, be destructive, contingent on the institutional setting (Baumol 1996). Because legislation creates new, "superfluous" avenues for entrepreneurial discovery, firms can leverage digital privacy law to further their interests. Opportunities created by legislation are not necessarily wealth-enhancing or consumer-satisfying. Frequently, they consist of opportunities to strangle competition or sink resources into transferring rents. I examine a few cases that illustrate the standard rent-seeking concerns.

A 2015 *New York Times* article reports that Facebook is being probed by European regulators, under both antitrust and privacy violation allegations. As Facebook has become increasingly diversified, it offers not only its traditional social media platform, but also messaging and photo sharing services. After acquiring several messaging applications, Facebook drew the ire of large European telecommunication companies which began lobbying for increased antitrust oversight to curtail the "virtual monopoly" the social media site has over "how people send messages on their smartphones," (Scott 2015). The deputy director of enforcement for data protection in France, however, also comments on the Facebook case that, "there are privacy issues," (Scott 2015).

Given Facebook's diversified nature, it is possible for telecommunications companies–firms not directly affected by digital privacy law, but which do compete with Facebook in offering messaging services–to lobby for privacy legislation that makes it costlier for the company to operate in Europe. Firms seeking to compete directly with Facebook as a social media platform may have little incentive to lobby for privacy laws that would disadvantage

themselves also, but firms that compete with Facebook on other margins, such as communication services, *do* have an incentive to lobby for restrictive privacy law. As Facebook has become more diversified, the firm inches closer to becoming a substitute for traditional telecommunications providers. The result is that digital privacy legislation may strike a blow at Facebook, while leaving the telecommunications firms unscathed. Thus, the very existence of digital privacy law creates a superfluous opportunity for entrepreneurs to innovate new ways to leverage the privacy strictures to their commercial benefit.

As another example, consider European cloud storage providers that are positioned to benefit even more directly from the forthcoming imposition of stricter digital privacy laws in the EU. Zettabox is a data storage startup which is anticipating that increased stringency of EU privacy law will allow them to compete with giants such as Amazon and Google. Though only employing 25 individuals at the time of this writing, Zettabox founders believe they are well-positioned to benefit from a new European Parliament law that will fine violators up to 100 million euros or 5% of global annual turnover, whichever is larger, for digital privacy violations. The law, which extends to every Internet company that does business in the EU, prohibits the transferal of data out of the EU unless the firm has gained explicit user permission (PCWorld.com 2015). Zettabox, based within the EU, promises to avoid these issues for European users by storing all data in EU data centers. U.S. companies, such as Amazon, have responded to the legislation by opening locations in Europe (TechWorld.com 2015).

Zettabox is just one example of a startup that not only benefits from the existence of strict privacy laws, but in fact, centers its entire competitive strategy around the hampered

ability of Amazon, Google, and other providers to effectively navigate EU privacy law. As such, the entrepreneurial leadership of Zettabox capitalized on the opportunity that the newly emerging configuration of digital privacy laws afforded. The analysis of Zettabox is important not because it is economically so significant (at least not yet). Rather, it demonstrates that digital privacy law is unambiguously altering the pattern of entrepreneurship that would exist on the unhampered market. Scarce resources are being shifted into the data storage industry, but such funneling would not occur without these laws. Whereas Section 3.2 highlighted the ways that digital privacy law stifles the entrepreneurial discovery process, the existence of Zettabox proves that these laws also create opportunity for superfluous discovery that would be unprofitable in an unregulated market. As such, these laws shift entrepreneurs' discovery capabilities (and scarce resources) into lines of production that would be entirely superfluous in the absence of the law creating the new opportunity.

Finally, additional evidence that rent-seeking may be a motive in legislating privacy law comes from a closer look at EU privacy law in practice. As Viktor Mayer-Schonberger (2010) details, European individuals have overwhelmingly chosen not to enforce their digital privacy rights in court, despite the extensive levels of protection that EU law grants them. He finds that in Germany, a country of 80 million citizens, not a single individual selected to enforce his or her digital privacy rights in the courts during the 1990's. This suggests that it is not the citizenry who lobby for the imposition of strict privacy law. If not the citizenry, then perhaps certain entrepreneurs favor the laws because they present an entry barrier to their rivals.

The preceding discussion demonstrates that digital privacy legislation may shield domestic firms from their foreign rivals. Kitchenman (cited in Bergkamp 2003: 150) confirms this observation when he states that, "Restrictions on the flow of information in a more information-oriented age may be the equivalent at the dawn of this new century to tariffs between nations at the dawn of the last." Regardless of whether digital privacy law merely happens to raise barriers to entry or whether such barriers result from the explicit intent of special interests, these laws subvert the discovery process of the market. Consequently, consumers encounter less product variety, higher prices, lower quality, and a diversion of resources to rent-seeking ends. Because these costs are unseen, it is tempting to ignore them altogether. Instead, this paper has sought to illuminate some of them in order to yield a more comprehensive analysis of digital privacy law.

IV. Conclusion

The preceding pages have provided evidence for all three of Kirzner's perils. Such concerns should inform ongoing regulatory efforts. For instance, in late 2010, the White House Council created a Subcommittee on Privacy and Internet Policy and instructed it to, "promote innovation and economic expansion, while also protecting the rule of law and individual privacy," (cited in Campbell et al. 2015). This paper has offered several reasons to question whether those dual mandates–promotion of innovation and protection of individual privacy–are compatible ones. As such, this paper has three primary implications.

First, the current literature under-values the market process perspective on digital privacy problems. The literature on the economics of privacy is small; perspectives that

incorporate the entrepreneur are nearly absent altogether. This is a gap to be filled by economists seeking to explore how regulation stifles and redirects the market process. Economists working in this tradition might find it worthwhile to examine the ways entrepreneurs have responded to alleged failures in the market for digital privacy.

One view on digital privacy contends that the business models of e-commerce firms necessitate an inevitable "race to the bottom" with respect to consumer privacy. That is, these firms, in their pursuit of profit, must increasingly intrude on the privacy of their users in order to gain information that will confer a competitive edge. This view forms the basis of many who view regulation as the best (or only) way to curtail privacy-intrusive behavior.

Another perspective views privacy as just another margin on which firms compete. Companies such as Dropbox post their privacy policy prominently; they state they will collect personal information, but will not sell it to third parties. Other firms do engage in third-party resale. Furthermore, the presence of firms that "violate" personal privacy is not *ipso facto* evidence of market failure. Consumers possess disparate tastes for privacy and those firms that seemingly encroach on privacy may be offering other services that their competitors do not, and to customers who are willing to make the trade-off. It is presumptuous to assume that consumers have not made the appropriate cost-benefit calculations concerning their own privacy.

Future research could serve to adjudicate between these competing worldviews, and might start by exploring real-world entrepreneurial solutions to privacy issues. This paper briefly explored "web seals" as a way for firms to signal the quality of their privacy protection. Additional research in this area would doubtless illuminate other innovative

firms solving privacy issues as well as other mechanisms that entrepreneurs use to signal quality.

Second, the costs of digital privacy legislation may be extensive. The common theme uniting the problems that this paper highlights is the universal presence of opportunity-cost reasoning. The costs of privacy legislation are not easy to quantify or directly observe because they frequently consist of foregone opportunities of which all individuals remain unaware. There is extensive debate in the legal philosophy, computer science, and economics literatures about whether the state has a responsibility to enforce property rights in information that individuals generate in the digital arena.[22] This paper should inform that debate by highlighting some of the perils that such government-enforced privacy protection may entail.

Third, this research indicates that even seemingly "innocuous" legislation, such as digital privacy law, creates newly profitable avenues in the form of rent-seeking opportunities. Additionally, these laws carry the potential for future expansions of both scale and scope. Economists are well-aware of the rent-seeking opportunities that "major" interventions such as antitrust, tariffs, or monopoly grants entail. As illustrated by the case of Zettabox, however, privacy laws also create previously unrealized gains that entrepreneurs act to exploit. Furthermore, as Kitchenman documents, laws that restrict information flow–such as privacy laws–may be the 21st century equivalent of Mercantilist policies that dominated the world of centuries-past. Economists should thus look to analyze

[22]See, for example, Posner (1978, 1981), Stigler (1980), Bibas (1994), Clarke (1999), Lin (2002), Sarathy and Robertson (2003), Mayer-Schonberger (2010), Pavlou (2011), Pasquale (2013), and Henry (2015).

laws that may fly under the radar compared to other pieces of legislation that have traditionally captured their attention.

Bibas (1994), in a prescient article on digital privacy law, anticipates the knowledge problems that regulatory solutions impose. This paper, employing insights from the market process perspective, suggests that the problems of digital privacy regulation may be even more pervasive than Bibas anticipated. In an increasingly digital landscape, there has never been a more important time to examine the thorny issues that privacy raises. This paper calls economists who appreciate the entrepreneurial market process perspective to enter the discussion. Without their voices, regulatory responses–ones that preempt the entrepreneurial solution altogether–may be the inevitable outcome.

CHAPTER 3: Privacy Law as Price Control[23]

I. Introduction

Facebook founder and CEO, Mark Zuckerberg, claims that privacy is no longer a "social norm" (Johnson 2010), but survey evidence belies the assertion. For example, some 50% of American adults believe that online advertisers should not save a record of their digital activity. Furthermore, 93% say that being in control of who can access information about them is important (Madden and Rainie 2015). These attitudes notwithstanding, Internet companies such as Facebook and Google serve as platforms (middlemen) that enable advertisers to quietly collect large quantities of consumer information. Though thousands of companies engage in this behavior, it is difficult to estimate precisely how many firms rely on this model. However, the business strategy is an important source of revenue for several of the world's largest companies. Of the roughly $75 billion earned by Google in 2015, most of it is attributable to the company's ad business (Rosenberg 2016). Spending by firms on targeted advertising continues to grow due to its effectiveness relative to non-optimized advertising, a finding established by Yan et al. (2009) and Goldfarb and Tucker

[23] I also wish to thank Chris Coyne, Peter Leeson, Paola Suarez, David Lucas, Nicholas Pusateri, and two anonymous referees for their helpful comments on this paper. Any remaining errors are my own.

(2011).

Companies employing this model do not always disclose the nature or future uses of the information collected, leading some to conclude that information asymmetry is a pervasive feature of digital environments (Solove 2004; Hoofnagle 2005).[24] Due to this characteristic of digital interaction, many have argued that government regulation may be able to curb privacy-invasive practices. Here, I stick with Posner and Stigler's conception that privacy is the "concealment of information" (Posner 1977, p. 393) or "the restriction of the collection or use of information about a person or corporation," (Stigler 1980, p. 625). Such a definition is most amenable to the analysis of digital privacy, as well as to economic analysis more broadly.[25]

Regulation of digital privacy stems from fears regarding two potential uses of consumer data: illegitimate, fraudulent activity as well as legitimate activity that consumers frequently decry, such as behavioral ad targeting and price discrimination (De Corniere and De Nijs 2016). The most noteworthy regulation addressing these concerns is the European Union's (EU) 1995 Privacy Directive; yet, a theoretical analysis of that law has yet to be supplied. My paper seeks to fill that gap.

Scholars argue that consumers are frequently unaware that they are being tracked while online and are often ignorant of the type of information being collected. Because of this

[24]Note that firms themselves may collect information as in the case of Google saving all searches. Alternatively, firms may simply serve as the platform that enables advertisers to collect information.

[25]There are many different conceptions of privacy, however, even within economics. For example, Hirshleifer (1980) critiques the Posner-Stigler conception. As Tucker (2016) states: "Economics has struggled to arrive at a unified theory of privacy." Solove, a legal scholar, concurs: "Privacy is a concept in disarray," 2006. Thomson (1975) observes: "Perhaps the most striking thing about the right to privacy is that nobody seems to have a very clear idea what it is."

information asymmetry, some have concluded that digital privacy is inadequately protected and that the digital arena is a "classic example of a market failure," (Gertz 2002). As a result, many scholars suggest a government-imposed regulatory regime (Milberg, Smith, and Burke 2000; Gellman 2002; Solove 2004; Taylor 2004; Hoofnagle 2005; Hui and Png 2005; Hermalin and Katz 2006; Turow et al. 2009; Ohm 2010; Peppet 2011; Acquisti 2012; Pasquale 2012; Newman 2014; Acquisti, Taylor, and Wagman 2016).[26] Imperfect information is said to lead to "over-collection" relative to the perfectly informed ideal (Hirsch 2010, p. 455). As Hirsch (2010) notes, imperfect and asymmetric information can lead firms to "collect and use far more personal data than they could in a hypothetical perfect market."

One scholar has even ventured to argue that, because of alleged digital privacy violations, the Internet is little better than the Wild West (Hoofnagle 2003). Similarly, Newman (2014) contends that the 21st century's market failure in digital privacy is reminiscent of the 20th century's market failure in information about food and safety. Other scholars, however, take a more moderate perspective, contending that governments and firms must work together to craft digital privacy law (Kesan and Gallo 2006; Hirsch 2010). To the problem of information asymmetry, Solove (2004) adds that large Internet-based firms are able to exploit consumers due to bargaining inequity with respect to the surrender of information. Acquisti and Grossklags (2007) argue that behavioral biases, which could lead a consumer to undervalue privacy protection, only compound the problem of

[26]Some have noted that self-regulation, a way of establishing industry standards, is an alternative to government regulation. Most evaluations of self-regulation of digital privacy, however, have been negative (Swire 1997; Hoofnagle 2005; Hirsch 2010).

information asymmetry.[27]

Unsurprisingly, given these arguments, existing legislation aimed at curtailing information collection is advanced under the rhetoric of consumer protection. As a few leading economics of privacy scholars state: "Consumers have good reasons to be concerned about the unauthorized commercial application of their private information. 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," (Acquisti, Taylor, and Wagman 2016, p. 42). The most prominent example of regulation aimed at these concerns is the EU's forthcoming General Data Protection Regulation (GDPR), ratified in 2016, which states that: *"The protection of...persons in relation to the processing of data is a fundamental right...This Regulation is intended to contribute to the accomplishment of an area of freedom, security, and justice..."* Thus, those suggesting regulatory approaches to privacy see regulation as unambiguously welfare-enhancing.

My paper contributes to a small literature on the unintended consequences of digital privacy regulation (Stigler 1980; Posner 1981; Lenard and Rubin 2009; Goldfarb and Tucker 2011; Lerner 2012; Rochelandet and Tai 2012; Campbell, Goldfarb, and Tucker 2015; Kim and Wagman 2015; Fuller 2016).[28] These unintended consequences include

[27]It seems just as plausible, on the grounds of behavioral economics, that consumers might over-value their privacy. After all, a standard result in the behavioral economics literature is that individuals may over-estimate the probability of rare events, such as a privacy breach.

[28]Stigler and Posner examine broader privacy regulation, rather than digital privacy regulation specifically, but their analysis is applicable to the digital environment.

erecting entry barriers for small firms and increasing consumers' search costs. Even this literature, however, has devoted little attention to how firms–specifically ad-supported platforms–have adjusted to regulations that lower their profitability. Goldfarb and Tucker (2011) demonstrate that the EU Directive reduced average digital ad effectiveness, but their study stops short of exploring how firms responded in the wake of decreased ad effectiveness. Similarly, Lerner (2012) shows that venture capitalist investment in digital ad-supported firms fell in response to the Directive, but he does not explore the response by the affected firms. Theoretical examinations of the consequences of digital privacy law are even rarer. Romanosky and Acquisti (2009) offer a theoretical analysis of three potential regulatory approaches to data breaches, (*ex ante* regulation, *ex post* liability, and information disclosure), but perform no similar analysis of consumer privacy regulation.[29] Nonetheless, how firms react to digital privacy legislation is considered to be among the most important questions in this burgeoning literature (Acquisti, Taylor, and Wagman 2016, p. 479). Lastly, none of the foregoing papers makes my specific contribution: a reconceptualization of privacy law as a price control.

Despite fears regarding firms' privacy policies, information collection by firms serves a vital role in the so-called digital economy, a role so seminal that its absence would all but preclude some of the most popular sites on the Internet. Consumers surrender their data in exchange for web content, thereby enabling firms to charge a non-pecuniary "price" by way of this information collection. The EU Directive, by permitting consumers to side-step

[29]The topic of "data breaches" might be better categorized as a "cybersecurity" issue.

this price, effectively offering nothing to the firm in exchange for its services, acts as a price control. As a result, the traditional effects of price-fixing may follow in the wake of such digital privacy law: tie-in sales, altered investment patterns, and adjustment on other margins of the exchange. One of the oldest policy-related interests of economists—the theory of price controls—is applicable to one of their newest interests: digital privacy.

Some observers have noticed that digital advertisers in Europe employ more "creative" ads, relative to their US counterparts (Fulgoni, Morn, and Shaw 2010). Europe has also seen an explosion in the use of in-app purchases (Wauters 2014). One hypothesis to explain these differences is that European consumers have more intense preferences for creative or dramatic advertisements—or that the European consumer reacts more strongly to them than does the US consumer. An alternative hypothesis is that firms in Europe face differing constraints relative to those in the US. Foremost among these differences in constraints is the EU Privacy Directive that curtails the information-collecting practices that are so common among US-based firms. The observed differences between the two markets are thus a consequence of there being the "same players," albeit ones in a "different game," (Buchanan 2008).

Section 2 describes how information functions as a price in digital environments and how a mandated opt-in regime acts as a price control. Section 3 provides a more detailed analysis of the EU's regulation in practice and how it maps to a price control. Section 4 applies the theory of price controls to illuminate three effects the control may engender in digital markets. Section 5 discusses the political economy causes of privacy price control. Section 6 concludes with a few implications.

II. "Privacy Price Control" in Theory

There is a long tradition in economics of applying established theory to phenomena that have not yet been recognized as falling within the theory's purview. In an example from the economics of digital privacy literature, Farrell (2012) applies the taxonomy of final and intermediate goods to ask which better characterizes "privacy."[30] Similarly, Gneezy and Rustichini (2000) argue that "a fine is a price." The authors apply well-accepted price theory to a traditional topic in law and economics that invited a greater degree of clarification. To point out that privacy law is a price control is a similar endeavor.

The Internet's most frequently-trafficked sites are "free" in the sense that they charge a zero pecuniary fee, yet they require a non-pecuniary payment: information. Facebook is one example. The world's largest social media site boasts over 1.7 billion monthly active users as of late 2016 (Facebook 2016). While Facebook charges a zero money-price for accessing its services, the site does collect information from its users, as described in the company's "Data Policy," a document describing what types of information are collected.

Using the original site as a platform, advertisers collect various forms of "non-sensitive" data (IP address, geographical location, browsing history, or device information) through the use of surreptitious technologies, such as web bugs and cookies (Goldfarb and Tucker 2011). This data is then used to strategically place advertisements, a practice known as "targeted" or "behavioral" advertising. Typically, advertisers bid for space on platforms in order to have the privilege of access to consumers' information (De Corniere and De Nijs

[30]Farrell concludes that privacy is best analyzed as a final good rather than an intermediate good sought for the end of achieving some other good.

2016). Websites and those seeking to advertise in digital environments may also join an "ad network" (such as Adblade) that connects Internet platforms and firms attempting to engage in targeted advertising. As such, data collection forms the backbone behind the free provision of countless Internet services: social media sites, search engines, and a host of others.

The preceding paragraph describes the nature of the interaction between firms and consumers in the absence of any regulation: consumers visit the site and the site collects their information. Thus, the (unregulated) default is that sites may collect the information of any consumer on their site. Is this the appropriate legal default? A brief examination of the property rights arrangement reveals that this default mimics more traditional market exchanges. The website (and any associated services it provides) is owned by the website owner; thus, it should be unsurprising when a visitor is asked to make a payment upon her visit to the website owner's property.

In fact, a near-identical collection of consumer information occurs in many brick-and-mortar establishments. For example, many grocery stores now offer a frequent shopper card that collects and stores a record of consumer purchases so that stores can better tailor their offerings. Furthermore, countless owners of physical property attempt to secure that property via the means of security cameras, which collect the "information" of those setting foot on the property. Though "explicit consent" is not obtained from the consumer before engaging in this information collection, few argue that these practices constitute a violation of individuals' privacy (or property) rights.

In the above example, we could describe the information that has been surrendered as

comprising part of the price of accessing that property. If an individual wishes to acquire an orange at the grocery store, she pays not only the price of the orange, but may also surrender information to the frequent shopper database or to the security camera. To the extent that the latter "payments" confer disutility on her, the effective price of an orange at this store is greater than at a comparable store where she only pays the pecuniary price (Alchian 1967). Presumably, the privacy-sensitive consumer would buy a greater quantity of oranges from the store that did not collect information. In fact, there is empirical evidence that individuals are sometimes willing to pay a small premium for websites that better protect consumer privacy (Tsai et al. 2011).

The "total price" of many goods is comprised of both pecuniary and non-pecuniary components, but some prices may be entirely non-pecuniary. After all, a price is simply an exchange ratio. It is true that in a money-using economy, most prices are quoted in terms of money units, but that is not a necessary condition for something to be a price. If someone exchanges five apples for ten oranges, the price of an orange is half an apple. Thus, a price is the payment that one party makes to another in exchange for a good. By extension, if I visit an ad-supported website, the price I pay for consuming that site's content is the information collected about me upon my visit. This information might consist of the address of the site I visited just prior to the site in question, the address of the site I visited just subsequent to the site in question, and my geographical location. To the extent that uncertainty or information asymmetry obscures the nature of the information being collected, those too, are a non-pecuniary component of the price that consumers pay. Presumably, the modal consumer prefers more transparency to less, and so will view more

uncertainty as contributing to a higher effective price.

Of course, many firms (like Google) *voluntarily* enable browsers to opt out of providing information. Relatedly, consumers can adopt anonymization technologies that obscure their personal information. Because consumers can anonymize and thus forgo paying the full information price, it is true that the analogy to the price control may not be perfect, as one is not permitted to avoid paying the price of a good in traditional markets. However, and critically, individuals rarely alter the default, which in the unregulated world, is information collection (Acquisti, Taylor, and Wagman 2016). This is because there is typically some cost involved with obscuring one's digital activity. For instance, even sophisticated and privacy-sensitive Internet users may have a high opportunity cost of time and thus may not want to search for anonymizing techniques (Acquisti and Varian 2005).[31] To the extent that regulation reduces the quantity of individuals who are opted-in by way of changing the default, then the regulation acts as a price control by increasing the quantity of individuals who are not paying the price. Evidence also suggests that it is costly for firms to persuade users to switch the default setting (Goldfarb and Tucker 2011, p. 69).

The site offers the user content; the user offers the site information. Eventually, interaction between website owners and visitors establishes an equilibrium quantity of collected information. While information collection confers benefits on the collector, it is also costly. Costs include not only the technical ones of investing in technology suited for collection, but also the reputational ones that a firm might incur if consumers are

[31]Other companies, like Facebook, voluntarily implement an opt-in default in which service is conditional on surrendering certain personal information. Given that these firms have already implemented opt-in, we would expect them to be relatively less adversely impacted by a mandated opt-in.

uncomfortable with some aspect of the information collection (such as quantity, content, or process). Such information collection is not ancillary to the interaction between firms and consumers. Without this exchange, many "free" services would simply not exist, just as sellers of traditional goods cannot provide them for free. Furthermore, the use of personal information as a price is likely due to its efficiency relative to alternatives, such as paying a pecuniary fee. For example, the transaction costs associated with paying a fraction of a penny every time someone used Google Search would likely discourage large quantities of Internet activity.

Information's role as a price in the digital economy, as just described, is acknowledged by some policy-makers, legal scholars, and economists. For example, Farrell (2012, p. 261) observes: "...consumers can...make... payments to firms by viewing ads, and firms can make payments to consumers by offering free attractive content." Like all exchanges, both parties surrender some good in exchange for another good they value more highly.

Even some critics of this business model acknowledge that it mirrors a traditional transaction that relies on money for the medium of exchange. Critics lament, however, that consumers may not be fully informed about the details of the exchange (Whittington and Hoofnagle 2012). Whereas some firms' privacy policies state explicitly what information the firm will collect from visitors, other policies are less explicit, leaving the consumer to guess. As Hoofnagle and Whittington (2013) state, citing Facebook as an example: "These exchanges often carry a hidden charge: the forfeit of one's personal information." One could reasonably question just how "hidden" Facebook's "charge" actually is—the company posts its privacy policy prominently and in plain-language. Hoofnagle and

Whittington (2013) object, however, because the company represents itself as being "free" (the company states prominently on its homepage: "It's free and always will be") when, in fact, it charges a non-pecuniary price by collecting consumer information. These scholars, then, acknowledge the exchange relationship between firms and consumers, but wish it was more transparent. Put alternatively, these scholars wish the price consisted of an observable pecuniary fee, rather than the less observable non-pecuniary information collection.

If personal information is the price that consumers pay for a website's services, then regulation that sets a price other than the market price is an instance of price-fixing. A large body of scholarship explores the effects of price controls. The traditional theory of price controls is so familiar to economists that a literature review is superfluous.[32] Indeed, there are few policies that generate as much consensus among economists as does the detrimental effects of rent control (Alston, Kearl, and Vaughan 1992; Jenkins 2009). Traditional theory states that a binding price ceiling is one in which the legal price is set below the equilibrium price. A ceiling set above the equilibrium price would be a price control, but would be irrelevant, as it does not impinge on any exchanges.

By extension, a law that enables web visitors to sidestep providing the information that the firm is seeking (thereby creating a zero-information price) sets the legal price below the market price, making the control a binding one. If the market price of my visiting a site equals the information on the sites I visited just prior and subsequent to the site I am

[32]See Cheung (1974) for a survey of the literature on price controls.

currently browsing, then a law permitting me to obscure that information is a binding price control because it sets the legal price below the equilibrium price.

What justification exists for setting the legal price below the equilibrium price? Hirsch (2010) alleges that information asymmetry between firms and consumers results in "over-collection" of consumer information by digital firms.[33] Similarly, Acquisti and Grossklags (2007) worry that behavioral biases lead consumers to surrender a greater than optimal quantity of personal data. Solove (2004) appeals to bargaining inequity to argue that consumers over-surrender their information. Another way to state these "over-collection" claims is that the "price" paid by consumers is greater than it would be in a model where information is perfect, where consumers are perfectly rational, and where bargaining power is equally distributed. Consumers would be willing to pay less in such a perfect-information world (Hirsch 2010). As a result, a regulation (i.e. a price control) which permits consumers to pay less than the market-clearing price moves the real world closer to the model's ideal.

One such regulation is the EU's Privacy Directive, the mechanics of which I describe below. It mandates that merchants collect consumer information only after acquiring consumer consent, thereby permitting consumers to deny firms the information they require as payment. By removing a digital "good"—personal information—from the public domain, the EU law significantly alters the nature of exchange activity between digital

[33]Consumers may indeed be unaware of all the uses to which a firm collecting their data will put it. Given that they continue to visit such sites, however, the costs of discovering this information must outweigh the benefits they receive from visiting the website. The presence of information asymmetry does not change the fact that this is an exchange between firms and consumers. Consumers can refrain from the exchange if they are made uncomfortable by the lack of information, just as someone could refrain from purchasing a used car for the same reason.

firms and visiting consumers. Before the law, websites charged consumers a "fee" in the form of personal information collected; after the law, consumers are legally permitted to avoid paying the fee. The law creates the potential for an "exchange" in which the firm is forced to accept a zero price for providing its services.

Mandating opt-in as a solution to digital privacy differs from a policy that simply informs consumers about the information-price they must pay to access a site's services. In the latter case, after receiving the information about the "true price," a consumer has two choices: visit the site and pay the price or refrain from visiting the site to avoid paying the price. Thus, browsers already possessed a property right in their information before the Directive; no one forced them to surrender their information unless they chose to visit an ad-supported site. The opt-in regime permits a browser to, in effect, "have his cake and eat it too." A visitor can now choose to both visit the site and also refrain from paying the price that would exist in the absence of the opt-in policy. I explore the precise mechanics by which this happens in Section 3.

Thus, the mandated opt-in, by altering the default property rights configuration, mimics traditional price ceilings which permit consumption of a good at sub-equilibrium prices. Just like in those traditional cases, however, we do not expect profit-maximizing firms to do nothing in the face of their altered constraints. Rather, we expect adjustments on myriad margins as firms search for their second-best constrained optimum. The case of digital firms is no different than their physical analogues. Supposing that the market is in equilibrium prior to the mandated opt-in, the latter restriction acts as a shock that generates search for the optimal (i.e. "second-best") margins of adjustment–the subject of Section 4.

Before turning to the particulars of the EU Directive in practice, it is helpful to note a few ways that digital privacy law *differs* from a standard price control. First, it is not clear that the privacy price control obscures the relative scarcities of goods, as do traditional price controls. The price system is an important conveyor of information, but that characteristic derives from the fact that money-denominated prices allow for a common unit of comparison between goods (Hayek 1945). By contrast, the quantity and quality of information that websites collect is not amenable to quotation in a common unit. Second, privacy law does not set a uniform price that all consumers must pay. Rather, it alters the total number of individuals who are paying the zero information-price. However, "...price control is applicable to any contract so long as the income receivable by one or more of the contracting parties is regulated to a fixed amount," (Cheung 1974, p. 57). Such is the case with digital privacy law, though here the "income" is comprised of information. Third, websites are non-rivalrous, at least within a range. An additional browser on a site does not impede another's ability to view the same site. Consequently, we may not expect to see a large queue forming, at least one traditionally conceived.[34] There might still be a "shortage" of sorts, as some websites are forced out of business or reduce the quality of their offerings (more on this later).

III. "Privacy Price Control" in Practice

The EU began regulating digital privacy in 1995 via the "Data Protection Directive," since

[34]Of course, beyond a point, additional users increase the probability of a website crashing.

updated in 2002, 2009, and 2016.[35] The EU's Charter of Fundamental Rights states in Article 8 that: *"Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned..."* The Directive codifies this right. In 2002, the EU passed the "Privacy and Electronic Communications Directive" as an update to the 1995 Directive. Compliance with the 2002 law results "in a loss of valuable marketing data" for digital firms (Baumer, Earp, and Poindexter 2004, p. 410).

In this context, loss of marketing data translates directly into a loss of revenue. This loss of data (and thus revenue) derives from the way the law functions in practice. Web bugs are widely-used pieces of code that enable advertisers to track consumers–even across websites–and thus collect the "price" that websites charge. The Directive instructs that the placement of web bugs be governed by an "opt-in" default. As the Directive states: *"Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting a website,"* (EU 2002).

Granted, under the 2002 Directive, there is much legal ambiguity surrounding what constitutes obtaining a consumer's "consent" to data collection (Goldfarb and Tucker 2011; Borgesius 2015). But many firms have responded cautiously to the legislation, ensuring that they only collect data for targeted advertising purposes after explicit consent has been given (Goldfarb and Tucker 2011).[36] Lawyers adopting a cautious approach to the law have

[35]There is no overarching, federal digital privacy law in the US. However, Japan, China, South Africa, and Singapore have joined the EU in regulating digital privacy at the national level.

[36]Even in the case where "consent" is interpreted to mean that the visitor's default browser settings accept

even advised that sites not store IP addresses unless explicit consent has been obtained (Goldfarb and Tucker 2011, p. 60).

Consequently, the law functions as a price control: it prevents websites from collecting the full information-price that would prevail on the unhampered market, unless consumers consent to paying the full price. Importantly, the regulation reduces the ability of advertisers to optimize their offerings, resulting in a 65% decline in effectiveness for the average digital ad (Goldfarb and Tucker 2011), suggesting that the price control is a binding one.[37] The regulation does, indeed, impinge on the flow of information from consumers to firms and third-party advertisers.

In 2009, the EU further updated its 2002 Directive, clarifying that the opt-in default also applies to the placement of "cookies," pieces of data stored in a web-user's browser and used to track browsers across sites (this is sometimes referred to as the "Cookie Directive") (Goldfarb and Tucker 2011). In my terminology, the cookie collects part of the information price from browsing consumers. Between 2002 and 2009, cookies had been subjected to an opt-out default, but the 2009 amendment shifts the default information property rights to consumers while they are on websites.

For the purpose of applying the logic of price controls, it is then critical to determine whether websites may *exclude* browsers who do *not* opt-in. In other words, are websites able to effectively restrict their offerings only to those willing to pay the full (i.e. the

cookies, the logic of price control is still applicable. After all, a browser may change her browser's default settings, especially if prompted by a pop-up privacy notice. Most consumers will not change their default settings, but the law does alter the total number of consumers paying the full price.

[37] "Effectiveness" was measured as the "stated intention to buy" the product that had been advertised.

unhampered) information price? In fact, many websites have responded to the Directive by attempting to exclude "non-payers," through use of technologies like the "tracking wall," which effectively prevents those who have not opted-in from accessing the site (Borgesius 2015). By implementing a tracking wall, a firm forces a "take-it-or-leave-it" choice on the consumer: they may opt-in and enjoy access to the site or not opt-in and be restricted from access.

Such an ability to exclude non-payers would seemingly call the logic of price control into question. There are four primary reasons, however, why the logic of price control is still applicable.

First, the EU has *attempted* to significantly curtail the use of exclusionary techniques such as tracking walls. Consider the following statement by the EU's Article 29 Working Party: *"In some Member States access to certain websites can be made conditional on acceptance of cookies, however generally, the user should retain the possibility to continue browsing the website without receiving cookies or by only receiving some of them,"* (Borgesius 2015, p. 233). The committee further states: *"...websites should not make conditional 'general access' to the site on the acceptance of cookies,"* (Borgesius 2015, p. 233). In other words, websites are not supposed to exclude someone simply for refusing to opt-in. Nonetheless, Borgesius notes that use of "tracking walls" to exclude is somewhat common. This is due to the fact that implementation of the law is somewhat ambiguous and because enforcement may be weak, as may be the case with all instances of price

controls.[38]

The extent of enforcement may be a topic for future research, but the Article 29 Working Party, an advisory body to the EU on the application of the Directive, has commented that access to most websites should *not* be made contingent on opting-in. Thus, a Working Party commentary states: "*...the user should retain the possibility to continue browsing the website without receiving cookies or by only receiving some of them, those consented to that are needed in relation to the purpose of provision of the website service, and those that are exempt from consent requirement. It is thus recommended to refrain from the use of consent mechanisms that only provide an option for the user to consent, but do not offer any choice regarding all or some cookies*," (Kohnstamm 2013).

Once again, however, there is ambiguity as noted by one legal scholar who comments: "The careful phrases suggest that the Working Party doesn't mean to say that all take-it-or-leave-it choices are prohibited," (Borgesius 2015, p. 234). While stopping short of banning all tracking walls, the Working Party states that "websites should not make conditional 'general access' to the site on acceptance of all cookies," (Kohnstamm 2013). To draw the parallel to a price ceiling again, the browser is supposed to be permitted to consume the majority of a site's content at a sub market-clearing price.

Second, there are several cases in which a firm is almost certainly prohibited from implementing an exclusionary mechanism–even if the EU wishes to turn a blind eye to other cases of tracking wall implementation. These cases include when the firm is relatively

[38]Though rent control exists all over the world, there is large variance in enforcement between locales (Arnott 1995, p. 100).

monopolistic, when there are high switching costs to exiting a firm's services, when the firm primarily serves children, or if a service has millions of customers/browsers. Even if other firms are permitted to install a tracking wall, these firms are explicitly prohibited from doing so (Borgesius 2015, p. 234).

Third, firms may voluntarily elect to not exclude those not opting-in for various reasons. One reason might be that the considerable ambiguity surrounding the enforcement of the opt-in law might incentivize some firms to adopt a precautionary stance of not excluding those who do not opt-in. A second, perhaps more compelling reason, might be that it is better to have a non-opted-in consumer on the website–a consumer who can still be exposed to non-targeted ads–than to have no consumer at all. After all, advertisers are still willing to get their ads in front of consumers, though they are not willing to pay as much for a non-targeted advertising slot as when the ad is targeted. That average ad effectiveness fell in the wake of the EU Directive is evidence that many EU websites have non-opted in consumers browsing them (Goldfarb and Tucker 2011). Thus, it may be the case that not all firms are prohibited from excluding non-payers by way of technologies like the tracking wall. Many firms may opt to not exclude, however. This is analogous, again, to the case of rent control: a landlord would rather have a tenant paying the rent-controlled price than no tenant at all.

Fourth, additional research on the impact of these restrictions is also relevant because the EU recently unified and strengthened the measures contained in the earlier Directive by way of the forthcoming General Data Protection Regulation (adopted in mid-2016), set to replace the Directive and take effect in mid-2018. As Article 7 of the GDPR states:

"*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract,*" (EU 2016). In other words, the GDPR judges consent to not have been freely given if access to a firm's services is contingent on surrendering information. Unlike the Directive, which leaves implementation to EU member states, the new Regulation automatically applies to member states. It would be surprising if legal battles were not fought in the wake of the GDPR, but the current wording indicates that use of exclusionary technologies is prohibited.

In sum, the logic of price control is not applicable to those firms which are permitted and find it profitable to exclude. These may include small firms, not primarily serving children, who do not have a monopoly position, or where enforcement of the price control is relatively weak. Nonetheless, the logic of price control is applicable to many EU-based firms that are prohibited from exclusionary techniques: large firms, those primarily serving children, those judged as being monopolistic, and those where bans against exclusionary techniques like tracking walls are enforced. Furthermore, the logic will seemingly apply to all EU firms collecting information under the GDPR which takes effect in mid-2018.

IV. Unintended Consequences of "Privacy Price Control"

In what follows, I describe three major areas of "unintended consequences" that often follow in the wake of price-fixing. The challenge is identifying how these effects manifest

themselves in the digital context. My claim is *not* that there will be a complete absence of these effects in markets without the price control (for example, in the US market where there is not yet comprehensive, EU-style privacy regulation) and that they only manifest themselves in markets subject to the price control (the EU). Rather, I am contending that there should be an increase in these phenomena *relative* to the unregulated market. While phenomena such as tie-in sales are often associated with a restriction like rent control, this is not to deny that they often also result from competition between sellers in a purely free market. For example, a landlord may tie the purchase of the apartment to furniture in an unhampered market, but such a decision becomes all the more likely when rent control is imposed. Additionally, there is reason to believe that should a seller implement tie-in sales when these are contrary to consumer preference, that seller will be out-competed by other sellers offering more favorable terms. The imposition of rent control, however, enables the implementation of tie-in sales to exploit the excess demand.

4.1 Tie-In Sales

A free market requires an absence of regulation on contractual terms, such as the transferability of goods (Cheung 1974). Yet, a mandated opt-in regime—as codified in the EU Directive—alters the terms on which personal information is transferred to the Internet platform attempting to collect it. As such, this law acts as a partial attenuation of the right to receive "income" (information) from website visitors. For many firms, revenue from advertisers, who pay to access this information, constitutes the major (or only) source of income.

Rent control is among the most commonly explored examples of price-fixing. In this

familiar case, the law attenuates, by means of a price ceiling, the income that landlords may earn from tenants. Like digital privacy law, the stated intent of rent control is to benefit consumers. Specifically, it is claimed that poorer tenants will experience increased welfare because less of their income will be devoted to housing, a good for which demand is relatively inelastic. For decades, however, economists have documented the harmful effects of rent control, effects that fall disproportionately on the poorest tenants, in part because high-income housing is usually exempt from the price control.

In the face of a price control, parties that are harmed resort to second-best methods of maintaining their profitability. One textbook method by which landlords adjust to the attenuation of their income is through the implementation of tie-in sales. A tie-in sale exists when the purchase of one product is mandated by the purchase of some other product offered by the same seller. The emergence of tie-in sales under a regime of rent control is due to the fact that price controls cannot control every aspect of an exchange (Barzel 1997, p. 16-32). As a result, landlords may attempt to recoup their lost income (and also exploit the queue that exists under rent control) by tying the sale of apartment accoutrements to the sale of the lodging itself. Common tie-in sales include a "key fee," whereby the landlord charges a potential tenant a substantial fee to acquire the key to the apartment. Another common example is the practice of charging for the furniture contained in the apartment– when that furniture was previously subsumed under the apartment's market price.

An opt-in regime, which permits the consumer to pay a zero price, also fails to control anything other than a few, narrow characteristics of the initial exchange of information for services. As a consequence, website providers are also free to implement a form of tie-in

sales themselves. Thus, Internet platforms may shift from services offered for "free" (that is, a zero pecuniary price) to fee-based models.[39] There may be many instances of these models arising on the unhampered market because they are superior at satisfying consumer preferences in a cost-effective manner. Whereas landlords may implement "key fees" or tie the purchase of furniture to one's rental contract, website owners may implement "free trials," "in-app purchases," or "premium" features (often referred to as "freemium"), now for sale, that were previously available for free.

Most Internet users are familiar with the use of the free trial. During a free trial, the website entices potential consumers by offering free services. After the free trial has expired, consumers must pay if they desire continued access to the site's services. This payment may be a one-time fee, or more often, consist of a "subscription model" that requires monthly or annual payments. The in-app purchase is another technique that mimics the key fee. In this model, users download a "free" application that has "hidden" fees inside that the user must pay if he wants to gain full access to the application's capabilities. Though most commonly used in gaming applications, websites might also employ this model in an attempt to recoup the lost revenue from advertisers. The in-app purchase is a way for websites and application producers to tie the purchase of game-enhancing features to the purchase of the game itself, thereby mimicking the key fee. For those concerned that information collection is problematic because such a practice is fundamentally "hidden," it is instructive to note that digital privacy regulation may

[39]Any empirical investigation of a shift to fee-based services must be careful to distinguish market-driven adoption of such business models from adoption following as a direct consequence of regulation.

encourage a greater number of other "hidden" business practices, such as in-app purchases. In fact, recent surveys indicate that in-app purchases are the least popular monetization technique among those who play mobile games. The model ranks behind other popular montization methods, such as video advertising and premium pricing (Handrahan 2016).

"Forced up-trading" is related to the phenomenon of tie-in sales. Commonly, sellers will produce several product lines of varying quality that are priced accordingly. The existence of price controls may incentivize producers to drop the lower-quality good in an attempt to "force" consumers to shift to the more expensive product. Alternatively, producers may discontinue production of the lower-quality product because it is no longer profitable under the price control regime. Observers noted this practice by clothing manufacturers during WWII price controls, as well as by steel manufacturers during the Nixon-imposed price controls (Rockoff 1992). Internet sellers frequently offer "premium features" for which consumers must pay in order to access. At the same time, many other features of the site may be free. In the face of a price control, websites can engage in forced up-trading by dropping many of their free features, while retaining the paid, premium features. Relatedly, a website could implement a payment for a premium feature that was previously made available for free, what is commonly referred to as a "freemium" model. Common features that are restricted in a freemium model include storage space, time, bandwidth, and user support (Kincaid 2009). The privacy price control incentivizes the marginal firm–that is, the firm most unable to maintain its profit margins in the wake of the new imposition–to adopt business models such as these.

4.2 Investment Flight

Price controls alter the pattern of investment that would exist in their absence. This is a direct consequence of the price control lowering the rate of return from engaging in the activity whose price has been capped. As an example, when legislators impose rent control on low-quality housing, this reduces the rate of return from supplying low-quality housing. Consequently, investment in high-quality housing–not subject to the price controls–experiences an increased rate of return, relative to investment in low-quality housing. Entrepreneurs begin shifting capital goods out of the construction of lower-quality housing stock and into higher-quality stock.

In the digital context, this argument implies a lower rate of return from advertisers using Internet platforms as opportunities to collect consumer data. Advertisers' willingness to pay for advertising space likely falls because the information they are able to collect is less optimized.[40] As a result, investment may flow out of areas where the privacy price control has been imposed (ad-supported websites), and into non-price-controlled areas.

The first consequence of the tendency for investment to flee the price-controlled good is less specific to price controls *per se*, as it is to any regulation that raises the cost of business. That is, we may see a greater quantity of ad-supported Internet firms, *ceteris paribus*, registering in non-EU countries relative to the EU. Currently, the EU's Directive applies only to firms that are based in the EU, and not to firms based outside the EU, even

[40]Intuition suggests that laws curtailing the use of targeted advertising will cause revenue to Internet platforms to fall because digital advertisers are willing to pay less for non-optimized ad space. Hummel and McAfee (2015) show theoretically, however, that targeted ads can, under very specific conditions, reduce the revenue to the platform firm. Such a result follows from the combination of highly-optimized targeting and a few dominant bidders for ad space.

when EU citizens visit their site.[41] The Directive provides a specific example of a general principle. Just as rent-controllers do not set prices for the entirety of the housing stock, so too privacy price controllers cannot set the privacy policies of firms outside their jurisdiction. Consequently, investment in digital ad-supported business may flow out of the privacy price-controlled area. In fact, the argument is even narrower than this: investment will flow out of *firms* that are price-controlled and into *firms* that are not price-controlled, regardless of the specific locale of those firms. To the extent that some firms are permitted to erect "tracking walls," a possibility described in Section 3, we would not expect these firms to see as large a decrease in investment as those which are barred from using such exclusionary techniques.

Second, the privacy price control has been shown to have disparate effects. As Goldfarb and Tucker (2011) demonstrate, the 2002 Directive reduced the effectiveness of the average digital ad dramatically. They note, though, that this effect is only detectable on "general interest" websites. Specific interest sites, by comparison, did not experience a decrease in the average effectiveness of their advertisements. The authors hypothesize that this is because advertisers already possess a fairly accurate profile of the average visitor to a specific interest site. Someone frequently visiting a blog dedicated to long-distance running is more likely than the average consumer to be interested in purchasing high-quality

[41]One possible complication is the "EU-US Privacy Shield," which replaces the "International Safe Harbor Privacy Principles." The "Shield" governs the transfer of EU-citizen data from the EU to the US. The "Shield" is legally contested and applies to "personally identifiable information" (PII). As Goldfarb and Tucker (2011) note, it is not clear whether "clickstream data" should be categorized as PII or not. Nonetheless, as Goldfarb and Tucker (2011) find, there is a difference between US websites and EU websites regarding the quality of information they are able to collect from an EU browser. This suggests that, at least in practice, there is a significant difference between the way the EU rules apply to US and EU firms.

running shoes. Those visiting a general interest site (say a news site) are more likely to be a random consumer whose preferences are not as easily ascertained.

It follows that the practice of targeted advertising is a more valuable activity on general interest sites. One implication deriving from Goldfarb and Tucker (2011) is that the privacy price control may reduce the share of general interest sites relative to specific interest sites. Such would be an example of investment flowing out of an area where the price control binds and into an area where it does not. The rate of return in the former has fallen relative to the rate of the return in the latter.

The privacy price control also impacts the advertisers for which the Internet platform serves as a middleman. Because they possess less information about the consumers they are trying to reach, those advertising in a digital environment will experience a decreased rate of return. This implies that the rate of return from other means of advertising has risen relative to the digital platform. As a result, advertisers in the price-controlled region may shift some of their advertising activity to other platforms, such as print media. Even if use of print-based media is falling all parts of the world, the privacy price control might slow its decline in regions where it is binding.

Lastly, viewing privacy law as a price control generates a testable prediction due to variation in the business models offered by different digital vendors. Not every firm with a website derives revenue from the collection of consumer information. For some, that is the primary source of income. Others, however, serve both as a platform for advertisers and also engage in the sale of their products. An example of this would be a department store's website, such as Macy's. Part of Macy's digitally-generated revenue comes from

selling products online; another component consists of serving as a platform for advertisers. We should expect those firms that rely most intensely on the latter revenue source to be those that implement the most extreme adjustments in the wake of a price control, relative to those who also sell through their online portal. For a firm deriving revenue from various sources, access to consumer information is just one "stick" in the "bundle of rights" it possesses. The privacy law, in a sense, lessens the value of this "stick" but does not directly impact the contents of the rest of the "bundle." That is, firms that are primarily ad-based should be affected more dramatically than those firms that view ad revenue as only one component of their total revenue stream. As a result, we should expect to see investment flight into firms that have a greater number of "sticks" in their "bundle."

4.3 Altering Exchange Characteristics

Every exchange is comprised of a bundle of attributes; the exchange-price itself comprises only one of those many characteristics. A price control only sets the terms for one of the characteristics in the bundle being exchanged. Thus, in the face of a price control, parties may alter the composition of their offerings in order to maintain profitability as best they know how. For example, landlords faced with rent control may allow deterioration of their housing stock so that tenants are, in essence, purchasing a different good relative to the non-price-controlled exchange. To take another example, buyers of labor, faced with a minimum wage law, might attempt to maintain their margins by reducing the quality of workplace conditions, such as by running the air-conditioner less frequently. The price floor directly establishes the price of labor, but it also indirectly alters other characteristics of the employment contract.

Likewise, one effect of price ceilings on gasoline during the 1970's in the US was that sellers of high-quality gasoline benefited relative to low-quality sellers. This was a consequence of the law mandating that the maximum price for each seller was the maximum price they had previously charged at that station. Naturally, higher-quality providers had been selling at higher prices. They responded by retaining their high price, but cutting the quality of the gasoline they provided (Barzel 1997). Thus, the price control directly established a price for gasoline, but it also indirectly altered other aspects of the exchange, such as the quality of gasoline being purchased.

The exchange between browsers and firms is a complex one, and is therefore also subject to adjustment on various margins. The two-sidedness of ad-supported websites further heightens the complexity of the exchange between a platform and its visitors. On one side are consumers, exchanging their data for the website's services; on the other side are advertisers paying for advertising space. Due to this market's two-sidedness, platforms may be able to adjust on one or both sides of the market, with potential consequences for parties on either side.

The most visible consequence of a traditional price ceiling is that it creates a shortage. More careful analysis is required to notice that the control also alters other attributes of the exchange by re-allocating property rights. Since regulation allows consumers to easily forgo the payment that websites demand, sites may alter other attributes of the exchange. This is because the government stricture only controls one aspect of the exchange between

website visitors and the website: namely the "price" that the latter charges to the former.[42]

As already mentioned, Goldfarb and Tucker (2011) have demonstrated that the 2002 Directive reduced the average effectiveness of digital advertisements. Thus, each ad placed on a web page is less likely to generate a sale for the advertiser. Consequently, the per-unit price of ad space may fall as advertisers' willingness to pay for a given space falls. As in the case of gasoline sellers, platforms–which see their revenues from advertisers falling–may alter transaction attributes that are not subject to the price control. A corollary insight is that websites possessing a greater number of potential margins for potential adjustment are more likely to survive relative to sites with fewer margins for adjustment.

One way that the platform might respond is by increasing the total quantity of ads displayed on any given page. Consumers are familiar with the common practice of platforms placing banner ads on the side of the screen. Given that the price control makes each banner ad less targeted, platforms might increase the total quantity of ads that they support, in an attempt to maintain revenue neutrality.[43] Surveys show that browsers report banner ads to be distracting when they are attempting to consume a site's content (Adobe 2012).[44] Of course, banner ads would (and do) exist even in the absence of a law that might have the unintended consequence of increasing their total quantity–they would simply be

[42]Here I am concerned with counterintuitive results, and not simply with those that we might most easily predict. For example, one might easily imagine that regulation causes consumers to be faced with the same number of ads, only that these ads are less targeted. Even whether this is a welfare gain is itself questionable because it raises the search cost of a consumer finding a product (Varian 2009).

[43]This is also contrary to Weyl (2009) who predicts that a price control imposed on one side of a two-sided market will result in a price increase on the other side of the market. Here, the prices that advertisers are willing to pay likely fall. Of course, this logic does not run counter to Weyl; it simply demonstrates another peculiarity of the price control when information, rather than money, is the medium of exchange.

[44]The 2012 Adobe survey finds that 68% of web users see banner ads as "distracting."

less targeted. On the unhampered market, however, entrepreneurs engage in profit-and-loss calculations (Boettke 2001) that would enable them to place an optimal number of banner ads. Though research shows that both static (banner) and dynamic (audio and video) ads reduce visual search speeds (Burke et al. 2005), the price control may incentivize firms to exceed the optimal quantity (i.e., the quantity that economic calculation suggests is the most profitable) of ads.

The effect of the price control may be worse than simply increasing the quantity of banner ads. As Goldfarb and Tucker (2011) have demonstrated, average ad effectiveness fell only for static, banner ads. There was no corresponding decrease in effectiveness for dynamic ads, such as audio and video. The authors attribute this finding to the fact that the latter ads function primarily by "forcibly" intruding into the visitor's limited attention, whereas static ads must rely on catching a visitor who may already be interested in the ad's content. Recall that the privacy price control sets only one aspect of the exchange: the information to be collected by the website. It cannot control other aspects of the web browser's experience (just as it cannot control other aspects of the gasoline exchange). As a result, advertisers may shift to dynamic ads in the price-controlled region. Even if dynamic ads are growing as a share of all advertising in all areas of the world, we might then expect them to be growing fastest where the price control is binding.

Survey evidence shows that consumers dislike dynamic advertisements relative to other forms of advertisement which marketers commonly employ. For example, the typical American consumer prefers viewing TV ads to viewing ads on a website (Adobe 2012). Experience also suggests that such advertisements are more distracting than are static ads,

but consumers view even banner ads as a nuisance. An additional potential effect is that if dynamic ads serve as an impediment to consuming a website's content, then ad-supported websites may experience decreased traffic. In the end, a law designed to make the Internet safer may discourage the marginal consumer from browsing certain websites altogether.

The optimal quantity of dynamic ads is not zero; my contention is simply that the price control may push the usage of such techniques beyond the optimum. Entrepreneurs, operating in a regime of profit-and-loss, can determine the optimal quantity of such ads because they have access to the feedback inherent in the price system (Boettke 2001). Regulators do not possess similar feedback.

Lastly, traditional price control theory predicts a deterioration in the quality of a good being forced to trade below its equilibrium price. This is seen starkly in the case of rent control. The price control incentivizes landlords to forgo maintenance of their properties. Such a result holds for two reasons. First, there is a surplus of renters, reducing the need to compete on quality. Second, the price control lowers the rate of return for supplying the price-controlled good at all. The immediate effect of the privacy price control is to reduce the "revenue" that platforms are collecting because only some fraction of the visitors to their site pay an above-zero information-price. In short, the control reduces the profitability of the ad-supported firms, thus restricting their ability to engage in development of the site. Quality is an inherently subjective feature of any good. Nonetheless, theory suggests that the privacy price control will reduce the average quality of websites, particularly those that have fewer potential margins of adjustment.

In the digital arena, falling quality may occur on a wide array of margins, some of which

are not easily detectable. For example, the minimum wage does not always cause an increase in unemployment, as measured in the standard way. Instead, it may cause firms to cut the hours of their employees, while retaining the same workforce. A casual observer might be lead to conclude that the minimum wage has had no impact on employment, but such a conclusion would be spurious. Similarly, a website may reduce its customer service hours—a quality adjustment that would be difficult for a casual browser to detect.

V. The Political Economy of "Privacy Price Control"

Given their harmful effects, why are price controls so pervasive? To date, the economics of digital privacy literature has largely ignored the political economy aspects of digital privacy regulation. Such an oversight may be due to the relative dearth of actionable data or follow from digital privacy law being a relatively new legislative innovation. Yet, political economy aspects are important considerations for the imposition of traditional price controls. For one, the price control may incentivize rent-seeking relative to other forms of government-sanctioned privacy provision. Alternatively, it may prove to be an effective policy for government officials looking to boost their prestige. Second, regardless of whether it originates to serve special interests, the administration of a price control is inherently more costly relative to some alternative forms of intervention.

One commonly-offered explanation for the existence of price controls is that they benefit at least one, concentrated and identifiable, interest group. The classic example comes from minimum wage law. Historically, unions have been among the most vociferous advocates for the minimum wage. This is an attempt by unions to overprice the substitutes

for their labor services (Silberman and Durden 1976; Sobel 1999). The potential for the price control to be used as a policy lever incentivizes unions to sink resources into manipulating the political apparatus to their benefit.

Unlike the literature on the minimum wage, analysis of privacy law has thus far largely refrained from asking *cui bono*: "who benefits?" It seems apparent that platforms, advertisers, and (at least some) consumers are harmed by digital privacy law, so why are most developed nations looking to implement or strengthen digital privacy law? One answer is that just as traditional price controls may be leveraged by interest groups to impede competitors, privacy price controls can also serve the same function. The preceding pages have demonstrated that the privacy price control reduces the profitability of ad-based Internet platforms. Thus, firms that compete with ad-supported web services have an incentive to support the privacy price control. This could include websites that do not depend on the collection of consumer information, or it might include specific interest sites for which the price control is not as damaging as compared with general interest site peers.

There is some, albeit scant, evidence that private interests may favor the privacy price control. For instance, the Directive's impact on European financial services seems to have concentrated consumer lending among a few of the largest banks because potential entrants are denied easy access to consumer data. Consumer lending is also less frequent in Europe compared to the US because of the restrictions on selling consumer information (Bergkamp 2003). While a possibility—and one that may become increasingly relevant as countries begin passing more digital privacy laws—there is certainly no overwhelming evidence that specific commercial interests are responsible for the passage of most notable privacy laws.

To the contrary, deliberations over the latest update to the EU Directive (the GDPR, set to take effect in 2018) precipitated a wave of interest from private companies, but they almost universally opposed the new law or sought for a reduction in its stringency. This was true across the type and size of the firm.

What then explains the existence and growing pervasiveness of digital privacy law? A simpler and more compelling answer comes from an alternative explanation for price controls. Government officials are able to enhance some combination of their reputation, power, and budgets through price-fixing. This insight helps explain the passage of rent control, for instance. Municipal officials have an incentive to pass pro-tenant legislation as long as tenants fail to connect phenomena such as shortages and quality deterioration to the rent control itself. As long as tenants blame landlords for these effects, then government officials can garner additional support because they are "helping" the poor. As an example from digital privacy law, the European justice commissioner, commenting on the forthcoming GDPR states, "These new...rules are good for citizens and good for businesses" and that "they will profit from clear rules that are fit for the digital age," (Scott 2015).

It is apparent that the privacy price control hurts both platforms and advertisers, just as rent-control hurts landlords. The preceding pages have shown that the control may also harm consumers in subtle ways. Nevertheless, the privacy price control may still be a useful tool for governments. Surveys and experimental evidence (Acquisti, Taylor, and Wagman 2016) show that consumers value personal privacy in the digital environment. Such measures of how consumers value privacy are probably overstated because consumers are

not forced to give up anything for an additional increment of privacy. They are asked about the value of additional privacy, but are not required to bear the opportunity cost of privacy, such as higher search costs or lower website quality. Just as municipal officials respond to the "problem" of high rental prices, so too might regulators be responding opportunistically to the revelation that consumers value additional privacy protection. As long as the party allegedly being helped remains ignorant of the true source of the new costs they are bearing, government officials enjoy a boost in popularity and budgets to administer their newfound responsibilities. In short, the answer to the question "who benefits" may be regulators themselves.

Regardless of whether price controls are a consequence of rent-seeking by special interests (in this case, seemingly less likely) or whether they are a tool to enhance a bureaucrat's image or budget (in this case, seemingly more likely), they are inherently costly to administer. Because firms must be continuously monitored and subsequently sanctioned if they are found in violation, enforcement requires a permanent bureaucratic apparatus. Price controls are typically enforced either by undercover government agents or by buyers who report violations to the authorities (Lott and Roberts 1989). Both methods require maintaining a costly bureaucratic apparatus dedicated to handling violations.

If the problem facing consumers is information asymmetry, why is information disclosure not the preferred governmental solution, rather than a price control? Because it would not require an ongoing bureaucratic apparatus to administer, information disclosure would be a less costly policy option. Governments could simply implement a campaign warning Internet users of the risks of visiting websites that collect consumer data. Such a

policy would also likely reduce, but not entirely eliminate, the potential for groups to view privacy law as a tool to impede competitors. Warning consumers about the risks of using a certain product is probably less damaging to the producers of that product than is a price cap on its sale.

One reason we may not see this policy is that, while likely less costly, it would also be less likely to confer the same reputational benefits on the administering officials as would the price control. Information disclosure might strike some as being "easy" on firms that violate consumers' rights. As Hanson (2003) shows, in a world where banning some activity is a viable policy option, regulators will often select the ban over information disclosure because consumers are likely to ignore the disclosure if they know the ban is within the policy-maker's feasibility set. When a ban is an option, consumers may interpret weaker measures as "cheap talk"—evidence that the danger is insignificant. Simple information disclosure may do less to enhance a government's reputation as compared with more stringent measures, such as the privacy price control.

VI. Conclusion

To admit that privacy law is a price control is not a conclusive case against privacy legislation. Some see privacy as an inviolable right that must be purchased at any price. Similarly, economists agreeing on the disemploying effects of the minimum wage may still differ in their policy proposals. Some may simply conclude that a slight increase in unemployment is worth the other alleged benefits of the price control. So too might some conclude that the benefits of privacy protection outweigh the costs of this intervention.

Such a conclusion, however, should be tempered by careful consideration of the costs that the privacy price control may impose.

As such, this paper has two implications. First, scholars in digital privacy economics admit that there is "no unified theory of privacy in economics," (Tucker 2016). Such is, indeed, the case; nonetheless, there *is* a body of remarkably unified theory surrounding price controls. Theory that possesses a broad consensus should inform areas of investigation about which there are more questions. Though regulatory issues are far from the only line of inquiry in the economics of digital privacy, the theory of price controls is useful in predicting the effects of the mandated opt-in. An additional implication is that observed differences in the "creativity" of advertisements between the EU and US—a phenomenon noted at the beginning of this paper—may be due to facing different constraints as opposed to tastes differing between the regions.

Seeing privacy protection as a form of price control also generates several testable predictions. If, in fact, a digital privacy regime of opt-in is a price control, we may see Internet platforms adjusting on myriad margins in an attempt to maintain profitability. The theory of price controls, carefully applied, should inform the empirical strategy of future researchers. For example, do firms with a more diversified source of revenue streams exhibit greater survival rates in the wake of privacy laws such as the EU's Directive?

Second, those arguing for digital privacy regulation should be less confident that digital privacy regulation is welfare-enhancing. Some consumers, namely the most privacy-sensitive, doubtlessly do benefit from a restriction that grants them enhanced protection of the personal information they generate in digital environments. But it is impossible to

weigh the gain of the consumers who benefit against those who lose due to a general interest site being forced to close. Such an evaluation would require interpersonal utility comparison.

Furthermore, to conclude that digital privacy law necessarily raises consumer welfare is to disregard the economists' task of looking beyond what is easily "seen" to that which is largely "unseen." Like most regulations, legislators advance these laws under the pretense of consumer protection. As the argument goes, consumers suffer harm when they lack control over how their personal information is acquired or used. And, in fact, they may. Yet, economists generally agree that price controls are welfare-reducing; they may benefit by applying their well-founded aversion regarding price controls to questions in digital privacy law.

CHAPTER 4: Is the Market for Digital Privacy a Failure?[45]

I. Introduction

Survey evidence reveals that consumers strongly dislike digital firms collecting their personal information (Turow et al. 2009; Madden and Rainie 2015). Why then do so many firms engage in this practice when they could, instead, charge visiting consumers a fee that would protect their privacy?[46] One hypothesis is that Internet companies are exploiting information asymmetry and behavioral biases in order to collect more data than consumers would prefer if they could stop it (Hoofnagle and Whittington 2013: 639). Such a perspective models the relationship between information-collecting companies and their consumers as inherently exploitative (Calo 2013; Hoofnagle and Whittington 2013). For instance, Calo (2013) refers to "the exploitation of cognitive bias" in the context of digital privacy. He argues that collecting personal information permits a greater "personalization"

[45] I wish to thank Nicholas Freiling, David Lucas, Chris Coyne, Peter Leeson, and Peter Boettke for helpful suggestions. All errors are my own.

[46] "Privacy" is notoriously 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..." Hirshleifer (1980) notably takes issue with these conceptions, instead arguing that privacy should be conceptualized as "autonomy in society." Such disagreement–even among economists–illustrates the fact that "Privacy is a concept in disarray" (Solove 2006). Though these conceptions were formulated prior to the widespread adoption of digital technologies, they are well-suited to characterize interactions in the digital environment. Thus, Acquisti et al. (2016) note about the digital context: "Privacy is not the opposite of sharing–rather, it is control over sharing" (p. 445), a conception of privacy that echoes Posner's.

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, however idiosyncratic, and leverage that bias to the firm's advantage," (p. 1003). Acquisti (2004) agrees, stating that "individuals who genuinely would like to protect their privacy may not do so because of psychological distortions well-documented in the behavioral economics literature," (p. 7).

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

As Acquisti et al. (2016) observe, the economics of privacy is properly considered a sub-field of the economics of information, which has its roots in Hayek (1945), Stigler (1961), and Akerlof (1970) among others. Tabarrok and Cowen (2015) argue that the older, more "traditional" market failure of information asymmetry may be giving way to the new market failure of privacy violations. That is, those scholars argue that problems resulting from lack of information between buyers and sellers may be increasingly replaced by too much information flowing between the two parties. Other scholars, however, still view privacy issues as stemming from asymmetric information itself (Hirsch 2010). Consumers do not always know when a firm is collecting information, what information it is collecting,

or to what specific uses the information will be put.[47] Some then conclude that information asymmetry generates over-collection relative to the ideal of perfectly-informed market participants (Hoofnagle 2005; Hirsch 2010). Consequently, Newman (2014) maintains that the market for digital privacy is as much a failure as was the market in food and product safety during the 20th century.[48] Gertz (2002) also considers the digital marketplace a "classic example of a market failure" that should be regulated, a position advanced by many other leading commentators (Solove 2004; Vila et al. 2003; 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).[49] Solove (2004) adds that though he believes consumers would prefer a greater level of privacy, bargaining inequity between large corporations (such as Google) and individual consumers prevents Coasean solutions.

As a result of the market-failure perspective, some governments, most notably the EU (beginning in 1995 with an update set to take effect in 2018), have enacted legislation aimed at curtailing privacy-invasive practices by private firms.[50] Regulators express concern both about fraudulent use of consumer information and also legitimate practices– such as behavioral targeting of advertising and price discrimination (de Corniere and de

[47]Information asymmetry is inherent in every exchange. Consumers possess more information than firms prior to information collection. After collection, firms possess more information than consumers (for example, regarding how the information will be used).

[48] On Brown's (2013) reading of the literature, 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.

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

[50]Japan, Canada, Singapore, and South Africa have all recently passed digital privacy legislation, but the EU was the first-mover, enacting privacy legislation in 1995.

Nijs 2016). The latter practices have come under fire in no small part due to surveys which have revealed consumer dislike.

Interactions between consumers and web platforms consist of the latter collecting "non-sensitive" information directly from consumers or allowing third parties (advertisers) to use the site for surreptitious collection of consumer information (Goldfarb and Tucker 2011; de Corniere and de Nijs 2016). Sometimes referred to humorously as "mouse droppings" (Berman and Mulligan 1998), "non-sensitive" information may consist of device information, geographic location, browsing history, click-trail, and the like. Probably no website collects more "mouse-droppings" than the world's largest search engine: Google. In fact, the overwhelming majority 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. Other technologies–such as GPS–also increasingly rely on tracking users, enabling what some see as a privacy-rights violation (Schlag 2013). 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 working paper). Nonetheless, others complain that this information price is difficult to observe due to the frequent lack of transparency in the exchange between consumers and firms–evidence, once again, of market failure (Strandburg 2013).[51]

The strongest piece of evidence raised by the market-failure camp is survey and experimental evidence indicating that consumers value their privacy highly. Both non-

[51]I have argued that one implication is that regulation of this exchange functions as a price control (Fuller working paper)

academic research, such as Pew surveys, and academic studies suggest that a majority of consumers would 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) conduct a survey showing that 66% (and possibly up to 86%) of Americans do not prefer marketers to target their offerings–but that the vast majority of respondents use search engines that do just that, which suggests deception or exploitation to the authors.[52] Importantly, however, many of these surveys adopt an "unconstrained" view of the world that fails to remind respondents of privacy's opportunity cost.[53]

One possible conclusion to draw from these findings is that markets fail to satisfy consumer preference, perhaps due to information asymmetry. Yet, 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; Acquisti et al. 2016).[54] They complain that companies violate their privacy rights, but also provide firms with information voluntarily (Berendt et al. 2005; Norberg et al. 2007).

One 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).

[52]Lenard and Rubin (2009) argue that consumers derive significant benefits from information collection, the primary boon being lower search costs when consumers are trying to find a product.
[53]Sowell (1987) famously describes the difference between the "constrained" and the "unconstrained" visions.
[54]For example, consumers demonstrate a preference for the privacy-intrusive Google over the also-free search engine, DuckDuckGo, that refrains from collecting consumer information.

But the view that consumers are routinely making this trade-off and that markets are thus satisfying consumer demands has never been convincing to some scholars. For example, Acquisti et al. (2016) state 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) and that consumers confront "...decision-making hurdles...when dealing with privacy challenges, especially online, such as asymmetric information," (pps. 448, 477). 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). Thus, on this view, the quantity of information collection that we observe is not a result of fully-informed, rational consumers behaving according to long-run self-interest. Instead, it results from some combination of information asymmetry and behavioral weaknesses that cause behavior to deviate from true preferences to the benefit of firms and the detriment of consumers.

In what follows, I ask unique questions in one of the largest privacy surveys in the academic literature to date. To empirically examine three common claims in the economics of digital privacy that are intimately related and crucial to making the case for market failure, I solicit responses from 1,599 Google users.

Claim 1: There is widespread information asymmetry between firms and consumers. Consumers are unaware their data is being collected and/or are ignorant of the potential uses to which that data may be put (Tucker 2012; Acquisti et al. 2016: 447). "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). 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 via survey (Turow et al. 2009), which suggests that markets under-provide the economic good of privacy, perhaps because behavioral biases lead behavior to deviate from stated preferences (Acquisti 2004). That Acquisti et al. (2013) have presented evidence of an abnormally large endowment effect for privacy only bolsters the notion that consumers value their privacy highly. Yet, we know little regarding what the modal consumer would be willing to *sacrifice* to get additional privacy (FTC 2012).

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 in a recent *Journal of Economic Literature* paper, yet I argue that these fail to exhaust the possible reasons that consumers dislike information collection. Government activity may also play a role.

By addressing these claims, my paper contributes to a debate in the economics of digital privacy literature: is the digital marketplace a failure? There is a longstanding tradition in economics that sees markets as institutions that reconcile the demands of myriad individuals (Boettke 2007), but this perspective contrasts with a view popular in the

economics of digital privacy literature: that firms and consumers are fundamentally at odds (Hoofnagle et al. 2012).

Additionally, my paper improves on the existing literature in several ways. First, relative to other studies of the valuation of privacy, I increase the probability that my sample is truly random. Seminal and important studies often utilized samples that were not representative of the broader US Internet-using population.[55] My sample is larger and more representative of the Internet-using population in the U.S. Second, my survey queries respondents about their privacy valuation with respect to a specific company: Google. Third, my survey also generates responses to two questions that are related to the valuation of privacy: the extent of information asymmetry and the role played by government in generating distrust of information collection. These additional pieces of information yield a richer picture of consumer privacy valuation and enable a more satisfactory answer to the question of whether markets are failing to provide adequate privacy. Lastly, "privacy-sensitivity" (i.e. "the demand for privacy") is believed to have increased over the last fifteen years, suggesting that old research may be outdated (Goldfarb and Tucker 2012).

Section II provides additional background on privacy debates. Section III advances several related hypotheses. Section IV discusses my survey design. Section V discusses the results. Section VI acknowledges several limitations. Section VII concludes with a few implications

II. Background and Approach

[55]For example, Acquisti et al. (2013) survey female visitors to a large Pittsburgh mall.

Privacy is an economic good for most people in most contexts (Farrell 2012). Thus, it is unsurprising that survey and experimental evidence routinely show consumers preferring more privacy to less. However, surveys of consumers' attitudes regarding digital privacy are often open-ended and "unconstrained." For example, Turow et al.'s (2009) survey asks questions such as: "Please tell me whether or not you want the websites you visit to show you ads that are tailored to your interests."[56] 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 enforced by governments.[57] These researchers further 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." The paper also cites 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?"

That consumers express a preference for more of something that is widely viewed as an economic good (privacy) or less of something viewed as an economic bad (privacy invasion) is completely unsurprising. One might similarly expect that individuals would

[56]The authors of this survey find that 69% of respondents agree with the statement: "...there should be a law that gives people the right to know everything that a website knows about them" and that 92% agree there should be a law that requires "websites and advertising companies to delete all stored information about an individual, if requested to do so."

[57]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.

express a preference for higher incomes, more leisure, lower buying prices, higher selling prices, and more friends, *ceteris paribus*. An FTC report (2012), however, gets to the heart of the issue: "...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."

A query that reveals consumers' preferences for a greater quantity of privacy protection, *ceteris paribus*, is an "unconstrained approach" to consumer valuation of privacy. "Unconstrained" survey questions fail to remind consumers that acquiring an additional "unit" of privacy 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 involved.[58] Thus, this approach may reveal the "notional" demand of individuals, but not necessarily their "real" demand.

The economic approach, by contrast, necessarily asks "constrained questions."[59] This approach is superior because, for individuals choosing in the face of constraints, there are

[58]Clark and Powell (2013) confront similarly "non-economic" approaches as they seek to remind respondents of constraints in investigating sweatshop working conditions. Labor activists frequently 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. To correct for this unconstrained view, Clark and Powell conduct a survey of sweatshop workers that forces respondents to consider the opportunity cost of specific improvements to their working conditions. 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 increased risk.

[59]Note that Acquisti (2005) acknowledges that there are both costs and benefits to disclosure of personal information.

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, firms ask a zero money-price, enabling them to ask for a positive quantity of personal information.[60]

Because many Internet platforms earn revenue (in some cases, all their revenue) by collecting information about 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. Thus, a sound 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 (the *ceteris paribus* assumption)–but without surrendering any personal information.

Notably, Acquisti et al. (2013) conduct a survey that distinguishes between willingness to accept (WTA) money in exchange for disclosure of information and willingness to pay (WTP) money to protect otherwise publicly available information, and in so doing identify a "privacy endowment effect." They state that: "Empirical studies in which consumers are...asked to consider paying (or giving up) money to protect their privacy are much scarcer," (Acquisti et al. 2013: 254). Given that we live in a world where many firms currently finance their offerings by collecting consumer information, it is reasonable to ask whether this arrangement is superior, from the consumer's viewpoint, to the relevant

[60]As Boettke and Candela (2015) note, non-money differentials could include preferences for beauty, love, environmental pollution, racial discrimination and so on, but they are comprised of personal information in the case I explore.

alternative.[61]

To date, there are few existing studies of consumer valuation of privacy. 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 (Willingness to Accept), 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 (Willingness to Pay). Rose (2005) finds that 47% of respondents were willing to pay something to protect their privacy, but my approach differs in important ways. First, that study was concerned with a change in the legal regime governing digital privacy, whereas mine attempts to determine the value of privacy to consumers by injecting a greater measure of realism: consumers are choosing with respect to a company (Google) they interact with frequently. Second, that study took place in New Zealand, but privacy norms and attitudes are known to vary across cultures (Milberg et al., 2000). Perhaps most importantly, the study by Rose was conducted well over a decade ago, but privacy attitudes are known to shift in response to changing constraints (Penney 2016). The Internet in 2017 is far different than the Internet of 2007. In a more recent study, Tsai et al. (2011) find that, when a company makes its privacy-protective policies prominent, consumers are willing to pay a small premium for those features.[62]

In addition to examining consumer valuation of privacy, my survey explores two other

[61]Presumably, it is superior from the firm's standpoint since it is the strategy it has selected.

[62]This finding suggests that, contrary to the view of those seeing digital markets as a prisoner's dilemma, necessitating a "race to the bottom" with respect to consumer privacy (Hoofnagle 2003), privacy protection may function as a way for firms to differentiate themselves.

important questions that are related to valuation. The first, noted by Tucker (2012) to be among the most important questions in the economics of privacy literature, is the extent of information asymmetry between consumers and firms. Of course, if such asymmetry is minimal, this weakens the argument that the digital arena is a market failure with respect to under-provision of privacy. If consumers are well-aware of the information collection, but continue to demonstrate a preference for services that rely on this method of monetization, it is unclear why this is problematic or in need of a regulatory fix.

The other question regards *why* consumers dislike information collection by firms. Acquisti et al. (2016) supply several reasons that consumers dislike this business practice: "...price discrimination...spam...risk of identity theft...[and] the disutility inherent in just not knowing who knows what," (483).[63] To these phenomena that consumers may find distasteful, I add the possibility that data collection may be risky when governments possess the technological capability and legal authority to seize this data, thereby enhancing their mass surveillance capabilities. If this is a concern for consumers, it suggests that "government failure" must be considered alongside other explanations for why reliance on information collection worries consumers.

III. Hypotheses

Google's famous motto is: "Don't Be Evil." But the fact that the company

[63]For the purposes of this paper, I ignore two other issues with claiming that price discrimination is somehow 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 suggests that price discrimination increases market efficiency.

surreptitiously collects the information of over one billion individuals annually has led some to question whether the firm's very business model runs afoul of its chosen dictum (Hoofnagle 2009). Information is costly to acquire (Stigler 1961). Given that firms such as Google engage in costly information acquisition, they do so because the benefits outweigh the costs. The question then becomes whether the benefits that accrue to Google align with consumer preference, as argued by some (Cooper 2013), or whether there is a disconnect, as argued by others (Strandburg 2013).

Should consumers prefer greater privacy, there is a profitable opportunity in exposing Google's practices and setting up 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 to Google's 3.5 billion, far less than 1% of the traffic that Google experiences.[64] 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 the information collection troubled them sufficiently. For instance, physical encyclopedias are a substitute for Google search.

One possible objection is that few individuals are aware of Google's practices, and that this information asymmetry constitutes a market failure. Perhaps in the world of fully-

[64]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.

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. Low levels of information asymmetry cut against the argument of market failure that stems from uninformed consumers. From this, 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 those individuals with more inelastic demand for Google's services to possess a greater awareness regarding Google's information collection policies. In other words, information awareness increases with the cost of ignorance regarding Google's practices, a prediction in line with Becker and Rubinstein (2011). As Becker and Rubinstein show, those with a relatively inelastic demand for bus transportation resumed their routines more quickly after a terrorist attack on the bus system. In the case of digital activity, consumers with a relatively inelastic demand for digital services are those likely to be using Google "dozens of times per day or more." My prediction will only be true if the rational choice framework holds in the digital context, a context where it has been challenged by behavioral economics. Thus, I offer Corollary 1b:

Corollary 1b: *Those with a more inelastic demand for digital services better understand digital information collection.*

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 should express a demand for increased privacy (an economic good) 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. For many individuals (though not all), it is likely that the size of this cost is small. After all, billions of individuals voluntarily post pieces of personal information to social media sites, such as Facebook. As the FTC (2012) 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.

A critic might object that individuals volunteering information online is no indication of that person's true preferences–that biases are causing behavior to deviate from stated preferences. If this is the case, my survey should reveal that the average consumer has a large *stated* willingness to pay. Such a large stated WTP would be evidence for divergence between behavior and "true" preferences. From this, I offer Hypothesis 2:

Hypothesis 2: *Digital consumers prefer sacrificing some level of privacy to paying a pecuniary fee to digital producers.*

It is costly to use the price system (Coase 1937; Demsetz 1967). In the case of exchange between digital firms and consumers, these costs include the time allocated to submitting one's credit card information and processing that information. Of course, an increase in pecuniary exchanges in the digital environment also increases the probability of identity

theft–another serious cost. This suggests that consumers may be willing to pay far less in dollars than in personal information to access digital services. Thus, asking a personal information price may enable a greater quantity of digital activity than would asking a money price, given the price-system costs associated with the latter.

This has implications for the viability of large digital firms should they be forced to refrain from information collection in favor of money-prices. If average willingness to pay in money is low, then revenue will be insufficient to compensate Google (or any other information-collecting company) equivalently to its current revenue under the arrangement of selling consumer data. Furthermore, low stated willingness to pay cuts against the notion that consumers are falling prey to biases which cause their behavior to deviate from their "true" preferences. If the modal Google user expresses a low willingness to pay that, far from contradicting their digital behavior, actually aligns with it. Thus, I offer Corollary 2a:

Corollary 2a: *Consumer willingness to pay in dollars will be less than willingness to pay in information.*

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 acts as a constraint on consumers' digital behavior, this suggests that government failure, rather than (or, at least in addition to) market failure may be to blame for distrust of information collection. In other words, the business practice, by itself, may be insufficient to generate the level of discomfort expressed by consumers. Thus, I offer Hypothesis 3:

Hypothesis 3: *A source of discomfort with digital information collection is the risk of*

government privacy intrusion.

To test these hypotheses, I conducted a survey of randomly-selected Internet users. The survey was administered online intermittently between December 27, 2016 and January 11, 2017 to respondents across the U.S. It was programmed and administered by Haven Insights LLC and hosted at SurveyGizmo.com (Widgix, LLC). Respondents were directed to the survey by a number of 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

IV. Survey Design

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."

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." This question was asked to gain additional information about the respondents.

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?*

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.*

First, respondents with a positive willingness to pay (WTP) were asked about their annual WTP.

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

Next, the same respondents were asked about their per-search WTP. In order to avoid

potential confusion regarding appropriate values to enter (given the likely infinitesimal size of the average response), we provided respondents with several choices: "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." This question was asked to elicit whether the average individual is willing to pay enough to equal the quantity of revenue that Google earns annually through its current information collection methods.

V. Results and Discussion

My survey results largely confirm the hypotheses offered in Section III. 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, these users were queried about their level of knowledge of Google's business 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 that is oft-criticized by scholars (Hoofnagle

and Whittington 2013).

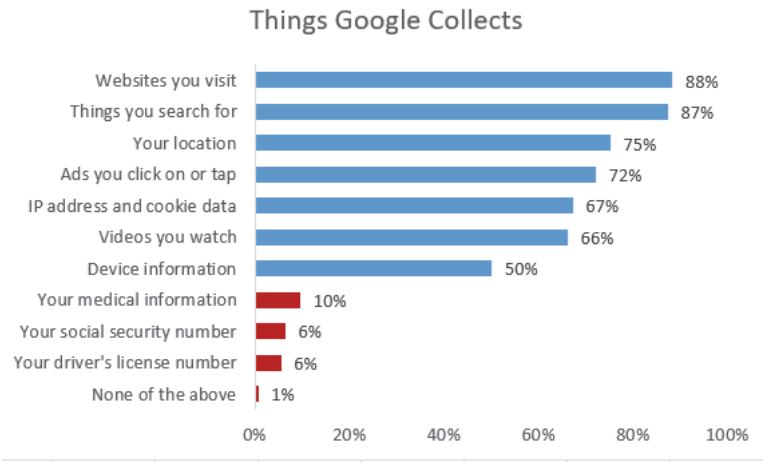

Figure 1: Low Levels of Information Asymmetry

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 an individual 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–yet these are browsers who voluntarily use the firm's services.[65]

Corollary 1b: *Those with a more inelastic demand for digital services better understand information collection.*

The prediction of Corollary 1b is borne out by the data. The more inelastic demanders of Google's services are more aware of the information practices, a finding that follows directly from the idea that the cost to being uninformed is greater for them than relatively elastic demanders. 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%.

Hypothesis 2: *Digital 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 and possibly because it lowers their 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 say that they "like seeing the ads customized to my

[65]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.

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. 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 under-providing the good, and thus failing. Tellingly, of the 71% of all respondents who said they would prefer not to be tracked, a full 74% are unwilling 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 (again, 71% of all U.S. Google users), the overwhelming majority are not willing to sacrifice *anything* to achieve that privacy. Put differently, almost 82% of all Google users are unwilling to pay anything for marginal improvements to privacy.

Corollary 2a: *Consumer willingness to pay in dollars will be less than willingness to pay in information.*

The evidence overwhelmingly supports Corollary 2a: among those with a positive WTP to conceal information from Google–between 18% and 19% of all Google users–the values are consistently very 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.[66] Furthermore, among those indicating a positive WTP (again, only 26% of

[66]Three of the four were $100,000 or greater.

those preferring not to experience information collection), a full 17% indicated they would be willing to pay $0 dollars annually to protect their privacy, suggesting that perhaps they *also* should have answered as the majority did, indicating no positive willingness to pay. Adding these individuals to the group with no WTP reduces the percentage of Google users with any positive WTP to just over 15%.

Among those indicating a positive WTP, including that group that entered a "$0" when prompted to include a numeric value, the average annual WTP equals $56.85. After having removed values above $10,000, however, even this median is driven by several outliers, as evidenced by a standard deviation of 207.86. Removing all entries of $1,000 or greater (four additional responses) yields a mean WTP of $36.48 annually.[67] 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 approximately $14,778,400,000 (that is, multiplying the number of those with a positive WTP by the average WTP). This figure would amount to roughly 21% of Google's current annual information-sales revenue, which is its most important revenue stream.

Such a large standard deviation, however, suggests that the median is better suited to provide an accurate picture of WTP. In the dataset in which all responses of $10,000 or above have been omitted, the median annual WTP equals $15. In other words, of the

[67]Removing all responses of $500 and greater (five additional responses) yields a mean annual WTP of $28.

roughly 18% of Google users willing to pay to protect their information, half are not willing to pay more than $15 annually. For perspective, the National Soft Drinks Association estimates that the average American household spent about $850 on soft drinks in 2012.[68] Such a low WTP suggests that, even if a problem, digital privacy may not be worthy of being addressed via policy tools.

Because individuals might experience 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 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 valuations are consistent with the low annual privacy valuations.

As stated above, Google serves roughly one billion users annually and earns roughly $70 billion annually in targeted advertising revenue. 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 Google users have a positive WTP in the first place, this question revealed that 59% of these would not 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 collecting information.

[68]See here for this information: http://peopleof.oureverydaylife.com/much-americans-spend-soft-drinks-11124.html

These results may be construed as being inconsistent with 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 rights 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 possessing a property right in their information, have little willingness to pay 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 willingness to pay 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 stated valuation of privacy would be even higher than if personal ownership was not the default.

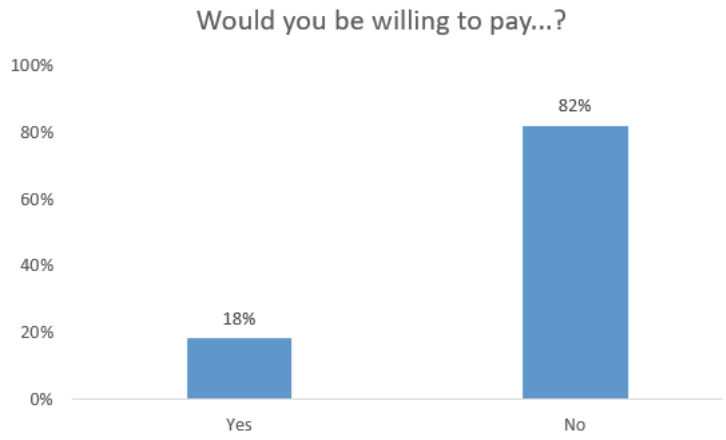

Figure 2: Low Willingness to Pay for Privacy

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

The evidence supports Hypothesis 3: the literature has largely ignored an important reason for why individuals express dislike of digital information collection, and my findings also provide support for the reasons offered by Acquisti et al. (2016). For example, about 70% of consumers indicated that they were concerned with "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 real concern. By contrast, only 28% indicated any dislike for the common practice of price discrimination, which is frequently blamed for generating consumer dislike of information collection.[69] This suggests that, at the very least, concern over government intrusion should be included alongside dislike of practices such as price discrimination. 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 are the main concerns individuals have).

Respondents were then asked to rank their concerns ordinally. Fear of government intrusion earned a mean rank of 2.6 out of a possible seven options, suggesting that it is important, though not the most important concern for most users. 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 abuse suggests that, rather than there being "over-collection" of information by firms, there may be "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

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

from information *under-collection.* Given consumers' concern about government over-reach, this 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 argues. 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.

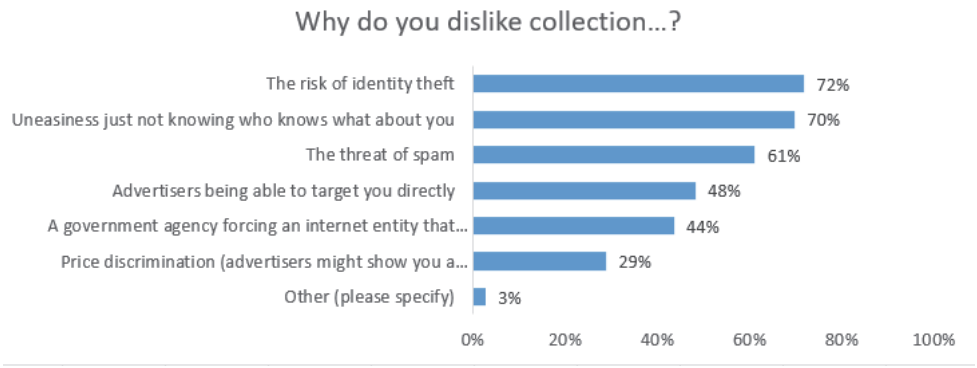

Figure 3: Dislike of Information Collection

In sum, at least with respect to Google, there is little evidence of widespread information asymmetry. There is no WTP to protect privacy by over 4 out of 5 Google users and a low average WTP among the remaining 1 out 5. Lastly, there is some evidence that government failure should also be recognized as a culprit in generating consumer distaste for information collection by private firms.

VI. Limitations

My study 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). 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).

Second, privacy is a somewhat slippery concept (Thompson 1975; Posner 1978; Berman

and Mulligan 1998; Solove 2006). Survey respondents surely answered 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 not be representative of the Internet-using population. If anything, those responding to an online survey may be less privacy-sensitive than those who do not. This is a potential weakness of any survey of privacy which is conducted in a digital environment.

None of these potential limitations constitutes a serious objection to the design of my study. Rather, they are reasons to not overstate my conclusions or apply my findings without first thinking hard about context.

VII. Conclusion

My paper has three primary implications. First, one resolution to the so-called "privacy paradox" is that individuals only express a significant demand for digital privacy when they are not forced to consider the opportunity cost of making that choice. This is unsurprising in light of the fact that privacy is an economic good for most individuals. Therefore, the question is not whether individuals prefer more privacy but rather how much of other goods individuals are willing to exchange for it. The question has never been

whether consumers value privacy at all but rather how strongly they value it. At least in the context of interacting with Google, my results suggest that they 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 actually prefer this method to the alternatives. Put differently, there is little paradox at all–simply a positive preference for more, rather than less, of an economic good, *ceteris paribus*.

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." 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.[70] Citizens are reasonably 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 their 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 individuals interacting within a regime of property, contract, and consent.

[70]See, for example, Koppl (2002) on "Big Players" and their role in shaping expectations.

CHAPTER 5: Concluding Remarks

This dissertation has one major implication: policymakers should adopt humility in the implementation of digital privacy policy. Because regulation of new technologies enables an expansion of bureaucratic scope and scale, the incentive is usually to regulate. When regulators can provide evidence of alleged harm inflicted on consumers by some technology, it only bolsters the rationale that regulatory fixes are a necessary corrective. Yet, the justification for regulation of digital privacy rests on two related, but questionable, arguments: first, that the market has failed and secondly that government can effectively implement a solution and at a lower cost than market-solutions.

Supposing that one accepts the argument that some combination of information asymmetry and consumers' behavioral biases yield failure in the digital privacy market, what then? One route is to conclude that the market, having failed, will *necessarily* be improved by government. This conclusion is a variant of the "Second Singer Fallacy," in which a Roman emperor after hearing the first singer sing immediately awards his prize to the second singer on the grounds that he can be no worse (Boettke et al. 2007). The first two chapters of this dissertation illuminate the unseen costs and unintended consequences of governmental attempts to improve on digital markets. Recognizing the flaws (or "perils") inherent in government fixes suggests that comparative institutional analysis is

appropriate in judging between government and market. It is imperative to compare real-world institutions to real-world institutions. Comparing real-world markets populated by imperfect human actors with idealized governments populated with omniscient and beneficent actors is an unfair contest. As I have argued, regulation of digital privacy engenders all three perils Kirzner described. Furthermore, certain forms of digital privacy regulation—namely, the mandated opt-in—function similarly to a price control.

To actually perform comparative institutional analysis, it is necessary to examine the accuracy of claims regarding the functioning of market institutions in practice. In the economics of digital privacy literature, it is common to claim that there is widespread information asymmetry between firms and consumers, that consumers possess a high willingness to pay for privacy but that bargaining inequity prevents any Coasean solution, and that consumer dislike of information collection is due solely to market-based practices. If these three claims are correct that, indeed, bolsters the claim that digital markets have failed. Yet, these three claims have received surprisingly little empirical scrutiny in the digital privacy literature. This is even more surprising given the role these propositions play in supporting the claim of market failure and the claim that follows from it: that government should intervene.

Chapter three empirically evaluates these three related claims. If consumers are generally well-informed, if they have low willingness to pay, and if the potential for government intrusion contributes to their dislike of information collection, this suggests there is actually no market failure at all. In fact, at least with respect to Google, I find well-informed consumers, low willingness to pay, and distrust of potential government abuse.

This finding undermines the case for governmental remedies because it casts doubt on the significance of the problem.

Thus, it is possible to view this dissertation as comprising both an "internal" and an "external" critique of consensus views in the economics of digital privacy literature. If one grants the market has failed, it does not logically follow that government will improve on the failure. Furthermore, there is evidence to believe that the market has not failed. Taken together, these two arguments provide a strong case for a *laissez-faire* approach to privacy in digital environments.

REFERENCES

Acquisti, Alessandro. "Privacy in Electronic Commerce and the eEonomics of Immediate Gratification." In *Proceedings of the 5th ACM conference on Electronic commerce*, pp. 21-29. ACM, 2004.

Acquisti, Alessandro, and Jens Grossklags. "Privacy and Rationality in Individual Decision Making." *IEEE Security & Privacy* 1 (2005): 26-33.

Acquisti, Alessandro, and Hal R. Varian. "Conditioning Prices on Purchase History." *Marketing Science* 24, no. 3 (2005): 367-381.

Acquisti, Alessandro, and Jens Grossklags. "What can Behavioral Economics Teach us about privacy." *Digital Privacy: Theory, Technologies and Practices* 18 (2007): 363-377.

Acquisti, Alessandro, and Ralph Gross. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." In *International Workshop on Privacy Enhancing Technologies*, pp. 36-58. Springer Berlin Heidelberg, 2006.

Acquisti, Alessandro. "Privacy and Market Failures: Three Reasons for Concern, and Three Reasons for Hope." *J. on Telecomm. & High Tech. L.* 10 (2012): 227.

Acquisti, Alessandro, Leslie K. John, and George Loewenstein. "What is Privacy Worth?" *The Journal of Legal Studies* 42, no. 2 (2013): 249-274.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The Economics of Privacy." *Journal of Economic Literature* 54, no. 2 (2016): 442-492.

Akerlof, George A. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* (1970): 488-500.

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

Alston, Richard M., James R. Kearl, and Michael B. Vaughan. "Is There a Consensus among Economists in the 1990's?" *The American Economic Review* 82, no. 2 (1992): 203-209.

Arnott, Richard. “Time for Revisionism on Rent Control?” *The Journal of Economic Perspectives* 9, no. 1 (1995): 99-120.

Barzel, Yoram. *Economic Analysis of Property Rights*. Cambridge University Press, 1997.

Baumer, David L., Julia B. Earp, and J. C. Poindexter. “Internet Privacy Law: A Comparison between the United States and the European Union.” *Computers & Security* 23, no. 5 (2004): 400-412.

Baumol, William J. “Entrepreneurship: Productive, Unproductive, and Destructive.” *Journal of Business Venturing* 11, no. 1 (1996): 3-22.

Becker, Gary S., and Yona Rubinstein. “Fear and the Response to Terrorism: An Economic Analysis.” *University of Chicago mimeo* (2004).

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. “Privacy in e-commerce: Stated Preferences vs. Actual Behavior.” *Communications of the ACM* 48, no. 4 (2005): 101-106.

Bergkamp, Lucas. European Community Law for the New Economy. Intersentia nv, 2003.

Berman, Jerry, and Deirdre Mulligan. “Privacy in the Digital Age: Work in Progress.” *Nova L. Rev.* 23 (1998): 551.

Bibas, Steven A. “Contractual Approach to Data Privacy, A.” *Harv. JL & Pub. Pol’y* 17 (1994): 591.

Boettke, Peter J. 2001. *Economic Calculation. The Austrian Contribution to Political Economy* in *Calculation and Coordination. Essays on Socialism and Transitional Political Economy*, ed. Peter J. Boettke.

Boettke, Peter. “Liberty vs. Power in Economic Policy in the 20th and 21st Centuries.” *Journal of Private Enterprise* 22, no. Spring 2007 (2007): 7-36.

Boettke, Peter J., Christopher J. Coyne, and Peter T. Leeson. “Saving Government Failure Theory from Itself: Recasting Political Economy from an Austrian Perspective.” *Constitutional Political Economy* 18, no. 2 (2007): 127-143.

Boettke, Peter J., and Rosolino A. Candela. “Price Theory as Prophylactic against Popular Fallacies.” (2015).

Borgesius, Frederik J. Zuiderveen. 2015. *Improving privacy protection in the area of behavioural targeting*. Wolters Kluwer Law & Business.

Brown, Ian. "The Economics of Privacy, Data Protection and Surveillance." *Handbook on the Economics of the Internet* (2016): 247.

Buchanan, James M. "Afraid to be Free: Dependency as Desideratum." In *Policy Challenges and Political Responses*, pp. 19-31. Springer US, 2005.

Buchanan, James M. "Same Players, Different Game: How Better Rules Make Better Politics." *Constitutional Political Economy* 19, no. 3 (2008): 171-179.

Budnitz, Mark E. "Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate." *SCL Rev*. 49 (1997): 847.

Burke, Moira, Anthony Hornof, Erik Nilsen, and Nicholas Gorman. "High-Cost Banner Blindness: Ads Increase Perceived Workload, Hinder Visual Search, and are Forgotten." *ACM Transactions on Computer-Human Interaction (TOCHI)* 12, no. 4 (2005): 423-445.

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

Campbell, James, Avi Goldfarb, and Catherine Tucker. "Privacy Regulation and Market Structure." *Journal of Economics & Management Strategy* 24, no. 1 (2015): 47-73.

Clark, J. R., and Benjamin Powell. "Sweatshop Working Conditions and Employee Welfare: Say it Ain't Sew." *Comparative Economic Studies* 55, no. 2 (2013): 343-357.

Clarke, Roger. "Internet Privacy Concerns Confirm the Case for Intervention." *Communications of the ACM* 42, no. 2 (1999): 60-67.

"Click Here: The State of Online Advertising." *Adobe.* October 2012. https://www.adobe.com/aboutadobe/pressroom/pdfs/Adobe_State_of_Online_Advertising_Study.pdf

"Cloud Startup Zettabox Touts Privacy and Local Storage to Appeal to EU Customers." *PCWorld*. Last modified June 10, 2015. http://www.pcworld.com/article/2934112/cloud-startup-zettabox-touts-privacy-and-local-storage-to-appeal-to-eu-customers.html

Coase, Ronald H. "The Nature of the Firm." *Economica* 4, no. 16 (1937): 386-405.

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

Craig, Terence, and Mary E. Ludloff. "Privacy and Big Data." O'Reilly Media, Inc., 2011.

Cheung, Steven NS. "A Theory of Price Control." *The Journal of law and Economics* 17, no. 1 (1974): 53-71.

De Corniere, Alexandre, and Romain De Nijs. "Online Advertising and Privacy." *The RAND Journal of Economics* 47, no. 1 (2016): 48-72.

Demsetz, Harold. "Information and Efficiency: Another Viewpoint." *The Journal of Law & Economics* 12, no. 1 (1969): 1-22.

Demsetz, Harold. "Toward a Theory of Property Rights." *The American Economic Review* 57, no. 2 (1967): 347-359.

DeVries, Will Thomas. "Protecting Privacy in the Digital Age." *Berkeley Tech. LJ* 18 (2003): 283.

EU. 2002. *Directive on Privacy and Electronic Communications*.

EU. 2016. *General Data Protection Regulation*.

European Commission. Press Release Database. "*Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses.*" January 2012.

European Union Agency for Fundamental Rights. *Handbook on European Data Protection Law*. 2014.

Executive Office of the President. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. February 2012.

Executive Office of the President. President's Council of Advisers on Science and Technology. Report to the President. *Big Data and Privacy: A Technological Perspective*. May 2014.

Ezor, Jonathan. *Privacy and Data Protection in Business*. LexisNexis, 2012.

Facebook. 2016. *Company Info*. [Accessed 10/20/2016].

Farrell, Joseph. "Can Privacy be Just Another Good?" *J. on Telecomm. & High Tech. L.* 10 (2012): 251.

Federal Trade Commission. "*Protecting Consumer Privacy in an Era of Rapid Change*." FTC Report, Washington, DC (2012).

Federal Trade Commission. "Children's Online Privacy Protection Rule; Final Rule, Part II, 2013," *Federal Register* 78, no. 12 (January 17, 2013): http://www.gpo.gov/fdsys/pkg/FR-2013-01-17/pdf/2012-31341.pdf#page=38

Foldvary, Fred E., and Daniel B. Klein. "*The Half-Life of Policy Rationales: How New Technology Effects Old Policy Issues*." Knowledge, Technology & Policy 15, no. 3 (2002): 82-92.

Fulgoni, Gian, Marie Morn, and Mike Shaw. "How Online Advertising Works: Whither the Click in Europe." *comScore.* February 2010. http://iabireland.ie/wp-content/uploads/2012/08/Whither_the_Click_in_Europe.pdf

Fuller, Caleb S. "The Perils of Privacy Regulation." *The Review of Austrian Economics* (2016): 1-22.

Fuller, Caleb. 2017. "Privacy Law as Price Control." *Working Paper* (2017): 1–27.

"FTC Privacy Report." *Oliver and Grimsely.* Last modified May 2, 2013. http://www.olivergrimsley.com/2013/05/ftcprivacyreport/

Geiger, Jutta. "Transfer of Data Abroad by Private Sector Companies: Data Protection under the German Federal Data Protection Act, The." *German LJ* 4 (2003): 747.

Gellman, Robert. "Privacy, Consumers, and Costs-How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete." In *Digital Media Forum, Ford Foundation*. 2002.

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

Gneezy, Uri, and Aldo Rustichini. "A Fine is a Price." *The Journal of Legal Studies* 29, no. 1 (2000): 1-17.

Goldfarb, Avi, and Catherine E. Tucker. "Privacy Regulation and Online Advertising." *Management Science* 57, no. 1 (2011): 57-71.

Goldfarb, Avi, and Catherine Tucker. "Shifts in Privacy Concerns." *The American Economic Review: Papers and Proceedings* 102, no. 3 (2012): 349-353.

Granovetter, Mark S. "The Strength of Weak Ties." *American Journal of Sociology* (1973): 1360-1380.

Gross, Ralph, and Alessandro Acquisti. "Information Revelation and Privacy in Online Social Networks." In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp. 71-80. ACM, 2005.

Handrahan, Matthew. "IAP the Least Popular Form of Monetisation Among Players." *Gamesindustry.biz.* April 7, 2016. http://www.gamesindustry.biz/articles/2016-04-07-iap-the-least-popular-form-of-monetisation-among-players

Hanson, Robin. "Warning Labels as Cheap-Talk: Why Regulators Ban Drugs." *Journal of Public Economics* 87, no. 9 (2003): 2013-2029.

Hayek, Friedrich August. "The Use of Knowledge in Society." *The American Economic Review* (1945): 519-530.

Heath, Nick. "EU Privacy Laws to Spell an End to Facebook for Free?" *ZDNet.* Last modified January 10, 2013. http://www.zdnet.com/article/eu-privacy-laws-to-spell-an-end-to-facebook-for-free/

Hermalin, Benjamin E., and Michael L. Katz. "Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy." *Quantitative Marketing and Economics* 4, no. 3 (2006): 209-239.

Hirsch, Dennis D. "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation." *Seattle UL Rev*. 34 (2010): 439.

Hirshleifer, Jack. "Privacy: Its Origin, Function, and Future." *The Journal of Legal Studies* (1980): 649-664.

Higgs, Robert. "Regime Uncertainty." *The Independent Review* 1, no. 4 (1997): 561-590.

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

Hoofnagle, Chris Jay. "Privacy Self Regulation: A Decade of Disappointment." *Consumer Protection in the Age of the 'Information Economy'* (Jane K. Winn, ed.) (Ashgate 2006) (2005).

Hoofnagle, Chris Jay. "Beyond Google and Evil: How Policy Makers, Journalists and Consumers Should Talk Differently about Google and Privacy." *First Monday* 14, no. 4 (2009).

Hoofnagle, Chris Jay, Ashkan Soltani, Nathaniel Good, Dietrich J. Wambach, and Mika D. Ayenson. "Behavioral Advertising: The Offer You Cannot Refuse." *Harvard Law & Policy Review* 6, no. 2 (2012): 273.

Hoofnagle, Chris Jay, and Jan Whittington. "Free: Accounting for the Costs of the Internet's Most Popular Price." *UCLA L. Rev.* 61 (2013): 606.

Hui, Kai Lung, and Ivan PL Png. "Economics of Privacy." In Handbook of Information Systems and Economics. 2005.

Hummel, Patrick, and R. Preston McAfee. "When Does Improved Targeting Increase Revenue?" In *Proceedings of the 24th International Conference on World Wide Web*, pp. 462-472. ACM, 2015.

Ieuan Jolly. "Data Protection in United States: Overview." *PracticalLaw*. Last modified July 1, 2014. http://us.practicallaw.com/6-502-0467#a89631

Ikeda Sanford. The Dynamics of Interventionism. *Advances in Austrian Economics*. (8) 2005:21-57.

Jamal, Karim, Michael Maier, and Shyam Sunder. "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of Ecommerce Privacy Disclosure and Practice in the United States and the United Kingdom." *Journal of Accounting Research* 43, no. 1 (2005): 73-96.

Jenkins, Blair. "Rent Control: Do Economists Agree?" *Econ Journal Watch* 6, no. 1 (2009).

John, Leslie K., Alessandro Acquisti, and George Loewenstein. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information." *Journal of Consumer Research* 37, no. 5 (2011): 858-873.

Johnson, Bobbie. "Privacy's Dead: Facebook Chief." *The Sydney Morning Herald.* January 19, 2010. http://www.smh.com.au/business/privacys-dead-facebook-chief-20100118-mgs8.html

Kirzner, Israel M. *Discovery and the Capitalist Process*. University of Chicago Press, 1985.

Kesan, Jay P., and Andres A. Gallo. "Why are the United States and the European Union Failing to Regulate the Internet Efficiently? Going Beyond the Bottom-up and Top-down Alternatives." *European Journal of Law and Economics* 21, no. 3 (2006): 237-266.

Kim, Jin-Hyuk, and Liad Wagman. "Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis." *The RAND Journal of Economics* 46, no. 1 (2015): 1-22.

Kincaid, Jason. 2009. *Startup School: Wired Editor Chris Anderson on Freemium Business Models*. [Accessed 10/24/2016].

Kohnstamm, Jacob. 2013. *Working Document 02/2013 providing guidance on obtaining consent for cookies*. _ [Accessed 3/14/17].

Koppl, Roger. *Big Players and the Economic Theory of Expectations*. New York: Springer, 2002.

Lenard, Thomas M., and Paul H. Rubin. "In Defense of Data: Information and the Costs of Privacy." (2009).

Lerner, Josh. "The Impact of Privacy Policy Changes on Venture Capital Investment in Online Advertising Companies." *Analysis Group* (2012): 1-27.

Litan, Robert E. "Balancing Costs and Benefits of New Privacy Mandates." *AEI-Brookings Working Paper* (1999): 99-03.

Lin, Elbert. "Prioritizing Privacy: A Constitutional Response to the Internet." *Berkeley Tech. LJ* 17 (2002): 1085.

Lott Jr, John R., and Russell D. Roberts. "Why Comply: One-sided Enforcement of Price Controls and Victimless Crime Laws." *The Journal of Legal Studies* 18, no. 2 (1989): 403-414.

Madden, Mary. "Public Perceptions of Privacy and Security in the Post-Snowden Era." *Pew Internet.* Last modified November 12, 2014.

Madden, Mary, and Lee Rainie. 2015. "American Attitudes About Privacy, Security, and Surveillance." *Pew Internet.* Last modified May 20, 2015.

Manne, Geoffrey and Ben Sperry. "Innovation Death Panels and Other Economic Shortcomings of the White House Proposed Privacy Bill." *Truth on the Market* (blog). March 18, 2015, http://truthonthemarket.com/2015/03/18/innovation-death-

panels-privacy-bill/

Marthews, Alex, and Catherine Tucker. "Government Surveillance and Internet Search Behavior." (2015). *Available at SSRN 2412564*.

Martinez, Marian Garcia, Andrew Fearne, Julie A. Caswell, and Spencer Henson. "Co-Regulation as a Possible Model for Food Safety Governance: Opportunities for Public–Private Partnerships." *Food Policy* 32, no. 3 (2007): 299-314.

Mayer-Schönberger, Viktor. "Beyond Privacy, Beyond Rights—Toward a 'Systems' Theory of Information Governance." *California Law Review* (2010): 1853-1885.

Milberg, Sandra J., H. Jeff Smith, and Sandra J. Burke. "Information Privacy: Corporate Management and National Regulation." *Organization Science* 11, no. 1 (2000): 35-57.

Mises, Ludwig von. *Human Action, Scholars' Edition*. Auburn: Mises Institute. (1998).

Mole, Beth. "New Flu Tracker Uses Google Search Data Better than Google." *ArsTechnica*. November 9, 2015.

Neef, Dale. *Digital Exhaust: What Everyone Should Know about Big Data, Digitization and Digitally Driven Innovation*. Pearson Education, 2014.

New Singapore Data Protection Law: What You Need to Know. London: *Olswang LLP*, 2012. Accessed June 29, 2015. http://www.alston.com/files/docs/OlswangNew_Data_Protection_Law.pdf

Newman, Nathan. "The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google." *Wm. Mitchell L. Rev.* 40 (2014): 849-1611.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors." *Journal of Consumer Affairs* 41, no. 1 (2007): 100-126.

"Number of Monthly Active Facebook Users Worldwide as of 1st Quarter 2015 (in Millions)." *Statista*. Accessed June 25, 2015. http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

O'Brien, Daragh. "Start-ups, Data Privacy and Disruption." *PrivacyAssociation*. Last modified August 21, 2014. https://privacyassociation.org/news/a/start-ups-data-privacy-and-disruption/

Ohm, Paul. “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization.” *UCLA L. Rev.* 57 (2010): 1701.

Online Privacy Protection Act of 2003, California Statute. Section 22575-22579. http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579

Pasquale, Frank. “Privacy, Antitrust, and Power.” *Geo. Mason L. Rev.* 20 (2012): 1009.

Pavlou, Paul A. “State of the Information Privacy Literature: Where are we Now and Where Should we Go?” *MIS Quarterly* 35, no. 4 (2011): 977-988.

Penney, Jonathon W. “Chilling Effects: Online Surveillance and Wikipedia Use.” *Berkeley Tech. LJ* 31 (2016): 117.

Peppet, Scott R. “Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future.” *Nw. UL Rev.* 105 (2011): 1153.

Posner, Richard A. “Economic Theory of Privacy.” *Regulation* 2 (1978): 19.

Posner, Richard A. “The Economics of Privacy.” *The American Economic Review* (1981): 405-409.

Rochelandet, Fabrice, and Silvio HT Tai. “Do Privacy Laws Affect the Location Decisions of Internet Firms? Evidence for Privacy Havens.” *European Journal of Law and Economics* 42, no. 2 (2016): 339-368.

Rockoff, Hugh. *Price Controls*. Library of Economics and Liberty. 30 March 2017. http://www.econlib.org/library/Enc/PriceControls.html

Romanosky, Sasha, and Alessandro Acquisti. “Privacy Costs and Personal Data Protection: Economic and Legal Perspectives.” *Berkeley Technology Law Journal* 24, no. 3 (2009): 1061-1101.

Rose, E. "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*, pp. 180c-180c. IEEE, 2005.

Rosenberg, Eric. “The Business of Google.” *Investopedia.* August 5, 2016. Accessed October 25, 2016. http://www.investopedia.com/articles/investing/020515/business-google.asp

Rothbard, Murray Newton. *Man, Economy, and State*. Vol. 2. Princeton: Van Nostrand, 1962.

Sachs, Benjamin R. "Consumerism and Information Privacy: How Upton Sinclair can again save us from ourselves." *Virginia Law Review* (2009): 205-252.

Sarathy, Ravi, and Christopher J. Robertson. "Strategic and Ethical Considerations in Managing Digital Privacy." *Journal of Business Ethics* 46, no. 2 (2003): 111-126.

Schlag, Chris. "The New Privacy Battle: How the Expanding Use of Drones Continues to Erode our Concept of Privacy and Privacy Rights." *Pitt. J. Tech. L. & Pol'y* 13 (2012): 1-22.

Scholz, Lauren Henry. "Privacy as Quasi-Property." *Iowa L. Rev.* 101 (2015): 1113.

Scott, Mark. 2015. "Europe Approves Tough New Data Protection Rules." *The New York Times*. Accessed September 15, 2016. https://www.nytimes.com/2015/12/16/technology/eu-data-privacy.html?_r=0

Sharon Gaudin. "Social Networks Credited with Role in Toppling Egypt's Mubarak." *Computerworld*. Last modified February 11, 2011. http://www.computerworld.com/article/2513142/web-apps/social-networks-credited-with-role-in-toppling-egypt-s-mubarak.html

Shirky, Clay. "The Political Power of Social Media." *Foreign Affairs* 90, no. 1 (2011): 28-41.

Silberman, Jonathan I., and Garey C. Durden. "Determining Legislative Preferences on the Minimum Wage: An Economic Approach." *Journal of Political Economy* 84, no. 2 (1976): 317-329.

Sobel, Russell S. "Theory and Evidence on the Political Economy of the Minimum Wage." *Journal of Political Economy* 107, no. 4 (1999): 761-785.

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. NYU Press, 2004.

Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* (2006): 477-564.

Sowell, Thomas. *A Conflict of Visions.* New York: William Morrow, 1987.

Stigler, George J. “The Economics of Information.” *Journal of political economy* 69, no. 3 (1961): 213-225.

Stigler, George J. “An Introduction to Privacy in Economics and Politics.” *The Journal of Legal Studies* (1980): 623-644.

Strandburg, Katherine J. “Free Fall: The Online Market's Consumer Preference Disconnect.” *U Chi Legal F* 2013 (2013): 95-711.

“The Children’s Online Privacy Protection Act (COPPA).” *Consumercal*. Accessed June 26, 2015. http://consumercal.org/about-cfc/cfc-education-foundation/what-should-i-know-about-privacy-policies/california-online-privacy-protection-act-caloppa-2/

Swire, Peter. “Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the US Department of Commerce.” (1997).

Swire, Peter P. “Efficient Confidentiality for Privacy, Security, and Confidential Business Information.” *Brookings-Wharton Papers on Financial Services* 2003, no. 1 (2003): 273-310.

Tabarrok, Alex, and Tyler Cowen. "The End of Asymmetric Information." *Cato Unbound. http://www. cato-unbound. org/2015/04/06/alex-tabarrok-tyler-cowen/end-asymmetricinformation* (2015).

Taylor, Curtis R. “Consumer Privacy and the Market for Customer Information.” *RAND Journal of Economics* (2004): 631-650.

Thierer, Adam. “Privacy Law’s Precautionary Principle Problem.” *Me. L. Rev*. 66 (2013): 467.

Thomson, Judith Jarvis. “The Right to Privacy.” *Philosophy & Public Affairs* (1975): 295-314.

Tom Sands, email correspondence, May 28, 2015.

Tom Sands, email correspondence, May 12, 2016.

Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study.” *Information Systems Research* 22, no. 2 (2011): 254-268.

Tucker, Catherine E. “The Economics of Advertising and Privacy.” *International journal*

of Industrial organization 30, no. 3 (2012): 326-329.

Tucker, Catherine. 2016. "Privacy and the Internet". In *Handbook of Media Economics*, ed. by Simon Anderson, Joel Waldfogel, and David Stromberg. Elsevier.

Turow, Joseph, Jennifer King, Chris Jay Hoofnatle, Amy Bleakley, and Michael Hennessy. "Americans Reject Tailored Advertising and Three Activities that Enable It." *Departmental Papers (ASC)* (2009): 137.

United States Congress. *Consumer Privacy Bill of Rights Act of 2015*. Administration Discussion Draft. https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf

Varian, Hal R. "Economic Aspects of Personal Privacy." In *Internet Policy and Economics*, pp. 101-109. Springer US, 2009.

Wauters, Robin. "Analysis: An Appraisal of the Burgeoning European 'App Economy,' and its Growing Pains." *Tech.eu.* Last modified February 13, 2014. http://tech.eu/features/540/analysis-app-economy-europe/

Weyl, E. Glen. "The Price Theory of Two-Sided Markets." *Available at SSRN* 1324317 (2009).

Whittington, Jan, and Chris Jay Hoofnagle. "Social Networks and the Law: Unpacking Privacy's Price." *NCL Rev.* 90 (2012): 1327-2162.

Yan, Jun, Ning Liu, Gang Wang, Wen Zhang, Yun Jiang, and Zheng Chen. "How Much can Behavioral Targeting Help Online Advertising?" In *Proceedings of the 18th International Conference on World Wide Web*, pp. 261-270. ACM, 2009.

Yang, Shihao, Mauricio Santillana, and S. C. Kou. "Accurate Estimation of Influenza Epidemics Using Google Search Data Via ARGO." *Proceedings of the National Academy of Sciences* 112, no. 47 (2015): 14473-14478.

Vila, Tony, Rachel Greenstadt, and David Molnar. "Why We Can't be Bothered to Read Privacy Policies Models of Privacy Economics as a Lemons Market." In *Proceedings of the 5th International Conference on Electronic Commerce*, pp. 403-407. ACM, 2003.

"Zettabox Gambles on EU Privacy Law to Take on Google, Amazon and Microsoft in Cloud Storage Battle." *Techworld.* Last modified June 11, 2015. http://www.techworld.com/news/cloud/cloud-startup-zettabox-touts-privacy-and-

local-storage-to-appeal-to-eu-customers-3615326/

CURRICULUM VITAE

Caleb S. Fuller was born on September 19, 1990 in Columbus, Indiana and is an American citizen. He graduated from Christian Liberty Academy in 2009. He received his Bachelor of Arts degree in economics from Grove City College in 2013. He began attending George Mason University in the fall of 2014 and received his Master of Arts degree from George Mason University in 2015. His research has been published in the *Review of Austrian Economics,* the *Journal of Entrepreneurship and Public Policy,* the *Independent Review, Economic Affairs,* and the *Journal of Business Venturing Insights.* In fall 2017, he will begin as an assistant professor at Grove City College.