

The Perils of Privacy Regulation

Caleb S. Fuller^{*†}

March 25, 2016

Abstract

Digital privacy law is intended to correct market failure, specifically information asymmetry. Though legislators allegedly craft digital privacy regulation to protect consumers, some advocates have understated the costs that digital privacy laws impose. With Kirzner's market process framework as a guide, I investigate examples demonstrating that digital privacy law may restrict valuable information flows, increase privacy and security risks, erect barriers to entry, heighten entrepreneurial uncertainty, and incite rent-seeking. My research suggests that policy-makers should reconsider the costs of digital privacy law.

Keywords: Economics of Privacy, Regulation, Market Process

JEL-Classification: K29, L51, B53

^{*}Email: cfuller5@gmu.edu.

[†]I wish to thank Chris Coyne, Nicholas Pusateri, Renato Lima de Oliveira, and participants in George Mason University's Hayek Program's weekly graduate student paper seminar for their helpful remarks on drafts of this paper. Any errors are my own.

1 Introduction

In a digitally connected society, 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 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."

Using insights from the market process tradition in economics, I argue that these calls for top-down regulatory solutions should be tempered by a full accounting of the costs which these regulations may impose. What are the costs of relying for privacy protection on a regulatory agency rather than seeking for it in pure market provision? Other examinations into the costs of digital privacy regulation (Rubin, 2009) have focused extensively on the ways that these laws constrict the free flow of information. As Rubin (2009) indicates, this focus is due to the economists' preoccupation with the perfect competition model in which perfectly informed agents are the ideal. Though I also discuss the constriction of value information flows, I take a slightly different tact than authors such as 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, 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. Digital privacy law imposes costs by stifling the unfettered market process, by failing to provide an analogue to the markets’ disciplinary corrective of profit-loss accounting, and by creating superfluous avenues of discovery.

Following Rubin (2009), I examine regulations which curtail (or even ban) the collection and use of “nonsensitive information”—information 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, the sale of that information to third parties, the collection of data from social media accounts, and the use of information gathered online to pinpoint an individual’s identity or location. The reasons for this collection are myriad, but common ones include the ability to target advertising directly toward interested consumers or conduct demographic analysis on one’s customer base.

Visions of a world where online vendors 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, 2013) may admittedly frighten the average internet user.¹ Buchanan (2004) notes people are “afraid to be free,” and this appears notably so on the internet. Some prefer Buchanan’s “parental socialism,” desiring the state to impose privacy rules. Yet, as DeVries (2003) maintains, the idea that individuals have a property right in personal

¹See Hirsch (2011) 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.

information is a “recent” invention.

There is, however, 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.² This paper does not adjudicate that debate. For the purposes of this analysis, I follow Posner (and others) in maintaining that the state should not assign property rights to individuals in the information they generate through digital activities. As Posner (1978) states, “people should not—on economic grounds in any event—have a right to conceal material facts about themselves.” Stigler (1980) agrees, arguing that, “...there is no reason to interfere to protect one party...the efficient amount of information will be provided in transactions, given the tastes of the parties for knowledge and privacy.” To the extent that individuals wish to conceal personal information, they should be free to make the appropriate investments, but others should also be free to uncover this information through investments of their own.³

Digital privacy law is not neutral with respect to the workings of the market; as Kirzner (1985) argues, all intervention stifles and redirects the market process. Specifically, digital privacy law has the potential to restrict valuable information flows, exacerbate privacy and security risks, raise barriers to entry, increase entrepreneurial uncertainty, and introduce new opportunities for political entrepreneurship. As such, my research suggests that digital privacy 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 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

²See, 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).

³An example might help to clarify this logic. Most would not contend that a brick-and-mortar store violates the property rights of its clients by maintaining a video camera for security purposes. It should be further noted that such a camera poses the potential for greater privacy intrusions than do many of the technologies that Internet sellers use to collect information about their customers (see Rubin, 2009 for a discussion of the types of information that firms commonly collect and the technologies they use to collect it).

illuminate five costs of digital privacy law. Section 4 concludes with implications.

2 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...”⁴ Posner (1981) argues that legislation which protects personal data results in efficiency losses due to information asymmetries, since employers 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 which are themselves based on appeals to asymmetric information. The first is that privacy is a fundamental human right that internet companies often disregard (Lenard and Rubin 2009). The second is that the market for digital privacy fails; consequently, regulation must correct the deficiencies inherent in the unhampered market.

Solove (2004) asserts 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 in this context. “Big Data and Privacy: A Technological Perspective” (2014) refers to “privacy rights” throughout, stating that:

⁴Hirshleifer (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.

“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 (2011) 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). In a similar vein, Thierer (2014) notes that privacy legislation is characterized (unfortunately) 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).

In the same way that regulatory agencies purport to ensure consumers’ best interests by imposing food safety mandates,⁵ groups like the FTC maintain they are protecting vital consumer interests by passing digital privacy law. This market-failure reasoning, however, appears dubious.

⁵Hirsch (2011) advocates for 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).

First, lack of information does not entail that consumers are unable to act in accordance with their preferences. The information informing any 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” (Demsetz, 1969) that condemns the real world to failure via comparison to an inherently unobtainable model. Third, some appear puzzled by 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, without profit-and-loss accounting, it is impossible to determine whether bureaucratic strictures regulate data in a manner consistent with consumer preference. Even if it were granted that markets under-provide a good, it would not follow that governments provide the optimal quantity (Kirzner, 1985).

Market process theory illuminates some costs that advocates of digital privacy law overlook. Identifying these costs is not a shut case against regulation since advocates might contend that the benefits outweigh attendant costs. Cataloguing such costs allows us to evaluate the debate holistically, however. To the extent that consumer privacy laws restrict valuable information flows, increase security risks, raise barriers to entry, heighten uncertainty, or incentivize rent-seeking, they are costly.

Kirzner’s (1985) discussion of regulation illuminates many of the costs digital privacy law imposes. First, Kirzner discusses the “*unsimulated discovery process*.”⁶ Because there are no market prices providing feedback, government officials cannot know the appropriate price or quantity of a good to supply. Technology only heightens the complexity of the economic system, rendering it less knowable (Klein and Foldvary, 2002). As I demonstrate in Sections 3.1 and 3.2, 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.⁷

⁶Kirzner also discusses the “*undiscovered discovery process*,” but that is unimportant for this discussion.

⁷Note 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.

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 consist of opportunity costs, they are impossible to measure. In Section 3.3, I demonstrate the subtle ways that digital privacy law erects barriers to entry. Complementary to Kirzner’s insight, Higgs (1997) argues that uncertainty about policy changes dampens investment activity. Higgs’ insights complement Kirzner’s because ever-shifting legal rules create an environment in which entrepreneurs experience heightened difficulty forecasting a project’s rate of return. As I show in Section 3.4, 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 manufactures “entirely new, and not necessarily desirable opportunities for entrepreneurial discovery,” (1985: 144), the “*superfluous discovery process*.” In the language of Baumol (1990), 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 the citizenry. At the same time, domestic internet-based companies may look to the state for protection from foreign competition. In Section 3.5, I show how digital privacy legislation is one way that political entrepreneurs may balance these competing demands.

3 Some Overlooked Costs of Digital Privacy Regulation

3.1 Restricting Valuable Information Flows

In the absence of market prices to guide decision-making, privacy regulators may fail to provide

the optimal level of privacy protection. Instead, they might err by constricting information flows even when unrestricted flows align with demonstrated consumer preference. Consumers may, indeed, incur costs 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.

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 solutions that balance these competing demands. By contrast, government restriction of information flows often focuses exclusively on the costs of accessing personal information, while understating the benefits. Regulation persists 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.

The EU’s Data Protection Directive is one example of a regulation that focuses on the costs to the exclusion of the benefits of information flow.⁸ 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 meets stringent requirements. The ban covers information collected by personal or automated means and extends to anonymized data. The 2012 FTC report, “Protecting Consumer Privacy in an Era of Rapid Change,” also adopts a paternalistic approach that seeks to deny customers the ability to make this trade-off according to their own valuations. It states, “...com-

⁸The Directive also contains provisions for protecting against true invasions of property, such as credit card theft.

panies 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 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. The proposed draft would prohibit the collection of personal information of EU citizens by any organization—even one located outside the EU. 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). As one legal expert observes, the new 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).

Varian (1996) 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 they reduce the total quantity of advertisements needed to achieve that sale (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 (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 dependent on business models that utilize personal information.

Though over a billion users have demonstrated their preference for Facebook's service, some commentators see applications 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).⁹ 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.

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 access to dispersed, local, knowledge that no individual mind could access.

⁹An 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.

As one example, consider Google’s “Flu Trends” algorithm. This program detects search terms that indicate the presence of influenza. 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 ordinary methods (hospital records, for instance), the analysis and dispersion of such information would likely be time-consuming and costly. The Google service aggregates local knowledge, making it almost instantly available to individuals looking to avoid “hot-spots” or to those trying to identify an outbreak. Consequently, it facilitates the faster containment of epidemics as individuals are able to easily avoid hard-hit areas.¹⁰

Thus, in this case, restriction of information flows reduces 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.

3.2 Increasing Privacy and Security Risks

Because regulators possess neither the local, specialized knowledge, nor the profit incentives to make informed decisions, privacy regulation also has the potential to accomplish the opposite of its stated intentions—it may, in fact, increase security threats. That is, government failure is a possibility in the case of privacy provision. 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 information to identify specific individuals. The proposed 2015 “Consumer Privacy Bill of Rights Act”¹¹ would force firms to abandon such 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

¹⁰The knowledge that Google’s flu tracker algorithm aggregates is Hayekian in the sense that it is localized and dispersed, though not tacit.

¹¹This piece of legislation is based on the Obama Administration’s 2012 “Consumer Privacy Bill of Rights.”

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 a much easier target for identity thieves.¹² Consequently, legislation crafted with the intent to protect so-called privacy rights may enable serious property rights violations.¹³ 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.

Another example of privacy law having the opposite of its intended effect comes from a case-study that compares the privacy practices of e-commerce companies in the U.S. and the U.K. Market process theory argues 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 this particular margin.

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

¹²I 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.

¹³As Hirsch (2011) 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).

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 expand the privacy risks that consumers face as seen in the two preceding examples. Section 4.5 demonstrates that where digital privacy legislation is concerned, public interest rhetoric is not sufficient to ensure public interest outcomes.

3.3 Erecting Barriers to Entry

Tucker et al. (2015) discuss the EU Data Protection 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 browsing patterns—opt-in requires obtaining the user's explicit consent. Though not the focus of their analysis, these authors mention how firms may use TrustE, a software provider that ensures compliance with the opt-in directives as handed down by the EU. As these authors note, installing the TrustE software imposes a fixed cost on all firms seeking the ability to support customized advertising (Tucker 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. 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 the complexity of COPPA has impacted startups

for which he has worked, technology executive Tom Sands¹⁴ (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 unviable to pursue that age group. Larger companies, with significant development and legal resources, are at an obvious advantage in these 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 an initial 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.

Market process theory also suggests that the mandate to discreetly dispose of data after the purpose for which it was collected has been fulfilled hampers the potential for entrepreneurial innovation. It is impossible for any individual or firm to perfectly foresee future market conditions or 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 EU’s extensive Directive is another instance of legislation imposing compliance costs that favor large firms. Consider the “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 demon-

¹⁴Sands is a technology executive who has experience with large companies as well as several startups, including several directly involved in providing digital privacy solutions.

strate 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.

Digital privacy consultant, Daragh O'Brien, writing in a popular outlet (PrivacyAssociation.com, 2014), further discusses the anti-competitive 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.

The laws discussed above impose 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.

3.4 Heightening Regime Uncertainty

Higgs (1997) identifies the uncertainty induced by capricious law-makers; this 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’ insights contrasts with those who argue that privacy legislation reduces uncertainty. Milberg et al. (2000), for example, argue that societies with high “uncertainty avoidance” prefer regulatory approaches to privacy protection. By this, the authors mean that consumers may operate with less fear of privacy intrusion if privacy law is extensive.

The EU’s proposed GDPR also states that its measures will improve consumer confidence on-line, 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 system of U.S. privacy law constitutes a “sectoral model.” That is, law-makers pass rules reactively¹⁵ 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. 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, and one with potentially large consequences. As innovators observe this pattern of reactive legislation, they may become 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

¹⁵Note that Milberg et al. (2000) argue that one benefit of digital privacy law is that it would *correct* the “reactive” failures of private firms.

(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...” Further, 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.¹⁶

Finally, to propose a standardized, international privacy law, while possibly serving as a corrective to consumers' uncertainty, would likely only exacerbate the knowledge 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. 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 increases the uncertainty faced by the innovator. With vaguely worded legislation, entrepreneurs face uncertainty concerning the scope of activities that the law covers. This disincentives the innovation of new technologies that touch on privacy issues and it also discourages entrance into markets governed by laws that cede discretion to bureaucratic decision-makers.

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

¹⁶Obviously, the same conclusion holds for entrepreneurs in any country.

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) targets 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, which could include a desire for increased power or a larger budget. 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 technolo-

gies 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.

3.5 Inciting Rent-Seeking

Firms can leverage digital privacy legislation to further their material interests. This is because legislation creates new, “superfluous” avenues for entrepreneurial discovery. Disequilibrium 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.¹⁷

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.” The deputy director of enforcement for data protection in France, however, also comments on the Facebook case that, “there are privacy issues.”

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

17

Rigorous public choice analysis also demands symmetry of assumptions regarding private and public actors. To the extent that internet users exhibit the biases and irrationalities that Acquisti (2007) identifies, this implies that political actors—themselves internet users—suffer from the same misperceptions. How do these misperceptions on the part of legislators affect the laws that they write? If consumers regularly underestimate the risks of some activities and overestimate the risks of others, should we expect political actors to be systematically superior in their own assessment of digital privacy risks? Do political actors resort to the same flawed heuristics that allegedly guide consumer decision making?

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. Digital privacy legislation may strike a blow at Facebook, while leaving the telecommunications firms unscathed.

As another example, consider European cloud storage providers that are positioned to benefit even more directly from the imposition of the EU's strict digital privacy laws. 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 preceding discussion demonstrates that domestic firms may leverage digital privacy legislation in order to bar 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.”

Similarly to how European telecommunication companies and Zettabox benefit from digital privacy law, Kitchenman discusses how privacy legislation shields European financial services providers from having to compete with foreign providers. EU privacy laws give domestic financial services providers an implicit monopoly over consumer information by denying foreign entrants the necessary information to offer competing services. The result has been a concentration of these services in the largest banks, inability of foreign providers to compete, lower-quality customer service, and higher prices (Bergkamp, 2003). In this case, it is evident that the concentrated special interests of large financial institutions benefit from laws that, at first glance, might seem contrary to their ends.

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.

Since 1977, the Federal Data Protection Act has governed German privacy issues. This legislation, however, imposes significant fixed costs on even the smallest of firms. As Geiger (2003) details, the law applies to “private sector companies in so far as they process or use personal data in or 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. The additional fact that so few German citizens have appealed to the law to enforce their digital privacy rights raises suspicions that rent-seeking motives may have been in play.

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.

4 Conclusion

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 Tucker, 2015). This paper has offered several reasons to question whether those dual mandates—promotion of innovation and protection of individual privacy—are compatible ones. I do not maintain that all five costs that I identify hold in every case, but simply note them where the existing literature has failed to do that much. As such, this paper has three main implications.

First, the current literature under-values the ability of entrepreneurs to offer solutions to 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 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 encroach 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. 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—as does the behavioral economics of privacy literature—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 touched on the presence of “web seals” as a way for firms to signal the quality of their privacy protection. Future 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.

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 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, anticipates the knowledge problems that digital privacy 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. Their perspective reminds us that regulation always imposes costs and that entrepreneurs rarely fail to devise clever solutions to tricky problems. Without their voices, regulatory responses—ones that preempt the entrepreneurial solution altogether—may be the inevitable outcome.

References

- [1] Acquisti, A., and J. Grossklags. "Losses, Gains, and Hyperbolic Discounting: Privacy Attitudes and Privacy Behavior." *The Economics of Information Security* (2004): 179-186.
- [2] Acquisti, Alessandro, and Jens Grossklags. "Privacy and Rationality in Individual Decision Making." *IEEE Security & Privacy* 1 (2005): 26-33.
- [3] Acquisti, Alessandro, and Jens Grossklags. "What Can Behavioral Economics Teach Us about Privacy." *Digital Privacy: Theory, Technologies and Practices* (2007): 363-377.
- [4] Acquisti, Alessandro. "Nudging Privacy: The Behavioral Economics of Personal Information." *IEEE Security & Privacy* 6 (2009): 82-85.
- [5] Acquisti, Alessandro. "Privacy and Market Failures: Three Reasons for Concern, and Three Reasons for Hope." *J. on Telecomm. & High Tech. L.* 10 (2012): 227.
- [6] Acquisti, Alessandro. "The Economics of Privacy: Theoretical and Empirical Aspects." Preliminary. (2013).
- [7] Acquisti, Alessandro. "The Economics and Behavioral Economics of Privacy." *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (2014): 98-112.
- [8] Baumol, William J. "Entrepreneurship: Productive, Unproductive, and Destructive." *Journal of Business Venturing* 11, no. 1 (1996): 3-22.
- [9] Bergkamp, Lucas. *European Community Law for the New Economy*. Intersentia nv, 2003.
- [10] Bibas, Steven A. "Contractual Approach to Data Privacy, A." *Harv. JL & Pub. Pol'y* 17 (1994): 591.
- [11] Buchanan, James M. "Afraid to be Free: Dependency as Desideratum." In *Policy Challenges and Political Responses*, pp. 19-31. Springer US, 2005.
- [12] Budnitz, Mark E. "Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate." *SCL Rev.* 49 (1997): 847.
- [13] Campbell, James, Avi Goldfarb, and Catherine Tucker. "Privacy Regulation and Market Structure." *Journal of Economics & Management Strategy* 24, no. 1 (2015): 47-73.
- [14] Clarke, Roger. "Internet Privacy Concerns Confirm the Case for Intervention." *Communications of the ACM* 42, no. 2 (1999): 60-67.
- [15] "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>

- [16] Coase, Ronald H. "The Lighthouse in Economics." *Journal of Law and Economics* 17, no. 2 (1974): 357-376.
- [17] Craig, Terence, and Mary E. Ludloff. "Privacy and Big Data." O'Reilly Media, Inc., 2011.
- [18] Demsetz, Harold. "Information and Efficiency: Another Viewpoint." *The Journal of Law & Economics* 12, no. 1 (1969): 1-22.
- [19] DeVries, Will Thomas. "Protecting Privacy in the Digital Age." *Berkeley Tech. LJ* 18 (2003): 283.
- [20] 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.
- [21] European Union Agency for Fundamental Rights. *Handbook on European Data Protection Law*. 2014.
- [22] 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.
- [23] 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.
- [24] Ezor, Jonathan I. *Privacy and Data Protection in Business: Laws and Practices*. Lexis-Nexis, 2012.
- [25] Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change." FTC Report, Washington, DC (2012).
- [26] 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>
- [27] "Flu Trends. How Does This Work?" *Google*. Accessed June 25, 2015. <https://www.google.org/flutrends/about/how.html>
- [28] 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.
- [29] "FTC Privacy Report." *Oliver and Grimseley*. Last modified May 2, 2013. <http://www.olivergrimsley.com/2013/05/ftcprivacyreport/>
- [30] 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.

- [31] Granovetter, Mark S. "The Strength of Weak Ties." *American Journal of Sociology* (1973): 1360-1380.
- [32] Hayek, F. A. "The Use of Knowledge in Society." *American Economic Review* 35, no. 4 (1945): 519-530.
- [33] Hayek, F. A. *Law, Legislation and Liberty: A New Statement of the Liberal Principles of Justice and Political Economy*, v. 1: Rules and Order. London: Routledge, 1973.
- [34] Hayek, F.A. *New Studies in Philosophy, Politics, Economics, and the History of Ideas*. Chicago: University of Chicago Press, 1978.
- [35] 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/>
- [36] 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.
- [37] Henry, Lauren. "Privacy as Quasi-Property." *Iowa Law Review*, Forthcoming (2015).
- [38] Hirsch, Dennis D. "Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation, The." *Seattle UL Rev.* 34 (2010): 439.
- [39] Hirshleifer, Jack. "Privacy: Its Origin, Function, and Future." *The Journal of Legal Studies* (1980): 649-664.
- [40] Higgs, Robert. "Regime Uncertainty." *The Independent Review* 1, no. 4 (1997): 561-590.
- [41] 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).
- [42] Hui, Kai Lung, and I. P. L. Png. "The Economics of Privacy." *Economics and Information Systems* (2006).
- [43] Ieuan Jolly. "Data Protection in United States: Overview." *PracticalLaw*. Last modified July 1, 2014. <http://us.practicallaw.com/6-502-0467#a89631>
- [44] Ikeda Sanford. *The Dynamics of Interventionism*. *Advances in Austrian Economics*. 2005; 8:21-57.
- [45] 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.

- [46] Kirzner, Israel M. *Discovery and the Capitalist Process*. University of Chicago Press, 1985.
- [47] Litan, Robert E. “Balancing Costs and Benefits of New Privacy Mandates.” AEI-Brookings Working Paper (1999): 99-03.
- [48] Lin, Elbert. ”Prioritizing Privacy: A Constitutional Response to the Internet.” *Berkeley Tech. LJ* 17 (2002): 1085.
- [49] 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/>
- [50] 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.
- [51] Mary Madden. “Public Perceptions of Privacy and Security in the Post-Snowden Era.” *Pew Internet*. Last modified November 12, 2014. <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>
- [52] Mayer-Schönberger, Viktor. “Beyond Privacy, Beyond Rights—Toward a ‘Systems’ Theory of Information Governance.” *California Law Review* (2010): 1853-1885.
- [53] 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.
- [54] Mises, Ludwig von. *Human Action*. Ludwig von Mises Institute, 1949.
- [55] Neef, Dale. *Digital Exhaust: What Everyone Should Know about Big Data, Digitization and Digitally Driven Innovation*. Pearson Education, 2014.
- [56] *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
- [57] “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/>
- [58] O’Brien, Daragh. “Start-ups, Data Privacy and Disruption.” *Privacy Association*. Last modified August 21, 2014. <https://privacyassociation.org/news/a/start-ups-data-privacy-and-disruption/>
- [59] 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>

- [60] Pasquale, Frank. "Privacy, Antitrust, and Power." *Geo. Mason L. Rev.* 20 (2012): 1009.
- [61] 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.
- [62] Posner, Richard A. "Economic Theory of Privacy." *Regulation* 2 (1978): 19.
- [63] Posner, Richard A. "The Economics of Privacy." *The American Economic Review* (1981): 405-409.
- [64] Rothbard, Murray Newton. *Man, Economy, and State*. Vol. 2. Princeton: Van Nostrand, 1962.
- [65] Sarathy, Ravi, and Christopher J. Robertson. "Strategic and Ethical Considerations in Managing Digital Privacy." *Journal of Business Ethics* 46, no. 2 (2003): 111-126.
- [66] 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>
- [67] Shirky, Clay. "The Political Power of Social Media." *Foreign Affairs* 90, no. 1 (2011): 28-41.
- [68] Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. NYU Press, 2004.
- [69] Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* (2006): 477-564.
- [70] Stigler, George J. "An Introduction to Privacy in Economics and Politics." *The Journal of Legal Studies* (1980): 623-644.
- [71] "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/>
- [72] Swire, Peter P. "Efficient Confidentiality for Privacy, Security, and Confidential Business Information." *Brookings-Wharton Papers on Financial Services* 2003, no. 1 (2003): 273-310.
- [73] Thierer, Adam. "Privacy Law's Precautionary Principle Problem." *Me. L. Rev.* 66 (2013): 467.
- [74] Tom Sands, email correspondence, May 28, 2015.
- [75] 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>

- [76] Varian, Hal R. "Economic Aspects of Personal Privacy." *Privacy and Self-regulation in the Information Age* (1996).
- [77] "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/>