Journal of Economic Literature 2016, 54(2), 442–492
http://dx.doi.org/10.1257/jel.54.2.442

The Economics of Privacy†

Alessandro Acquisti, Curtis Taylor, and Liad Wagman*

This article summarizes and draws connections among diverse streams of theoretical and empirical research on the economics of privacy. We focus on the economic value and consequences of protecting and disclosing personal information, and on consumers' understanding and decisions regarding the trade-offs associated with the privacy and the sharing of personal data. We highlight how the economic analysis of privacy evolved over time, as advancements in information technology raised increasingly nuanced and complex issues. We find and highlight three themes that connect diverse insights from the literature. First, characterizing a single unifying economic theory of privacy is hard, because privacy issues of economic relevance arise in widely diverse contexts. Second, there are theoretical and empirical situations where the protection of privacy can both enhance and detract from individual and societal welfare. Third, in digital economies, consumers' ability to make informed decisions about their privacy is severely hindered because consumers are often in a position of imperfect or asymmetric information regarding when their data is collected, for what purposes, and with what consequences. We conclude the article by highlighting some of the ongoing issues in the privacy debate of interest to economists. (*JEL* D82, D83, G20, I10, L13, M31, M37)

1. *Why an Economics of Privacy*

The value and regulation of information assets have been among the most interesting areas of economic research since Friedrich Hayek's 1945 treatise on the use of knowledge in society. Contributions to what has become known as the field of *information economics* have been among the most influential, insightful, and intriguing in the

*Acquisti: Heinz College, Carnegie Mellon University. Taylor: Department of Economics, Duke University. Wagman: Stuart School of Business, Illinois Institute of Technology. We are grateful for useful comments and suggestions provided by the reviewing team, as well as by Omri Ben-Shahar, Rainer Boheme, Alessandro Bonatti, Ryan Calo, James Cooper, Avi Goldfarb, Jens Grossklags, Chris Hoofnagle, Kai-Lung Hui, Nicola Jentzsch, Jin-Hyuk Kim, Brad Malin, Helen Nissenbaum, Andrew Odlyzko, Randal Picker, Ivan Png, Soren Preibusch, Giancarlo Spagnolo, Lior Strahilevitz, Catherine Tucker, Tommaso Valletti, Hal Varian, and Frederik Zuiderveen Borgesius. Acquisti gratefully acknowledges support from the Alfred P. Sloan Foundation and the Carnegie Corporation of New York via an Andrew Carnegie Fellowship. Taylor's research was supported in part by NSF grant SES-1132187. Wagman gratefully acknowledges support from the Yahoo Faculty Research and Engagement Program. The statements made and views expressed in this manuscript are solely the responsibility of the authors. All errors are the authors' own.

† Go to http://dx.doi.org/10.1257/jel.54.2.442 to visit the article page and view author disclosure statement(s).

profession. Seminal studies have investigated the informative role of prices in market economies (Stigler 1961); the creation of knowledge and the incentives to innovate (Arrow 1962); the prevalence of asymmetric information and adverse selection (Akerlof 1970); the transmission of private information through signaling activity (Spence 1973); and voluntary disclosures (Grossman 1981; Milgrom 1981). It may be proper, however, to think of information economics not as a single field, but as an amalgam of many related subfields. One such subfield now receiving growing attention by economists is the subject of this article: the study of privacy.

Privacy is difficult to define. It means different things to different people. It has been described as the protection of someone's personal space and their right to be left alone (Warren and Brandeis 1890); the control over and safeguarding of personal information (Westin 1967); and an aspect of dignity, autonomy, and ultimately human freedom (Schoeman 1992). While seemingly different, these definitions are related, because they pertain to the boundaries between the self and the others, between private and shared, or, in fact, public (Altman 1975).

As individuals and as consumers, we constantly navigate those boundaries, and the decisions we make about them determine tangible and intangible benefits and costs, for ourselves and for society. Thus, at its core, the economics of privacy concerns the trade-offs associated with the balancing of public and private spheres between individuals, organizations, and governments. Economists' interest in privacy has primarily focused on its *informational* dimension: the trade-offs arising from protecting or sharing of personal *data*.[1] Other subfields of information economics therefore relate to the topic of this article, because they pertain to the trade-offs arising from the public or private status of information. For instance, an auction may be structured in such a way that its participants will reveal their true costs or valuations, or a tax mechanism may be designed so that the agents will truthfully reveal their types. However, whereas research on auctions and optimal taxation may pertain to the *private* information of abstract economic agents (which could be consumers, firms, or other entities), the field of *privacy economics*, which is our focus, pertains more specifically to *personal* information of actual individuals. As a consequence, of course, the field is often influenced by research in the other branches of information economics.

This article reviews the theoretical and empirical economic literature investigating individual and societal trade-offs associated with sharing and protecting personal data. In particular, it focuses on the flow and use of information about individuals by firms. In so doing, the article identifies a number of key themes. One theme is that characterizing a single unifying economic theory of privacy is hard, because privacy issues of economic relevance arise in widely diverse contexts. Nevertheless, we are able, within a given context, to identify a number of robust theoretical insights emerging from the literature. A second key theme is that both economic theory and empirical analysis of privacy expose varying scenarios. In some, privacy protection can decrease individual and societal welfare; in others, privacy protection enhances them. Thus, it is not possible to conclude

[1] Some of the economic issues we consider in this article arise when personal information is or becomes no longer private because it is shared with, or accessed by, one or more entities (for instance, an email provider monitoring a user's messages). Other issues arise when that information is or is made public, and thus possibly accessible by a multitude of entities (for instance, a member of a social networking site publicly sharing personal information on her profile). In this article, we will sometimes use the term "public" to refer to both types of scenarios—that is, to information that is no longer private.

unambiguously whether privacy protection entails a net "positive" or "negative" change in purely economic terms: its impact is context specific. A third key theme relates to the observation that consumers are rarely (if ever) completely aware about privacy threats and the consequences of sharing and protecting their personal information. Hence, market interactions involving personal data often take place in the absence of individuals' fully informed consent. Furthermore, specific heuristics may profoundly influence consumers' privacy decision making.

1.1 *The Value of Personal Data and the Value of Privacy*

Economists' interest in informational privacy, generally intended as the control or protection of personal information, can be readily understood: the protection and disclosure of personal data are likely to generate trade-offs with tangible economic dimensions. The transition of modern economies toward production of knowledge and recent radical advancements in information technology (in particular, the rise of the Internet) have vastly enlarged the amount of individual information that can be collected, stored, analyzed, and repurposed for new uses. The ascent of the so-called Web 2.0 (blogs, social media, online social networks) has rendered individuals no longer mere consumers of information, but public producers of often highly personal data. The spread of mobile computing and sensor technologies has blurred the distinctions between digital and physical, online and offline. All of this has led to services that simultaneously generate and capture digital trails of personal and professional activities—activities that were previously conducted in private and left little or no trace.[2] Simultaneously, the Internet has evolved from an architecture of decentralized and possibly anonymous interactions (Berners-Lee 2000), to one where packets of data capturing all types of behaviors (from reading to searching, from relaxing to communicating) are uniquely (Bendrath and Mueller 2011) and sometimes personally (Xie, Yu, and Abadi 2009) identified. In this environment, a few "gatekeeper" firms are in a position to control the tracking and linking of those behaviors across platforms, online services, and sites—for billions of users. As a result, chronicles of peoples' actions, desires, interests, and mere intentions are collected by third parties, often without individuals' knowledge or explicit consent, with a scope, breadth, and detail that are arguably without precedent in human history.

Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties. In an effort to leverage the value inherent in personal data, new services (such as search engines and recommender systems), new companies (such as social networking sites and blogging platforms), and even new markets have emerged—such as markets for "crowdsourcing" (Schenk and Guittard 2011), or a complex online advertising ecosystem (Evans 2009). Existing services such as travel

[2] For instance, the act of listening to music online using a streaming service (as opposed to buying a CD in a physical store) can be captured by the streaming service. The streaming service thus can know the songs to which the user listened, from where, for how long, or how many times. This data can be combined with other information about the individual, and then used in various manners: to compile a profile of the listener; to infer his or her other interests and preferences; to present him or her with targeted advertising; or to sell his or her information to data aggregators or other parties.

agencies, record companies, and news media have also been affected and, in some cases, transformed.

The tools and products made possible by the increased availability of personal data have borne benefits for data subjects and data holders alike. Despite those benefits, public concerns over personal privacy have increased. With the advent of Internet and data analytics, issues surrounding the protection or sharing of personal data have emerged as crucial nexuses of economic and policy debate.[3] Over the years, national surveys have consistently found widespread evidence of significant privacy concerns among Internet users.[4] From the standpoint of self-interested individual behavior, the economic motive behind concerns for privacy is far from irrational. It is nearly self-evident. If it is true that information is power, then control over *personal* information can affect the balance of economic power among parties. Thus, privacy can simultaneously be a source of protection from the economic leverage a data holder could otherwise hold over the data subject (if the merchant figures out how little you know about the product you are browsing, he may steer you towards merchandise or prices that serve his interests better than yours); as well as be a tool the data subject may strategically use against the nonholder (if the salesperson cannot estimate your reservation price, you may be able to exploit this information asymmetry to cut a nice bargain).

Privacy is not the opposite of sharing—rather, it is control over sharing. For the individual, therefore, the potential benefits of strategically sharing certain data while protecting other data are quite apparent. So are the potential costs of having too much information disclosed to the wrong parties (from price discrimination to other more odious forms of discrimination; from social stigma to blackmailing; from intangible nuisances to identity theft). Equally apparent, however, are the costs that others may incur when they find themselves in a position of information asymmetry and have less information than the subject. For instance, the security firm that cannot conduct background checks on job applicants may end up hiring the wrong employees. As Posner (1981) points out, privacy is redistributive—as is, of course, the *lack* of privacy.

Beyond mere questions of redistribution, the trade-offs associated with protecting or sharing personal information are nuanced for both the data subject and for the market as a whole (as well as society). First, individuals can directly benefit from sharing their data. Advantages can be both psychological (Tamir and Mitchell 2012) and economic: for instance, personalized services and discounts one receives after joining a merchant's loyalty program; or reduced search costs and increased accuracy of information retrieval one experiences when a search engine tracks them more closely. Those benefits turn into opportunity costs when the individual chooses not to reveal certain personal data.

Second, both positive and negative externalities arise through the complex interplay of data creation and transmission. In particular, the benefits arising from individuals sharing their information, because of advances in data mining, may be enjoyed by society as a whole. For instance, aggregation of online searches may unveil unexpected interactions between pharmaceutical drugs (White et al. 2013), or possibly provide early alerts for epidemics (Dugas et al.

[3] Consider, for instance, the 2013 White House's report on "Big Data: Seizing Opportunities, Preserving Values," available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

[4] For instance, a Pew Research Center survey of 1,002 adult users conducted in 2013 found that 86 percent had taken steps online to remove or mask their digital footprints, and 68 percent believed that current laws were not good enough in protecting online privacy (Rainie et al. 2013).

2012).[5] Conversely, other individuals' comfort with sharing data ("I have nothing to hide") may legitimize expansions of intrusive surveillance programs that affect the rest of society. Society may suffer when certain behaviors stay hidden (consider insider trading or social progress being delayed and social norms failing to evolve because of individuals' fears of disclosing legitimate but fringe opinions); but society may also benefit when other information is suppressed (around the world, various jurisdictions allow certain juvenile criminal records to be expunged with the belief that unfettered reintegration of minors has positive social value). Similarly, an individual may personally benefit from other people's sharing (for instance, collaborative filtering of other users' movie ratings may produce accurate viewing recommendations); conversely, an individual may pay a price when a merchant's analytical tools permit the latter to accurately predict the reservation price of the former, based on the past behavior of other consumers. In fact, even an individual's costs (and ability) to protect her information may be a function of the disclosure choices made by others. That "anonymity loves crowds" is a common refrain in the literature on privacy-enhancing technologies, reflecting the observation that, online as offline, it is easier to hide as one among many who look alike. Conversely, protecting one's data becomes increasingly costly the more others reveal about themselves (for instance, the success of online social networks has encouraged other entities, such as online news sites, to require social media user IDs in order to enjoy some of their services, thus curtailing users who do not want to create social media accounts), or altogether infeasible (even if an individual chooses to protect certain data, that data may still be inferred through the analysis of similar individuals who did not choose to protect theirs; see, e.g., Jernigan and Mistree 2009).

Analyzed as economic goods, privacy and personal information reveal other, peculiar characteristics. First, when shared, personal information can have characteristics of a public good, such as nonrivalry and nonexcludability (a complex online advertising ecosystem engages in trades of Internet users' personal information; in fact, it is hard to prevent released data from being duplicated and accessed by other parties, or to control its secondary uses). And yet, one of the core tenets of informational privacy is the ability to keep that information protected—that is, to exclude someone from knowing or using certain information. The value of keeping some personal information protected and the value of it being known are almost entirely context-dependent and contingent on essentially uncertain combinations of states of the world. Furthermore, privacy sensitivities and attitudes are subjective and idiosyncratic, because what constitutes sensitive information differs across individuals. Specifically, individuals differ in what they may experience if some private information were to be shared with others or made public, as well as in their beliefs that the information may in fact be released. For instance, the healthy individual who just lost his job may flaunt his active lifestyle on social media, but hide his unemployment status to avoid shame; the reverse may be true for the affluent manager who was just diagnosed with a sexually-transmitted disease. Different pieces of information will matter differently to different people (your piano teacher may not be as interested in the schools you attended as your potential employer). The value of information will change over time (an online advertiser may not be as interested in logs of your online activity from five years ago as in your activity right now). In

[5] For a critique of those very claims, however, see Lazer et al. (2014) and section 4.4.

fact, the value and sensitivity of one piece of personal information will change depending on the other pieces of data with which it can be combined (your state of birth and your date of birth, alone, may not uniquely identify you; together, they may allow the prediction of your Social Security number with some accuracy; see, e.g., Acquisti and Gross 2009).

Second, disclosing data often causes a reversal of informational asymmetries: beforehand, the data subject may know something the data holder does not (for instance, a customer's willingness to pay for a good); afterwards, the data subject may not know what the data holder will do with their data, and with what consequences (for instance, how the merchant will use the customer's information, including estimates of her reservation price, following a purchase). As a result, privacy trade-offs are also inherently intertemporal: disclosing data often carries an immediate benefit, be it intangible (friends "liking" your online status updates) or tangible (a merchant offering you a discount). The costs of doing so are often uncertain, and are generally incurred at a more distant point in time (a future prospective employer may not like that risque photo you had uploaded from vacation as much as your friends did at the time; a merchant may collect information about you today, and use it for price discrimination the next time you visit its store).

Third, privacy trade-offs often mix the tangible (the discount I will receive from the merchant; the increase in premium I will pay to the insurer), with the intangible (the psychological discomfort I experience when something very personal is exposed without my consent), and the nearly incommensurable (the effect on society of surveillance; the loss of autonomy we endure when others know so much about us).

Fourth, privacy has elements of both a final good (one valued for its own sake), and an intermediate good (one valued for instrumental purposes; see, e.g., Farrell 2012). Attitudes towards privacy mainly capture subjective preferences; that is, people's valuations of privacy as a good in itself (privacy as a final good). But those valuations are separate from the actual trade-offs that arise following the protection or sharing of personal data (from price discrimination to identity theft; from coupons to personalized services)—that is, from the value of privacy as an intermediate good (for instance, regardless of whether an individual thinks "my life is an open book, I have nothing to hide," that individual will still suffer tangible harm if she is a victim of identity theft).

Fifth, it is not always obvious how to properly value privacy and personal data. Should the reference point be the price one would accept to give away their data, or the amount they would pay to protect it? Or, should it be the expected cost the data subject may suffer if her data is exposed, or the expected profit the data holder can generate from acquiring her personal information? For most products and services that economists traditionally study, the way to address these questions is generally self-evident: the market captures the accurate price of privacy and personal data, reflecting the reservation prices of different buyers (data holders) and sellers (data subjects). However, there is yet no open, recognized market for personal data in which data subjects themselves can participate. Personal data is continuously bought, sold, and traded among firms (from credit-reporting agencies to advertising companies to so-called "infomediaries," which buy, sell, and trade personal data), but consumers themselves do not have access to those markets: they cannot yet efficiently buy back their data, or offer their data for sale (although the concept of personal-information markets for consumers, or individuals' markets for privacy, has been around since the mid-1990s; see, e.g.,

Laudon 1996, and section 2.1 of this survey). Moreover, 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 (Berthold and Böhme 2010). However, individuals do engage daily in transactions involving their personal data. With a query on a search engine, the searcher is implicitly selling information about her current interests in exchange for finding relevant results. By using an online social network, members are implicitly selling information about their interests, demographics, and networks of friends and acquaintances in exchange for a new method of interacting with them. Applying the principle of revealed preference, we could infer people's valuations for their personal data by observing their usage of those tools. However, for service providers, data trading is the essence of the transaction, whereas from the perspective of the data subject, the trade of personal data is a secondary, mostly inconspicuous, and often altogether invisible aspect of a different, more salient transaction (having a question answered, interacting with peers online, and so forth).

1.2 *Focus of the Survey*

Information asymmetries regarding the usage and subsequent consequences of shared information, as well as heuristics studied by behavioral decision researchers, raise questions regarding individuals' abilities, as rational consumers, to optimally navigate privacy trade-offs. They raise questions about the extent to which individual responsibility, market competition, and government regulation can steer the market towards a balance of disclosure and protection of personal data that best serves the interests of the different parties. These observations bring us to even more questions: Are there privacy "equilibria" that benefit both data holders and data subjects? What is the allocation of surplus gained from the usage of individuals' personal data? How should that surplus be allocated—based on market forces, treating privacy as another economic good, or based on regulation, treating privacy as a fundamental right? And should an allocation favor the data subject as the owner of the data, or the data holder who invested in collecting and analyzing the information?

The studies we review in the remainder of this article investigate these diverse issues. The review focuses on the economic value and consequences of privacy and personal information, and on consumers' understanding of and decisions about the costs and benefits associated with data protection and data sharing. In investigating these issues, we focus more on microeconomic than macroeconomic analyses. We focus on scholarly work published in economic journals—although, due to the nature of the subject, we also draw from fields such as psychology, marketing, information systems, and computer science. We begin with a survey of the theoretical literature on privacy (section 2). The survey highlights how the economic analysis of privacy evolved over time, as advancements in information technology raised increasingly nuanced and complex issues associated with the protection and sharing of personal information. A key theme emerging from this literature is that there is no unequivocal impact of privacy protection (or sharing of information) on welfare. Depending on context and conditions, privacy can either increase or decrease individual as well as societal welfare. Next, we survey the empirical literature on privacy trade-offs, as well as what is known about consumers' attitudes and behaviors towards privacy (section 3). The review of the empirical work on privacy reveals various insights. First, it confirms the principal theme arising from the theoretical literature: empirical evidence exists both for scenarios in which

the protection of privacy slows innovation or decreases economic growth and scenarios in which the opposite is the case. A second insight highlights consumers' inability to make informed decisions about their privacy, due to their being often in a position of imperfect information regarding when their data is collected, with what purposes, and with what consequences. A third insight relates to heuristics that can profoundly influence privacy decision making, since privacy trade-offs are intertemporal in nature and often uncertain. Finally, we highlight current issues in the privacy debate that may be of interest to economists (section 4).

Previous scholarship has distinguished different dimensions of privacy such as seclusion, secrecy, solitude, anonymity, autonomy, freedom, and so forth.[6] As noted, this review focuses on informational privacy. Even under such a narrow focus, however, different dimensions and definitions of privacy emerge from the literature, such as privacy as *control over usage* versus privacy as *protection against access* of personal information. Thus, this article covers studies ranging from those that aim to capture individuals' willingness to pay to protect their data, to those that capture the economic consequences of sharing or protecting data. Furthermore, when appropriate, the review touches upon other dimensions of informational privacy, such as the value of anonymity (which is a form of privacy for identity information: it removes the link between a person and data items relating to that person); or the economic dimensions of spam or the do-not-call registry (which relate to intrusions of a person's cyberspace made possible by knowledge of her information); or the burgeoning literature on the economics of information security (which sometimes relates to privacy, for instance in studies of data breaches or identity theft that involve personal data, but more often relates to the protection of information infrastructures and other types of informational assets).

The diversity of privacy definitions and scenarios is reflected in the selection of manuscripts in this review. Figure 1 in the online appendix depicts some of the connections among the different areas of privacy that we survey. The reader should not hope to find a unified theory of privacy, nor a single framework incorporating and connecting the diverse scholarly contributions we review. Privacy means different things to different people, and privacy issues with economic relevance arise in the most diverse contexts: from price discrimination to identity theft; from spam to targeted advertising. What connects these diverse definitions and scenarios is that they all involve the negotiation and management of the boundaries between private and public, and that those boundaries determine tangible and intangible trade-offs. Some of those privacy trade-offs may not just be intangible, but in fact immeasurable. The economics of privacy focuses on measurable, or at least assessable, privacy components. Some (perhaps, many) of the consequences of privacy protection, and its erosion, go beyond the economic dimensions—for instance, the intrinsic value of privacy as a human right, or individuals' innate desires for privacy regardless of the associated economic benefits or lack thereof. Using economics to study privacy does not imply the belief that such other, noneconomic dimensions do not exist or are unimportant. Quite the opposite: we acknowledge those dimensions but do not focus on them. We urge the reader to keep that in mind when considering the broader policy implications of the economics of privacy.

2. *The Economic Theory of Privacy*

In this section, we discuss three waves of research in the economics of privacy: an

[6] For a taxonomy, see Solove (2007).

early wave dating back to the 1970s and early '80s; a middle wave active in the 1990s; and a more recent and growing third wave. For illustrative purposes, several simple and parsimonious algebraic examples appear throughout the discussion. Due to the many diverse scenarios in which issues of informational privacy arise, and their many dimensions, the examples we offer are not meant to represent any particular model or class of models, but rather to illustrate the complexity inherent in privacy trade-offs and in any potential regulation.

2.1 *The First Wave*

While privacy is far from a modern concept (Westin 1967; Schoeman 1984; Ariès 1987),[7] the extraordinary advances in information technology that have occurred since the second half of the twentieth century have brought it to the forefront of public debate. A first wave of economic research consists of seminal works produced between the 1970s and early 1980s by Chicago School scholars such as George Stigler and Richard Posner, and competing arguments by scholars such as Hirshleifer (1971, 1980). By and large, this initial wave of work did not consist of formal economic models, but rather general economic arguments around the value or the damage that individuals, and society, may incur when personal information is protected, making potentially useful information unavailable to the marketplace.

Posner (1978, 1981) argues that the protection of privacy creates inefficiencies in the marketplace, since it conceals potentially relevant information from other economic agents. For instance, if a job seeker misrepresents her background and expertise to a hiring firm, protecting her personal information will negatively affect the firm's hiring decision. Therefore, the protection of the former's privacy comes at the cost of the latter's profitability. Removing an individual's personal information from the marketplace through privacy regulation ultimately transfers the cost of that person's possibly negative traits onto other market participants (see, also, Posner 1993).

Similarly, Stigler (1980) argues that regulatory interference in the market for personal information is destined, at best, to remain ineffective. Because individuals have an interest in publicly disclosing favorable personal information and hiding negative traits, those who decide to protect their personal information (for instance, a debtor who does not want to reveal her credit history) are de facto signaling a negative trait. In this case, regulatory interventions blocking the flow of personal information would be redistributive and inefficient: economic resources and productive factors would end up being used inefficiently, or rewarded unfairly, because information about their quality had been removed from the marketplace.

However, Hirshleifer (1971, 1980) asserts that rational economic agents may end up inefficiently overinvesting in collecting personal information about other parties, and that assumptions of rational behavior underlying the Chicago School's privacy models may fail to capture the complexity inherent in privacy decision making by individuals and organizations. Hirshleifer shows that, given equilibrium prices, the private benefit of information acquisition may outweigh its social benefit (for more recent examples, see Hermalin and Katz 2006; Burke, Taylor, and Wagman 2012; Wagman 2014). In a pure exchange setting, information may have no social value at all, because it results only in a redistribution of wealth from ignorant to informed agents.

While not temporally belonging to the first wave of privacy literature, Murphy

[7] Evidence of both a need and a desire for privacy, and a need and a desire for socializing and disclosing, can be found throughout history and across diverse societies; see, e.g., Acquisti, Brandimarte, and Loewenstein (2015).

(1995) and Daughety and Reinganum (2010) provide rebuttals to the Chicago School view. In particular, Daughety and Reinganum construct a model in which each individual cares about his reputation, but an individual's actions generate externalities (public good or bad). Under a regime of publicity, individuals distort their actions to enhance or preserve their reputations, whereas under privacy, they choose their individually optimal level of the activity. Thus, for example, both private and public welfare can be increased when information about an individual checking into a drug or alcohol rehab center remains private; otherwise, the stigma associated with doing so could deter him from seeking treatment. Similarly, if a physician were not bound by confidentiality, a patient may not feel comfortable sharing all the relevant details of her condition. On the other hand, when charitable contributions are public, amounts donated may increase, because contributing raises the reputation of the donor.

In a similar vein, but even more fundamentally, Spence (1973) can be viewed through a lens of privacy regulation. From this perspective, signaling activity may—as the Chicago scholars suggest—reveal payoff-relevant private information, but the aggregate cost of the signaling activity may nevertheless outweigh the benefits. Indeed, as is well-known, there are situations in which banning signaling behavior altogether (that is, enforcing a regime of complete privacy) may result in a Pareto improvement. This is illustrated in the following example inspired by Gottlieb and Smetters (2011), who report that nine of the fifteen most selective MBA programs in the United States do not disclose student grades to prospective employers.[8]

Example 1 (Signaling and Privacy): Suppose that an MBA student of privately known ability $\theta \in [0, 1]$ can earn grades of $g \geq 0$ by incurring effort cost g/θ. Upon graduating, her productivity on the job will be θ. Firms make competitive wage offers to each graduate. In particular, if the business school publicly reports its grades, then firm i makes an offer $w_i(g)$ to a graduate with grades g. On the other hand, if the business school keeps grades private, then firm i must make the same offer $\overline{w}_i$ to all graduates. The utility of a type θ student is given by

$$U(w, g; \theta) = w - \frac{g}{\theta}.$$

It is straightforward to verify that if grades are public, then in the unique outcome of a *least-cost separating equilibrium*, a student of ability θ will earn grades of $g^*(\theta) = \theta^2/2$ and receive a wage offer $w^*(g^*(\theta)) = \theta$. Her equilibrium payoff, therefore, will be $U^*(\theta) = \theta/2$. On the other hand, if the business school keeps grades private, then each student will earn a wage $\overline{w} = E[\theta]$ and will "waste" no effort on grade seeking. Thus, privacy of grades is a Pareto optimal policy if and only if $U^*(1) \leq E[\theta]$ or $E[\theta] \geq 1/2$.

2.2 *The Second Wave*

By and large, economists did not again exhibit particular interest in the economics of privacy for over a decade following the first wave of research. This changed in the mid-1990s, arguably because of progress in digital information technologies on multiple fronts (the proliferation of electronic databases and personal computers, the advent of the Internet, the diffusion of electronic mail), which led to a new set of economic issues involving the usage of personal data. This second wave is similar to the

[8] See, also, the US Family Educational Rights and Privacy Act (FERPA), in connection to the privacy of student education records, http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html, as well as the US Equal Employment Opportunity Commission (EEOC), which governs the federal legalities of information flows in hiring practices, http://www.eeoc.gov/laws/practices/.

first in terms of a preference for articulating economic arguments, rather than formal models. However, it is differentiated from the first wave not just temporally, but also in terms of the specificity of the privacy scenarios considered, and the emergent awareness of the role of digital information technologies. Works produced in this wave began focusing on issues such as the role of cryptographic technologies in affecting economic trade-offs of data holders and data subjects, or the establishment of markets for personal data, as well as the economic implications of the secondary uses of personal information.

In particular, Varian (1997) observes that the development of low-cost technologies for data manipulation generates new concerns for personal information processing. Varian nonetheless recognizes that consumers may suffer privacy costs when too *little* personal information about them is being shared with third parties, rather than too much. The consumer, he notes, may rationally want certain information about herself known to other parties (for instance, a consumer may want her vacation preferences to be known by telemarketers in order to receive offers and deals from them that may actually interest her). The same consumer, however, may rationally not want *too much* information to be known by others—for instance, information about her willingness to pay for the deals in which she is interested. The line of reasoning in Varian (1997) echoes Stigler's and Posner's approaches, but adds to it novel concerns associated with the secondary usage of personal data. A consumer may rationally decide to share personal information with a firm because she expects to receive a net benefit from that transaction; however, she has little knowledge or control over how and by whom that data will later be used. The firm may sell the consumer's data to third parties, which may lead to spam and adverse price discrimination, among other concerns (Odlyzko 2003). Such negative externalities may not be internalized by the consumer nor by the firm that distributes the information (Swire and Litan 1998).

Whereas Varian points out a possible individual cost from data protection (e.g., receiving irrelevant rather than relevant offers), a possible *social* cost of privacy is highlighted by Friedman and Resnick (2001). Friedman and Resnick focus on the availability of easy "identity changes" (for instance, cheap pseudonyms). Using a repeated prisoner's dilemma game, they show that distrust of newcomers is an inherent social cost of cheap pseudonyms—privacy of identity *can* be a barrier to trust building. However, it does not *need* to be: the authors also show that there are intermediate forms of identity protection that minimize those social costs, thereby providing both some degree of privacy and some degree of accountability.

Who, then, should hold an economic claim over personal data? The subject to whom the data refers or the organization that invested resources in collecting the data? In accordance with the Coase theorem (Coase 1960), Noam (1997) argues that whether or not a consumer's data will remain protected does not depend on the initial allocation of rights on personal information protection—that is, it does not depend on the presence or lack of a privacy regulatory regime. Instead, whether data will eventually be disclosed or protected ultimately depends on the relative valuations of the parties interested in the information. What the presence or lack of a regulatory regime *will* affect, however, is which party—the data subjects, or the data holders—will pay the other for access to, or protection of, personal data. In other words, the allocation of privacy rights may still have allocative and distributional consequences, differentially affecting the surplus of various parties, even when it may not have an effect on aggregate welfare. Coasian arguments in the analysis of privacy are also proposed by Kahn, McAndrews, and Roberds (2000), but

they depend on consumers being aware of, and internalizing, the costs and benefits of trading their private information.[9]

Laudon (1997) proposes the creation of information markets where individuals own their personal data and can transfer the rights to that data to others in exchange for some type of compensation. Similarly to the view proposed by Chicago School scholars, Laudon argues that the mere legal protection of privacy is outdated, and a system based on property rights over personal information would better satisfy the interests of both consumers and firms.[10] Clearly, however, a system of property rights over personal information would require appropriate legislation to define and assign those rights. This observation reveals that market-based and regulatory approaches to privacy are not binary opposites, but rather points on a spectrum. At one end of the spectrum, one would find regimes where no privacy legislation exists. Under those regimes, the protection of data relies entirely on consumers' marketplace behavior (for instance, strategies such as avoiding interactions with firms that do not provide adequate protection of one's data, or adopting privacy-enhancing technologies to prevent the leakage of personal data), and on firms' self-regulated, competition-driven data-handling policies. On the opposite end of the spectrum, privacy regulation would establish strict default protection of personal data and limitations over its usage. Somewhere in between, legislative initiatives may create a framework for property rights over personal data and for means to trade those rights across data subjects and potential data holders. While the assignment of property rights is generally welfare enhancing, granting consumers the right to sell their personal data may actually undermine consumer surplus, as illustrated in the following example.

Example 2 (A Market for Consumer Information): Consider a market for a certain good, composed of a measure 1 of massless consumers. The consumers' valuations for the good are uniformly distributed on [0, 1]. The market is served by a monopolist with production cost normalized to zero. Absent a market for information, the monopolist would set its price at $p^M = \frac{1}{2}$; it would earn profit of $\frac{1}{4}$; and the top half of the market would earn aggregate consumer surplus of $\frac{1}{8}$.

Now suppose that each consumer possesses verifiable information (e.g., place of residence or employment) that correlates perfectly with her valuation for the good. The monopolist first makes an offer to pay $r \geq 0$ to any consumer who reveals her information. It then uses the information thus obtained to make personalized price offers $\hat{p}(v)$ to those consumers who sold their information and it posts a common price p to all those who did not.

It is straightforward to verify that in the unique perfect Bayesian equilibrium of this game the following must hold. The monopolist offers $r = 0$ for information. Nevertheless, *all* consumers reveal their valuations, and the monopolist sets $\hat{p}(v) = v$ and $p = 1$. The intuition here is similar to that in Grossman (1981) and Milgrom (1981). The marginal anonymous consumer makes no surplus and, therefore, is always willing to reveal her valuation for an arbitrarily small payment, but this means that there can be no marginal anonymous consumer in equilibrium. That is, the set of anonymous consumers unravels from the bottom.

[9] Incomplete information and information asymmetries (for instance, a consumer not being even aware that her data is being collected) can limit the applicability of the Coase theorem to the analysis of privacy. For an analysis of the scope of the Coase theorem in the presence of private information, see Farrell (1987).

[10] For related work on property rights over personal information, see Litman (2000), Samuelson (2000), and Schwartz (2004).

This situation raises social surplus by $\frac{1}{8}$ and is allocatively efficient—the monopolist extracts all the social surplus of $\frac{1}{2}$. However, consumers are worse off: the unregulated market for information reduces consumer surplus from $\frac{1}{8}$ to 0, despite the fact that consumers initially owned property rights to their information.

2.3 *The Third Wave*

Following the commercial success of the Internet and the proliferation of databases containing consumer information, research on the economics of privacy dramatically increased at the start of the twenty-first century. Because so many transactions and activities, once private, are now conducted online, firms, governments, data aggregators, and other interested parties can observe, record, structure, and analyze data about consumer behavior at unprecedented levels of detail and computational speed (Varian 2010). As a result, the digital economy is, to a degree, financed by the organization of large amounts of unstructured data to facilitate the targeting of product offerings by firms to individual consumers. For instance, search engines rely on data from repeat and past searches to improve search results, sellers rely on past purchases and browsing activities to make product recommendations, and social networks rely on giving marketers access to their vast user bases in order to generate revenues. This third wave, while temporally close to the second, is differentiated by the fact that studies are rooted in more formal economic models and in empirical analyses, including lab experiments (we consider empirical analyses separately in section 3). In addition, this third wave is more directly linked to the novel economic issues brought forth by developments in information technology, including search engines, behavioral targeting, and social media. Thus, this third wave is more fragmented than the previous two in terms of the focus of analysis.

While much of the third wave is focused on issues surrounding privacy as the protection of information about a consumer's preferences or type (hence a significant number of models examine the relationships between privacy and dynamic pricing), different dimensions to privacy (and different dimensions of informational privacy) exist, and economic trade-offs can arise from different angles of the same privacy scenarios. Consequently, other streams of work we consider in this section include the rise of spam, the development of markets for privacy (Rust, Kannan, and Peng 2002), behavioral targeting, the economic analysis of (personal) information security, and the relationship between public goods, social recognition, and privacy.

2.3.1 *Privacy, Consumer Identification, and Price Discrimination*

Intended as the analysis of the relationships between personal data and dynamic pricing, the economics of privacy is closely connected to the vast stream of studies on intertemporal price discrimination based on consumer recognition. This literature solidifies the notion of consumer tracking and personalized pricing, but does not explicitly consider privacy issues in online environments. Chen (1997) studies discriminatory pricing when different consumers buy different brands, and Fudenberg and Tirole (1998) explore what happens when the ability to identify consumers varies across goods—they consider a model in which consumers may be anonymous or "semi-anonymous," depending on the good purchased. Villas-Boas (1999) and Fudenberg and Tirole (2000) analyze a duopoly model in which consumers have a choice between remaining loyal to a firm and defecting to a competitor, a phenomenon they refer to as "consumer poaching" (Asplund et al. 2008 demonstrate evidence

of this sort of poaching in the Swedish newspaper industry). They show that a firm always has an incentive to offer discounts to a rival firm's customers who have revealed, through their prior purchases, their preferences for the rival firm's product. Such discounts initially tend to reduce consumer price sensitivity for a firm's product, as consumers rationally anticipate them; hence prices rise in later periods, thanks to anticipated customer poaching. Chen and Zhang (2009) study a "price for information" strategy, where firms price less aggressively in order to learn more about their customers. Jeong and Maruyama (2009) and Jing (2011) identify conditions under which a firm should discriminate against its first-time and repeat customers.

More specific to privacy, Taylor (2004) finds that, in the presence of tracking technologies that allow merchants to infer consumers' preferences and engage in price discrimination, the usefulness of privacy regulatory protection depends on consumers' level of sophistication. Naïve consumers do not anticipate a seller's ability to use any and every detail about their past interactions for price discrimination; consequently, in equilibrium, their surplus is captured by firms—unless privacy protection is enforced through regulation. Regulation, however, is not necessary *if* consumers are aware of how merchants may use their data and buyers can adapt their purchasing decisions accordingly, because it is in a company's best interest to protect customers' data (even if there is no specific regulation that forces it to do so). This is an example of how consumers, with their choices, could make a company's privacy-intrusive strategies counterproductive (section 3 includes references to studies that highlight consumers' awareness and knowledge of tracking technologies and privacy trade-offs).

Similar conclusions are reached by Acquisti and Varian (2005), who study a two-period model in which merchants have access to "tracking" technologies and consumers have access to "anonymizing" technologies. Internet commerce offers an example: merchants can use cookies[11] to track consumer behavior (in particular, past purchases and browsing activities), and consumers can delete cookies, use anonymous browsing or payment tools, and so forth, to hide that behavior. Acquisti and Varian (2005) demonstrate that consumer tracking will raise a merchant's profits only if the tracking is also used to provide consumers with enhanced personalized services.

Complementary to the above works, Villas-Boas (2004) shows how strategic consumers may make a firm worse off in the context of dynamic targeted pricing. The reason is that once consumers anticipate future prices, they may choose to skip a purchase today to avoid being identified as a past customer tomorrow—and thus have access to lower prices targeted at new consumers. This strategic "waiting" on the part of consumers can hurt a firm both through reducing sales and diminishing the benefit of price discrimination, and may push a firm to voluntarily adopt a privacy-friendly policy.

Calzolari and Pavan (2006) consider the exchange of information regarding customers between two companies that are interested in discovering consumers' willingness to pay. They find that the transmission of personal data from one company to another may in some cases reduce information distortions and enhance social welfare (see also Pavan and Calzolari 2009; Kim and Choi 2010; Kim and Wagman 2015). Information disclosure is therefore not always harmful to the individual and may contribute to improving the welfare of all parties involved. Moreover, in

[11] Cookies refer to files that are stored on a user's device, which can be subsequently used to help recognize the user across different web pages, websites, and browsing sessions.

line with Taylor (2004), companies may be inclined to develop their own privacy protection policies for profit-maximizing purposes, even without the intervention of a regulatory body. Conitzer, Taylor, and Wagman (2012) confirm these findings in a model where strategic consumers can opt to remain anonymous towards sellers at some cost—a cost modeled as the monetary-equivalent burden of maintaining privacy. The authors show that consumer surplus and social welfare are nonmonotonic in this cost, reaching their highest levels at an intermediate level of privacy.

Other studies take intrinsic privacy concerns as given (with the source not necessarily modeled), and then analyze how these concerns affect equilibrium behavior: Gradwohl (2014) does so in the context of decision making in committees; Dziuda and Gradwohl (2015) in the context of interfirm communication to achieve cooperation; and Gradwohl and Smorodinsky (2014) examine some of the effects of privacy concerns on pooling behavior, misrepresentation of information, and inefficiency.

The sharing or protection of consumer data can also influence market competition. Campbell, Goldfarb, and Tucker (2015) demonstrate that, if privacy regulation only relied on enforcing opt-in consent, an unintended consequence may be the entrenching of monopolies. The authors show that consumers are more likely to grant their opt-in consent to large networks with a broad scope, rather than to less established firms. Hence, if regulation focuses only on enforcing an opt-in approach, users may be less likely to try out services from less established firms and entrants, potentially creating barriers to entry by leading to a "natural monopoly" in which scale economics include privacy protection. Kim, Wagman, and Wickelgren (2016) examine the effect of first-degree price discrimination on the welfare consequences of horizontal mergers. In their model, when there are three or more firms in the market and two of them merge, the postmerger loss in consumer surplus is substantially lower when firms first-degree price discriminate, compared to when they cannot. In contrast, this reduction is absent in a two-to-one merger, leading to substantial anticompetitive effects of the merger. Thus, their study illustrates that the merger effects of access to consumer data depend on market structure.

Armstrong and Zhou (2010) study a duopoly search model where consumers may choose not to purchase a product on their first visit—and sellers record this behavior. They show that, in equilibrium, firms set higher prices for returning consumers, whereby first-time visitors would pay discounted rates, and that such practices may lead consumers not to return. These types of pricing strategies can result in consumer backlash—akin to what took place with Amazon in 2001 (Anderson and Simester 2010), which may lead firms to commit upfront not to engage in such practices. Indeed, one theme resonating throughout this line of research is that firms with market power often benefit from committing to privacy policies. This is illustrated in the following simple example.

Example 3 (Repeat Purchases and Customer Tracking): Suppose a population of n individuals wishes to consume one unit of a good in each of two periods. Half of the individuals are high-valuation consumers who value the good at 1 in both periods and the other half are low-valuation consumers who value it at $\lambda \in \left(0, \frac{1}{2}\right)$ in both periods. Each consumer's valuation is privately known. The good is sold by a monopolist with production cost normalized to 0. The consumers and the firm are risk neutral and (for simplicity) do not discount the future. Also, it is common knowledge that the monopolist possesses a tracking technology (for instance, cookies or browser fingerprints) with which it can recall

whether a consumer purchased the good in the first period and what price he paid for it. Moreover, the monopolist may use this information to make personalized price offers to consumers in the second period.

It can be shown (see, e.g., Taylor 2004; Acquisti and Varian 2005) that on the path of play in any perfect Bayesian equilibrium of this game the following must hold: The monopolist makes first-period price offers $p_1 = 1$ to all consumers and second period offers $p_2 = 1$ to all consumers regardless of their purchase histories. A low-valuation consumer never purchases the good. A high-valuation consumer purchases with probability 1 in the second period but purchases with probability $\frac{1 - 2\lambda}{1 - \lambda} < 1$ in the first period (leaving the monopolist just indifferent between $p_2 = 1$ and $p_2 = \lambda$ following a first-period rejection).

If the monopolist could publicly commit not to use the tracking technology, then the price offers would be the same, $p_1 = p_2 = 1$, but high-valuation consumers would accept with probability 1 in the first period because rejections could never induce lower second-period prices. Thus, the tracking technology leads to strategic first-period rejections by high-valuation consumers, a Pareto inferior outcome that reduces welfare (in the form of monopoly profit) by $\frac{n\lambda}{1 - \lambda}$.

2.3.2 *Data Intermediaries*

A number of works have incorporated questions regarding privacy into the study of two-sided markets. Such studies can help us understand the role of large data holders—companies such as Google, Facebook, and Amazon—which in part act as intermediaries, selling advertising space to advertisers on one end and providing services and products to users on the other.

De Cornière (forthcoming) shows that when consumers actively search for products, targeting leads to more intense competition. In a framework in which consumers search sequentially after having entered a query on a search engine, he shows that targeting reduces search costs, improves matches between consumers and firms, and intensifies price competition. However, a profit-maximizing search engine may choose to charge too high an advertising fee, which can negate the benefits of targeting. Hence, the optimal level of accuracy in terms of advertising matching solves a trade-off between consumer participation and the profit of the intermediary.

Hagiu and Jullien (2011) study how intermediaries can use information about consumer characteristics in order to affect matching between firms and consumers. They show that if an intermediary receives a fee each time a consumer visits an affiliated firm, the intermediary has an incentive to direct consumers towards firms that they would not have visited otherwise. Doing so, the intermediary manipulates the elasticity of the demands faced by its affiliated firms. Bergemann and Bonatti (2015) study the acquisition of user-pertinent information by an advertising platform and its subsequent sale to advertisers. In their model, a data provider sets the price of an information record (e.g., a cookie). Advertisers subsequently acquire information records from the data provider, form posterior beliefs about consumer types, and purchase advertising space. The authors demonstrate situations where improved precision of user information leads to fewer records being purchased. Consequently, a data provider may choose to restrict or cap advertisers' access to information about users (that is, constrain or reduce its precision) in order to sell more records and generate greater profits.

Gehrig and Stenbacka (2007) examine lenders in a repeated-interaction framework and consider the possibility of information sharing among lenders (for instance, via credit bureaus). The authors demonstrate that in the presence of information sharing,

switching costs are essentially reduced, which relaxes competition for initial market shares and can end up reducing the welfare of borrowers. In other instances, firms may be reluctant to use first- or third-degree price discrimination, for fear of a public backlash. De Cornière and Nijs (2014) rule out direct price discrimination based on consumers' personal information by focusing instead on firms' bidding strategies in auctions for more precise targeting of their advertisements. That is, given that consumers' private information provides a finer and finer segmentation of the population, firms can compete to advertise their nondiscriminatory pricing over each of those consumer segments. By disclosing information about consumers, the platform ensures that consumers will see the most relevant advertisements, whereas when no information is disclosed under a complete privacy regime, ads are displayed randomly. They find that targeted advertising can lead to *higher* prices and, in line with Levin and Milgrom (2010) and Bergemann and Bonatti (2015), that improving match quality by disclosing consumer information to firms might be too costly to an intermediary because of the informational rent that is passed on to firms. Given a relationship between the match quality of advertising and consumer demand, it is then possible to specify conditions under which *some* privacy or some limits to disclosure are optimal for an intermediary (see, also, Cowan 2007).

In a related analysis, Board and Lu (2015) study the interaction between buyers, who search across multiple websites to learn which product best fits their preferences, and merchants, who manage disclosure policies regarding their products (such as advertisements, product trials, or reviews). In particular, the authors study how market outcomes vary as a function of the amount of consumer information accessible by the sellers. When consumers are anonymous and sellers cannot track their searches, there exists an equilibrium in which sellers disclose all of their product information in the limit as search costs vanish. However, when sellers are able to observe buyers (for instance, through tracking their online behavior) and can infer their beliefs, there is often a unique equilibrium, akin to the Diamond paradox (Diamond 1971). In this equilibrium, every seller adopts a monopoly disclosure policy that manipulates consumers to purchase the most profitable products, rather than the ones most suited to their needs. In other words, the ability to track buyers makes it possible for sellers to implicitly collude, a result that is similar in spirit to the relationship between privacy and market competition discussed in section 2.3.1.

Zhang (2011) also follows an approach that does not require the direct use of an intermediary and yields similar findings. She studies competitive markets with endogenous product design and demonstrates that in an effort to avoid more aggressive pricing from competitors, market leaders may choose to introduce mainstream products that appeal to the broader segment of the population. By doing so, rather than pursuing an approach of product differentiation, firms can limit consumers' strategic release of preference information—similar to what an intermediary would do—in order to dampen competition and facilitate product entry (see, also, Wickelgren 2015).

Another approach to limit the release of information by consumers is explored in the study of intermediary gatekeepers (Baye and Morgan 2001; Wathieu 2002; Pancras and Sudhir 2007)—a third party that provides consumers with access to some degree of anonymity, possibly at a cost. Consistent with the above works, Conitzer, Taylor, and Wagman (2012) show that it can be profit maximizing for both firms and a gatekeeper

to reach agreements for granting users the ability to freely anonymize.[12] At the same time, Taylor and Wagman (2014) demonstrate that the effects of firms' ability to target individual consumers on consumer surplus, profits, and overall welfare is context dependent, whereby any conclusions drawn from a given model must be understood within its specific market setting.

A common lesson arising from this literature is that firms—be they advertisers or data intermediaries—seldom possess socially optimal incentives to match consumers with products. This is illustrated with the following example suggested to us by Alessandro Bonatti.

Example 4 (Buying and Selling Consumer-Level Information): An advertiser faces a continuum of heterogeneous consumers and a monopolist data provider. The match value v_i between consumer i and the advertiser's product is uniformly distributed on $V = [0, 1]$. The advertising technology is summarized by the *matching function* $m(x) = \frac{cx^2}{2}$ that represents the expenditure by the advertiser required to generate a contact of intensity x. The complete-information profits from generating a contact of intensity x with a consumer of value v are $\pi(v, x) = vx - \frac{cx^2}{2}$.

A data provider knows the match value v_i of each consumer i, and sells this data to the advertiser at a constant price per individual p. Hence, if the advertiser acquires information about consumer i, it is able to tailor its choice of contact intensity to the match value, i.e., $x^*(v_i) = v_i/c$, and obtain profits of $\pi^*(v_i) = \frac{v_i^2}{2c}$. In contrast, the advertiser must choose a constant intensity level $\bar{x}$ for all other consumers. Because the constant intensity level $\bar{x}$ depends on the composition of the *residual set* of consumers, the advertiser's information-acquisition problem can be formulated as the choice of a *targeted set* of consumers $A \subset V$.

The demand for information about specific consumers can be traced back to two sources of *mismatch risk*: excessive versus insufficient advertising. Specifically, the profit-maximizing *residual* set for the advertiser in this case is a nonempty interval, $A^C = \left[\frac{1}{2} - 2\sqrt{cp}, \frac{1}{2} + 2\sqrt{cp}\right]$. In other words, the advertiser purchases information about both very high- and very low-value consumers. Note that $E\left[v_i | v_i \in A^C\right] = \frac{1}{2}$, which implies $\bar{x} = \frac{1}{2c}$. This is *too much* advertising for the consumers in the bottom half of the residual set and *too little* advertising for the consumers in the top half.

Finally, if the data provider incurs no *marginal* cost of supplying information, then it chooses p to maximize $p(1 - 4\sqrt{cp})$; i.e., it sets $p^* = \frac{1}{36c}$. The advertiser thus purchases data only on the bottom and top sixths of the market, treating all other consumers as if they had match value $\frac{1}{2}$.

2.3.3 *Marketing Techniques*

Some studies expand the analysis of privacy to include the costs of intrusions into an individual's personal sphere, such as unsolicited mail or spamming, as in Hann et al. (2008),

[12] Kearns et al. (2014) study the design of mechanisms that satisfy the computer science criterion of differential privacy (Dwork 2006)—put simply, the notion of being able to distinguish one agent (a consumer) from another in a dataset of consumer characteristics with only a low probability. They show that mechanisms can be designed to satisfy a variant of this criterion when there are large numbers of agents, and any agent's action affects another agent's payoff by at most a small amount. Other related mechanism-design issues have been studied. One issue is limiting "exposure," where agents internalize being exposed to the realized types and chosen actions of a subset of other agents (Gradwohl and Reingold 2010) or to the party responsible for implementing the mechanism (Gradwohl 2015). Another issue is "anonymity," where agents may seek to participate in a mechanism multiple times when anonymizing is too easy (Wagman and Conitzer 2014).

and personal preferences over privacy, as in Tang, Hu, and Smith (2008). Here, the theoretical study of privacy connects with the marketing literature on couponing, market segmentation, and consumer addressability (Blattberg and Deighton 1991). Works by Shaffer and Zhang (1995, 2002), Chen, Narasimhan, and Zhang (2001), Chen and Iyer (2002), Conitzer, Taylor, and Wagman (2012), and Shy and Stenbacka (forthcoming) obtain complementary results. These authors show that when a firm has control over consumers' privacy, it chooses to segment the population optimally for pricing purposes. Their findings demonstrate that price discrimination can lead to intensified price competition, where firms may possess incentives to (1) decrease the level of accuracy of targeted promotions, (2) differentially invest in customer addressability, and (3) seek commitment mechanisms not to price discriminate.

Hann et al. (2008) study a competitive market with heterogeneous consumers, some who draw no benefit from unsolicited marketing and some who are interested in receiving information about new products. They show that attempts to use technologies that prevent unsolicited marketing on one side, and sellers' efforts to use direct marketing on the other, constitute strategic complements: the higher the attempts of consumers to protect themselves from unsolicited marketing, the higher the use of direct marketing by sellers. Similarly, Hui and Png (2006) consider the use of private information for unsolicited marketing—in person, via telephone, mail, or email—which competes with the marketing efforts of other companies and may inconvenience individuals. In related work, Chellappa and Shivendu (2010) examine the trade-offs vendors and consumers face between privacy concerns and the personalization of services and products that the sharing of data may make possible.

Anderson and de Palma (2012) look at spamming as a problem of competition among senders of messages for the receivers' attention, which is a limited resource. Their model considers the costs that both parties have to incur in order to arrive at a transaction. These costs endogenously determine the number of messages sent by the sender and the number of messages read by receivers. If the cost of sending messages is too low, there will be a congestion problem, meaning that receivers will only read some of the messages sent (see, also, Van Alstyne 2007). In this case, a welfare-enhancing solution may be to add a small tax on the transmission of a message. Such a tax may increase surplus, because senders who send messages of low quality will be crowded out (it would be too costly for them to send a message), fewer messages will be sent, and more will be read. Spiegel (2013) identifies conditions under which firms may choose to bundle new software with advertisements and distribute it for free as adware. While adware is more affordable to consumers and may contain advertisements that help improve their purchasing decisions, it also entails a loss of privacy.

Linking the above works to the study of privacy, Van Zandt (2004), Armstrong, Vickers, and Zhou (2009), Anderson and de Palma (2012), and Johnson (2013) also investigate the topic of congestion due to consumers having limited attention. In their models, consumers can choose to "opt out" from receiving sellers' marketing. The result is a form of a prisoner's dilemma situation: while each consumer has a private incentive to opt out of intrusive marketing, when all consumers do this, price competition is relaxed and consumers are harmed. Targeted ads, however, can also be counterproductive, if they trigger the recipient's privacy concerns or her worries regarding the level of control over her private information (Tucker 2014). In this sense, targeted advertising is a form of unsolicited marketing. While spamming involves the indiscriminate sending

of advertisements, targeted advertising (or behavioral targeting), as the name suggests, consists of contacting a select group of recipients who, according to the information available to the sender about their previous behaviors or preferences, may be particularly interested in the advertised product or service.

Hoffmann, Inderest, and Ottaviani (2014) study targeted communications, a practice they refer to as hypertargeting, in the context of marketing and political campaigns. In a departure from the earlier literature on strategic disclosures (Grossman and Shapiro 1984; Milgrom 1981; Milgrom and Roberts 1986), they assume that firms must be selective when choosing the amount of information they communicate to consumers (e.g., due to space or time constraints). Since consumers differ in their preferences, firms may wish to market different product attributes to different consumers. They model hypertargeting as the selective disclosure of information to a specific audience, and characterize the private incentives and welfare impact of hypertargeting. They demonstrate that a privacy policy that hinders hypertargeting by, for instance, banning the collection of personally identifiable data, is beneficial when consumers are naïve, competition is limited, and firms are able to segment the market to price discriminate. Otherwise, privacy regulation may backfire, because a policy that, for instance, requires consumer consent, can allow firms to commit to abstain from selective targeting—even when doing so would benefit consumers.

The following example demonstrates that the common wisdom that imposing a tax on messages will fall more heavily on spammers, and thereby improve the average quality of contacts, need not necessarily be true.

Example 5 (Marketing and Spam): Suppose there are two firms, a spammer (firm 0) and a retailer (firm 1). There is a consumer who has time to open exactly one email message. If she opens a message from the retail firm she receives a payoff of $v > 0$ and the retailer receives gross profit of b_1. If she opens a message from the spammer, she receives expected payoff $-k < 0$ (a small fraction of consumers may receive a positive payoff from opening spam, but the majority receive a negative payoff) and the spammer receives $b_0 \in (0, b_1)$. Also assume $b_1 v > b_0 k$. The expected profit to firm i from sending the consumer m_i messages when its rival sends her m_j is

$$\Pi_i = \frac{m_i}{m_i + m_j} b_i - c m_i, \quad i \in \{0, 1\}, i \neq j,$$

where c is the marginal cost of sending a message. The expected payoff to the consumer from opening a single message at random is

$$U = \frac{m_1 v - m_0 k}{m_1 + m_0}.$$

It is straightforward to verify that in the unique perfect Bayesian equilibrium of this game the following must hold: firm i sends

$$m_i^* = \frac{b_j b_i^2}{c(b_1 + b_0)^2}$$

messages and receives expected profit

$$\Pi_i^* = \frac{b_i^3}{(b_1 + b_0)^2},$$

and the consumer receives expected payoff

$$U^* = \frac{b_1 v - b_0 k}{b_1 + b_0}.$$

Observe that charging the firms a tax of t per message (resulting in a marginal cost of $c + t$) reduces the number of messages sent by each firm, but has no impact on equilibrium payoffs. The firms would respond to a tax by sending proportionally

fewer messages, reducing the absolute number received by the consumer, but not their composition. In contrast, a filter that correctly identifies a fraction ϕ of the messages sent by firm 0 as spam both reduces the number of messages sent by each firm in equilibrium and raises the consumer's expected payoff to

$$U^{**} = \frac{b_1 v - (1-\phi) b_0 k}{b_1 + (1-\phi) b_0}.$$

3. *The Empirical Analysis of Privacy*

If our perusal of the theoretical economic literature on privacy has revealed one robust lesson, it is that the economic consequences of less privacy and more information sharing for the parties involved (the data subject and the actual or potential data holder) can in some cases be welfare enhancing, while, in others, welfare diminishing. The various streams of research we covered highlighted that, in choosing the balance between sharing or hiding personal information (and in choosing the balance between exploiting or protecting individuals' data), both individuals and organizations face complex, often ambiguous, and sometimes intangible trade-offs. Individuals can benefit from protecting the security of their data to avoid the misuse of information they share with other entities. However, they also benefit from the sharing of information with peers and third parties that results in mutually satisfactory interactions. Organizations can increase their revenues by knowing more about the parties they interact with, tracking them across transactions. Yet, they can also bear costs by alienating those parties with policies that may be deemed too invasive. Intermediaries can increase their revenues by collecting more information about users, yet offering overly precise information to advertisers can backfire by reducing competition among sellers.

Those nuanced trade-offs are reflected in the literature we examine in this section. We survey the empirical literature on the economics of privacy to highlight some of the costs and benefits of privacy protection and information sharing. The market for personal data and the market for privacy are two sides of the same coin, wherein protected data may carry benefits and costs that mirror or are dual to the costs and benefits associated with disclosed data for both data subjects and data holders. For instance, *disclosed* personal information (or lack of data protection) can result in economic benefits for both data holders (savings, efficiency gains, surplus extraction, increased revenues through consumer tracking) and data subjects (personalization, targeted offers and promotions, etc.). At the same time, such disclosures (or, the lack of protection of personal data) can be costly for both firms (costs incurred when data is breached or misused, or collected in ways that consumers deem too intrusive) and consumers (from tangible costs such as identity theft or (price) discrimination, to less tangible ones such as stigma or psychological discomfort; see, e.g., Stone and Stone 1990; Feri, Giannetti, and Jentzsch 2016). Furthermore, the *act* of collecting data can be costly for data holders (such as the investments necessary to establish customer relationship management systems).

Similarly, protected data (or, lack of data disclosure) can be associated with both benefits and costs for data subjects and potential data holders; such benefits and costs are often dual (that is, the inverse) of the benefits and costs highlighted above. For instance, data subjects and data holders may incur opportunity costs when useful data is not disclosed (for instance, they may miss out on opportunities for increased efficiency or increased convenience), although both parties may also benefit in various ways (consumers, for example, by reducing the expected costs associated with identity theft; firms, for example,

by exploiting privacy-friendly stances for competitive advantage). Furthermore, there are costs associated with the *act* of protecting data (investments necessary to encrypt data for the data holders to prevent *further* disclosures, costs of using privacy-enhancing technologies for the data subject, etc.).

In short, there can be many dimensions to privacy harms (Calo 2011) and to the benefits arising from personal information. The rest of this section does not attempt to provide a comprehensive enumeration of those dimensions, but surveys the areas that have attracted more empirical economic analysis.

3.1 *Privacy, Advertising, and Electronic Commerce*

Online advertising is perhaps the most common example of how firms use the large amounts of data that they collect about users. The greater availability of personally identifiable data on the Internet in terms of scope, quantity, and the precision with which firms can target specific users challenges the traditional distinction between personal selling and remote communication. As a result, the way advertising is targeted affects marketing strategies and competition between online and offline media (see, for instance, Athey and Gans 2010; Bergemann and Bonatti 2011; and Athey, Calvano, and Gans 2013). Already in 2008, fifty-six of the top one hundred websites (based on page views), accounting for 86 percent of page views for that group, presented some form of advertising, and likely derived most of their revenues from doing so (Evans 2009). By 2012, $36.6 billion were spent on digital ads, ahead of cable TV ($32.5 billion) and slightly below broadcast TV ($39.6 billion), with a rate of growth outpacing all other formats.[13] By 2015, digital ad revenues had reached $52.8 billion, accounting for just under a third of overall advertising.[14] Meanwhile, the market capitalization of the major publicly traded newspaper businesses in the United States *declined* by 42 percent between January 2004 and August 2008, compared to a 15.6 percent gain for the Dow Jones industrial average over that time period.

Key to the online collection of consumer information are the aspects of "targetability," the collection of data for the purpose of showing ads to specific subsets of users, and "measurability," the collection of data for the purpose of evaluating the efficacy of targeted ads. Data aggregators, advertising networks, and website operators establish relationships to enable them to track and target users across different websites and over time. Advertisers take advantage of the enhanced performance measurability of online advertising to experiment with different marketing messages before proceeding with a specific marketing campaign (see Lewis and Reiley 2014). Advertisers and website operators can track user behavior using several techniques—from web bugs (also known as beacons),[15] to cookies, to browser and device fingerprinting.[16] In fact, various and constantly evolving technologies (such as the aforementioned web bugs, or flash cookies, etc.) allow advertisers to track consumers' browsing activities and gain insight into their interests. For instance, web bugs are different from cookies because they are designed to be invisible to the user and are not stored

[13] See http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2012_rev.pdf.

[14] See http://tcrn.ch/1ymh9pB/.

[15] Web beacons are small pieces of code placed on websites, videos, and in emails that can communicate information about a user's browser and device to a server. Beacons can be used, among other things, for website analytics or to deliver a cookie to a user's device.

[16] Fingerprinting refers to technologies that use details about a user's browser and device in order to identify the user's browser or device over time. Fingerprinting can be used for the same purposes as cookies, but does not require files to be stored on a user's device, and is harder to both notice and evade.

on a user's computer. Without inspecting a web page's underlying code, a customer does not know that they are being tracked. Compared to traditional surveillance methods, collecting data about individuals online is cheaper and faster (Wilson and Brownstein 2009). Retention policies for that data (such as the length of time search engine queries or clickstream information can be stored and used by data holders) vary across organizations and jurisdictions, and can impact both welfare and market outcomes (Bottero and Spagnolo 2013). Search engines data, for instance, is collected about individual users using cookies, IP addresses, and other methods. Associated with this profiling are the search queries and subsequent clicks made by each user. In the past, Google was said to keep this information for nine months (eighteen months in the case of cookies) and anonymize it afterwards; Microsoft was said to keep this information for six months. But in practice, there is no real verification of whether data holders in fact delete or at least anonymize user information.

Despite the large sums of money spent on targeted advertising, however, its effectiveness is unclear. Farahat and Bailey (2012) estimate that targeted advertising in 2012 generated, on average, twice the revenue per ad as nontargeted advertising. However, some of these estimates have been challenged (Mayer and Mitchell 2012), and more recent empirical work has found evidence indicating that personalized advertising may be ineffective (Lambrecht and Tucker 2013). Blake et al. (2015) reinforce the latter findings. They measure the effectiveness of paid search by running a series of large-scale field experiments on eBay, and find evidence that returns from paid search are a fraction of conventional nonexperimental estimates (and can, in some cases, be negative). Targeted advertising, in principle, could provide consumers with information about products they want or are interested in, thereby reducing search costs and improving welfare. However, as the theoretical literature examined in section 2.3.3 suggests, the effects of targeting can be rather complex and nuanced, and not necessarily always positive for consumers. Consumers may even be offered products inferior to the ones they would have found otherwise, or even potentially damaging ones. For instance, data brokers sell lists of consumers to target individuals suffering from addictions such as alcoholism or gambling.[17] Additionally, concerns exist over the fact that tracking technologies are often made invisible to end-users (Smith 1999), whereby a significant lack of awareness and misconception exists among consumers regarding the extent, nature, and depth of targeting techniques (McDonald and Cranor 2010). Even sophisticated consumers may not be able to avoid being tracked, as the advertising and data industry has often found new ways of tracking and identifying users after consumers had learned about and adopted measures to counter existing forms of tracking (Hoofnagle et al. 2012).

On the other hand, concerns exist that the introduction of strict privacy regimes may inhibit either the tracking or the targeting of potential consumers, and in doing so, may dampen the development of electronic commerce (Swire and Litan 1998). European countries have raised barriers to the collection and use of personally identifiable data, including a requirement that firms seek explicit consent from consumers to collect information about their past purchases and recent browsing behavior. The European ePrivacy Directive (2002/58/EC) predominantly addresses the telecommunications sector, but also regulates the use of

[17] See, e.g., http://www.dmnews.com/media-one-gamblers-database/article/164172/.

cookies and similar tracking methods.[18] The EU ePrivacy Directive (Recital 24) explicitly states that "[s]o-called spyware, web bugs, hidden identifiers, and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, store hidden information, or trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned." With regards to tracking cookies, the directive permits their use on the condition that users provide their consent. The 2012 Do-Not-Track proposal by the Federal Trade Commission (FTC) suggests a set of guidelines somewhat similar to the EU ePrivacy Directive for the United States—giving consumers a way to opt out of having their data collected. However, as the FTC's proposal follows an opt-out rather than an opt-in approach, it may be less costly for US firms to continue collecting data and using targeted ads.[19]

Goldfarb and Tucker (2011b) examine the effects of the implementation of the EU ePrivacy Directive on purchase intentions, and find evidence that after the ePrivacy Directive was passed, hypothetical advertising effectiveness decreased significantly. They use the responses of 3.3 million survey takers who had been randomly exposed to 9,596 online display (banner) advertising campaigns to explore how strong privacy regulation in the European Union influenced the effectiveness of advertising. For each of the 9,596 campaigns, their data contains a treatment group exposed to the ads and a control group exposed to a public service ad. To measure ad effectiveness, they use a short survey conducted with both groups of users about their purchase intent towards an advertised product. They find that following the ePrivacy Directive, banner ads experienced a reduction in effectiveness of over 65 percent, in terms of changing consumers' purchase intents. They see no similar change in ad effectiveness in non-European countries during a similar time frame.

These findings raise a number of stimulating questions. One interpretation of the results is that privacy regulation can have a detrimental effect on the advertising industry. Moreover, as online advertising has become a primary source of revenue for many web-based businesses, the types of content and services provided on the Internet may shift as a result of privacy regulation. However, the decrease in hypothetical advertising effectiveness was only found within a subset of ads (static, content-specific, and small) whereas other types of ads were not at all affected (larger ads, dynamic ads, and ads consistent with the content of a website). This suggests a possible way forward for organizations. For instance, general interest websites may fine-tune ads based on the content of a specific web page to make it easier to monetize, providing ads that are more contextually appropriate. Another question raised by the results is whether any actual economic damage will be ultimately incurred by consumers (or by merchants as a whole) after the legislation discourages marketers from using tracking cookies. This may depend on whether the effect of behavioral

[18] See the Data Protection Directive (1995/46/EC) and the Privacy and Electronic Communications Directive (2002/58/EC, last amended by Directive 2009/136/EC, sometimes called the EU Cookie Directive), also known as the ePrivacy Directive, which regulates cookies and other similar devices. The current prescription is, in short, that certain types of cookies or similar methods must not be used unless the relevant Internet user: (1) is provided with clear and comprehensive information about the purposes of the storage of, or access to, those cookies; and (2) has given his or her consent.

[19] For instance, Johnson and Goldstein (2004) show that consumers tend to go with the default option chosen for them in the case of organ donation, despite heavy lobbying by organizations. That is, if the default approach is for consumers to be subscribed to targeted ads, then more consumers are likely to remain subscribed than under an opt-in system where consumers are by default unsubscribed.

advertising is more *persuasive* or more *informational*—that is, whether the main effect of behavioral targeting was simply a *switching* effect (that is, nudging and persuading consumers to buy from a certain merchant rather than another one), as opposed to an informational effect (that is, informing consumers about products or services of which they would not have otherwise been aware).

Related work has addressed the question of which format of ads advertisers should and should not use. White et al. (2008) find that consumers may experience "personalization reactance" by negatively reacting to highly personalized messages when the fit between the targeted offer and consumers' personal characteristics is not explicitly justified. Goldfarb and Tucker (2011a) find that obtrusive targeted ads—targeted in the sense that they are matched to the content of a website, and obtrusive in terms of visibility—are more likely to trigger privacy concerns among users in comparison to obtrusive but not targeted ads, or targeted but less obtrusive ads. These findings can help explain the enormous success of Google AdSense, a service that provides contextually targeted unobtrusive ads (AdSense accounts for about a third of Google's ad revenue, with the other two thirds coming from search advertising).[20] Moreover, it can help explain the apparent divide in online advertising between banner ads and unobtrusive targeted ads.

3.2 *Privacy and Price Discrimination*

Along with being targeted with personalized offers, consumers may also face price discrimination. Tracking and measurability, in addition to websites' ability to dynamically update and personalize prices for each visitor, are bringing online markets closer to the theoretical scenario of first-degree price discrimination. Indeed, much of the literature surveyed in section 2.3.1 focuses on merchants' ability to engage in forms of targeting that increasingly approach the textbook "ideal" of first-degree discrimination. Relative to the volume of theoretical analyses, however, empirical efforts to find evidence of Internet-based price discrimination have lagged behind. Valentino-Devries, Singer-Vine, and Soltani (2012) suggest that certain online retailers may be engaging in dynamic pricing based on their ability to estimate visitors' locations, and, specifically, the (online) visitor's physical distance from a rival brick-and-mortar store. Mikians et al. (2012, 2013) find suggestive evidence of price discrimination based on information collected online about consumers, as well as evidence of "search discrimination" (steering consumers towards different sets of products with different prices, following their searches for a certain product category). In particular, Mikians et al. (2013) suggest price differences of 10 percent to 30 percent for identical products based on the location and the characteristics (for instance, browser configurations) of different online visitors.

On the other hand, Vissers et al. (2014) find price *variation*, but no experimental evidence of consumer-based price *discrimination* in online airline tickets. In short, the evidence of systematic and diffuse individual online price discrimination is, currently, scarce. It is possible that firms may consider online price discrimination as not just challenging, but potentially risky.[21] And yet, anecdotal cases of firms selectively offering price discounts are ubiquitous (i.e., instead of raising prices to some consumers, firms may simply reframe their behavior by offering price discounts to others). It is also

[20] See https://investor.google.com/earnings.html. It is also worth noting that contextual targeting is also common in the offline world (e.g., magazines about fishing contain ads for fishing equipment).

[21] Consider, again, the backlash following Amazon's purported attempts at price discrimination (Anderson and Simester 2010).

possible that the infrastructure for accurate price discrimination (and its detection) is underdeveloped and still evolving—similarly to the case of behavioral ads (which, anecdotally, seem as likely to present consumers with offers of products they have already searched for or even bought, rather than undiscovered products in which they may be interested).

3.3 *Other Forms of Discrimination*

Price discrimination is probably the least odious form of discrimination involving the use of personal information. In many other markets, significant trade-offs can arise as function of the amount of personal information available to other parties, including scenarios where privacy protection will cause, or in fact hinder, discrimination.

Consider, for instance, hiring. Economists have long been interested in the role of information (Stigler 1962) and signaling (Spence 1973) in job market matching. And of course, there exists a vast economic literature on discrimination in hiring or wages. Experimental work has highlighted that employers may infer candidates' personal traits from information available on their resumés (such as the candidates' race from their names) and use that information to discriminate among prospective employees (Bertrand and Mullainathan 2004). In fact, fairer job market outcomes may sometimes be achieved after *removing* information from the marketplace. Goldin and Rouse (2000), for instance, find evidence that blind auditions (in which screens conceal the identities of candidates such as orchestra performers from the jury) foster impartiality in hiring and increase the probability that women will be hired. On the other hand, Bushway (2004) and Strahilevitz (2008) point out a different dynamic: when employers are not able to retrieve pertinent information about a job applicant (for instance, their criminal records) due to privacy regulation, employers may become increasingly reliant on statistical discrimination strategies. Thus, an employer's personal animus or bias may end up negatively and disproportionately affecting certain minorities. Under this scenario, expanding the information available to employers may generally lead to fairer and possibly more efficient outcomes.

Similarly contrasting dynamics arise on online dating platforms. By facilitating abundant signaling of personal traits and interests, dating platforms can facilitate matching and sorting (Hitsch, Hortacsu, and Ariely 2010). However, because most platforms allow members to screen and filter their populations on the basis of personalized criteria such as racial backgrounds, these platforms can reinforce racial dynamics already existing in face-to-face interactions (in a study of a popular online dating site, Lewis (2013) finds that users "disproportionately message other users from the same racial background"). On the other hand, choosing not to share certain information may be counterproductive for a site's members: the veil of anonymity (specifically, a member's ability to visit other members' profiles without leaving an identifiable trace of that visit) actually reduces the probability of that member finding matches on the site (Bapna et al. forthcoming). The variety of these outcomes exemplifies one of the major themes of this article: the consequences and implications of data sharing or data protection vary very much with context—such as what specific type of data is being shared, how, and when.

Consider, also, online platforms that allow tenants to find landlords and vice versa; or platforms that enable property owners to "share" their houses with short-term renters; or platforms that enable car owners to share their vehicles with other drivers or passengers. These examples of IT-enabled "sharing economies" may increase efficiency by improving how resources such as housing or vehicles are used. However, when these

platforms expose members' personal information, they may inadvertently foster discrimination. Using data from Airbnb (an online dwelling rental marketplace, on which the race of a landlord can often be inferred from profile photos on landlords' Airbnb accounts), Edelman and Luca (2014) find that New York City landlords who are not African American charge approximately 12 percent more than their African American counterparts for an equivalent rental.

Another example where expanding the amount of information that is available to the marketplace may influence discrimination concerns employment opportunities for individuals with criminal records. Evidence suggests that employers do use criminal records to screen candidates (e.g., Bushway 2004). Because of the stigmatizing effect associated with a criminal history, individuals with criminal records are more likely to experience job instability and wage decline (see, for instance, Waldfogel 1994; Nagin and Waldfogel 1995). Information technology has exacerbated the problem: large numbers of criminal histories are now computerized in state repositories and commercial databases. Thus, ex offenders may be trailed by their crime histories wherever they may apply for jobs. This can occur despite a criminal record being, at some stage, "stale." This is in contrast to Blumstein and Nakamura (2009), who point out that the likelihood of recidivism, or a person's relapse into criminal behavior, declines with time spent without committing a crime, and at a certain point in time, an ex offender who has remained "clean" can be regarded as providing no greater risk than a nonoffender counterpart of the same age. In those cases, there could be social benefits from forgetfulness (Blanchette and Johnson 2002).

In many countries, legislators are acutely interested in these problems, and finding the right balance of sharing and protection of personal information is a thorny matter of public policy. For instance, in the United States, several states authorize courts to expunge or seal certain criminal records—but only for certain types of arrests and convictions. Similarly, in most of the United States, an employer who asked about the religion of a job candidate would risk being sued under Equal Employment Opportunity laws; however, different types of information enjoy different protections (for instance, information regarding religious affiliation cannot even be inquired about in interviews, whereas other types of personal information may, theoretically, be inquired about, but should not actually be used in decisions concerning hiring or wages).

Information technology, however, has created new challenges in this context: many job candidates nowadays publicly provide personal information through social-network profiles, including information such as sexual orientation or religious affiliation, which may actually be protected under state or federal laws. Employers are not supposed to ask about such information during the hiring process—but searching for it online significantly reduces the risk of detection. Acquisti and Fong (2013) have investigated the role of social media in the hiring behavior of US firms. In the authors' experiment, they create online social-media profiles for job candidates and then submit job applications on behalf of those candidates to a sample of over 4,000 US employers. If an employer were to search online for the name found in the resumé and application it received, it would find the social-media profile of the candidate and be exposed to the experimental manipulation. Acquisti and Fong estimate that only a (sizable) minority of US employers likely searched online for the candidates' information, and that the overall effect of the experimental manipulations was small. However, they did find evidence of both search and discrimination among a self-selected set of employers. In this, as in other scenarios, it is still unclear the extent to which novel

information channels will reduce market frictions and increase efficiency, or in fact promote new forms of discrimination.

3.4 *Privacy and Health Economics*

Privacy protection may affect the extent and direction of data-based technological progress. Particularly significant privacy trade-offs arise in the context of technology adoption in the medical industry, as many new health-care technologies depend on information exchange (Schwartz 1997).

Innovations in digitizing health information can lead to quality improvements by making patient information easy to access and share. For instance, electronic medical records (EMRs) allow medical providers to store and exchange patient information using computers, rather than paper records. Hillestad et al. (2005) suggest that EMRs could reduce annual US health-care costs by $34 billion through greater efficiency and safety, assuming a fifteen-year period and 90 percent EMR adoption. However, privacy regulation may affect the rate and manner in which hospitals and health-care providers adopt EMRs. In the European Union, personal data recorded in EMRs must be collected, held, and processed in accordance with the Data Protection Directive. In the United States, the 1996 US Health Insurance Portability and Accountability Act (HIPAA) established some rules for privacy in health care, and the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act, devoted $19.2 billion to increasing the use of EMRs by health-care providers. US hospitals may hesitate to adopt EMR systems if (1) they are concerned about their patients' responses, and (2) if regulation intended to protect patient privacy ends up hindering the adoption of such systems because hospitals cannot properly utilize them by, for instance, exchanging patient information with other hospitals. (Although EMRs were invented in the 1970s, by 2005 only 41 percent of US hospitals had adopted a basic EMR system (Goldfarb and Tucker 2012a)). Using variations in medical privacy laws across US states and across time, Miller and Tucker (2007, 2009, 2011a, 2014a) provide evidence quantifying the effect of state privacy protection on the diffusion of EMRs. They find that privacy regulations restricting a hospital's release of patient information significantly reduced the adoption of electronic medical records, primarily due to diminished network effects in adoption. Their analysis suggests that state privacy regulation restricting the release of health information reduces aggregate EMR adoption by more than 24 percent. They further estimate that a 10 percent increase in the adoption of such systems can reduce infant mortality by 16 deaths per 100,000 births.

Miller and Tucker identify two schools of thought about the interplay of privacy concerns, regulation, and technological innovation. Although their discussion focuses on the health-care sector, their arguments apply more generally to the interaction between privacy laws and innovation. The first school of thought holds that regulatory protection inhibits technology diffusion by imposing costs upon the exchange of information. In addition to these trade-offs, hospitals are faced with complexities concerning state-specific regulation and information exchange across state lines. The second school of thought, instead, argues that explicit privacy protection promotes the use of information technology by reassuring potential adopters that their data will be safe.

Consider a possible example of the latter dynamics, in the context of Health Information Exchanges (HIEs). HIEs are information technology solutions that facilitate the sharing of patients' electronic medical records. They are expected to enhance information-sharing capabilities among

health-care entities, with the aim of improving the quality of care. Their adoption, however, is said to have been hindered by privacy concerns, and it is unclear how privacy laws, such as legislation restricting the disclosure of health records, impact their adoption. In the United States, state laws may incentivize HIE efforts, include specific privacy requirements for sharing health-care data, or both. Adjerid et al. (forthcoming) investigate the impact that different state laws had on the emergence and success of HIEs. They compare the adoption and success of HIEs in states with laws that limit information disclosure with states that do not have such laws. The authors find that the combination of adoption subsidies and stronger privacy protection (that is, legislation that includes strict requirements for patients' consent in order to use their medical data) is associated with greater HIE adoption than either under privacy protection alone, or, importantly, under subsidies alone. Their results suggest that there can be policy complementarities between privacy laws and other types of interventions (such as financial subsidies and technical assistance in the case of HIEs). Their findings also highlight that different degrees of privacy regulation can have different effects on technology innovation and on economic welfare. Regulators may thus find room for balancing meaningful privacy protection while incentivizing the adoption of information technology efforts.

Genetic research is another field where complex trade-offs may arise from the interplay of technological innovation and privacy regulation. Oster et al. (2010) use data from a prospective cohort study of approximately 1,000 individuals at risk for Huntington's disease (HD), a degenerative neurological disorder with significant effects on morbidity, to estimate adverse selection in long-term care insurance. They find evidence of adverse selection: individuals who carry the HD genetic mutation are up to five times more likely than the general population to own long-term care insurance. Other genes, such as those associated with increased risks of breast cancer, colon cancer, Parkinson's, and Alzheimer's diseases, have also been identified, and testing for these genes is becoming more common and more precise (Burton et al. 2007). This testing, in turn, is likely to increase the amount of private information stored about individuals. On the one hand, this information may be useful in developing treatments, vaccines, and immunizations. On the other, while US laws limit an insurer's ability to observe an individual's specific genetic information, marketers (e.g., for certain drugs and treatments) and advertising platforms may certainly be interested in it. A number of companies in fact aim at offering genetic testing to individuals at affordable rates.[22]

Relatedly, using data on genetic testing for cancer risks, Miller and Tucker (2014b) examine how state genetic privacy laws affect the diffusion of personalized medicine. They identify three approaches taken by states to protect patients' genetic privacy: requiring informed consent; restricting discriminatory usage by employers, health-care providers, or insurance companies; and limiting *redisclosure* without consent. They show evidence that the redisclosure approach encourages the spread of genetic testing, in contrast to the informed consent approach, which deters it.

The results in both Miller and Tucker (2014b) and Adjerid et al. (forthcoming) illustrate how privacy laws need to be tailored to take into account and balance

[22] For instance, 23andme (https://www.23andme.com/) did so before the US Food and Drug Administration (FDA) directed them to cease while they undergo a regulatory review process. Prior to their primary operations being halted, they would store individuals' DNA and offer updates on potential health issues as testing procedures advanced. Currently, they do so for a subset of of potential health conditions—those for which they received FDA approval.

specific and continually evolving trade-offs, and how rather than looking at privacy regulation in a binary, monotonic fashion, the effect of regulation on technology efforts can be heterogeneous, depending on the specific requirements included in the legislation. Consider, again, genetic data: genomic analyses may not only reveal information about an individual's current health, but also about future health risks, and this potential to reveal information is likely to expand. These analyses are useful for patients and health-care providers because they facilitate the delivery of personalized medicine. At the same time, as personal genetic and genomic information becomes increasingly available, consumers face new privacy risks—for instance, if such information reaches the hands of advertising platforms and data aggregators, the latter may use it to construct risk profiles for individuals and their biological relatives such as children and parents, combine it with other data, and improve their targeting of product offerings. Adding another angle to this discussion is Miller and Tucker's finding that genetic privacy laws have distinct effects beyond standard health data privacy laws—in particular, different laws may alter individual behavior.[23]

Yet another trade-off in this legislative balancing act arises from the observation that wider access to genetic and genomic analyses can lead to broader improvements in overall health care. However, and importantly, medical privacy and medical analytics (including genetic research) do not *have* to be antithetical. In 2015, the Nuffield Bioethics Council in the United Kingdom produced a report highlighting a series of recommendations for achieving two seemingly contrasting requirements: generating, using, and extending access to data (because doing so "is expected to advance research and make public services more efficient"); while, at the same time, protecting privacy ("as this is a similarly strong imperative, and a requirement of human rights law") (Nuffield Council on Bioethics 2015).

Another example of balancing health-related informational privacy with public benefits is the identification of infectious disease outbreaks—the reporting of these cases to state authorities is usually exempt from privacy restrictions. Rapidly identifying such outbreaks is critical for the effective initiation of public-health intervention measures, preparation and readjustment of vaccines, and the timely alerting of governmental agencies and the general public. Google Flu Trends, for instance, takes advantage of users' searches for influenza-related terms to provide both public-health professionals and the general population with a real-time, geographically specific view of influenza search activity in the United States.[24] Other monitoring services include HealthMap and the International Society for Infectious Diseases' Program for Monitoring Emerging Diseases.

3.5 *Privacy and Credit Markets*

In the United States, credit reporting was not regulated at the federal level until 1970, when the Fair Credit Reporting Act (FCRA) was legislated. The Act was subsequently amended several times. Currently, the credit-reporting industry is among the most regulated in terms of data protection. The FCRA established permissible purposes of credit information disclosure, codified information flows along the lines that they

[23] This finding is reminiscent of Johnson and Goldstein (2004) who, as previously mentioned, show that consumers tend to go with the default option chosen for them in the case of organ donation, despite heavy lobbying by organizations. That is, if the default approach is for consumers to disclose genetic information to their immediate health-care provider along the lines of the "redisclosure" approach, then more consumers are likely to accept the service than under the opt-in system of the "informed consent" approach.

[24] Also see, however, section 4.4 on the problem of drawing proper conclusions from the data.

had naturally developed in the market, introduced dispute settlement mechanisms and data correction procedures, and assigned expiration dates to negative information such as bankruptcy and payment defaults. Several information flows, such as those among nonaffiliates, were left unregulated at the federal level, although some states enacted their own regulations (Jentzsch 2006). The 1990s brought major reforms in the United States that were intended to strengthen financial privacy laws, in light of intensifying public debate about privacy erosion given advancements in information technology. The Consumer Credit Reporting Reform Act (CCRRA) of 1996 introduced for the first time duties for financial information providers. In order to correct inaccuracies in consumers' records, the CCRRA mandated a two-sided information flow to/from credit bureaus and providers, and formalized some information flows among affiliates.

The Gramm–Leach–Bliley (GLB) Act of 1999 extended the CCRRA by formally and legally allowing a variety of financial institutions to sell, trade, share, or give out nonpublic personal information about their customers to nonaffiliates, unless their customers direct that such information not be disclosed by opting out. The GLB Act, while granting consumers the option to opt out, restricts it to nonaffiliates. An affiliate is defined as any company that controls, is controlled by, or is under common control with another company. Consumers have limited (if any) power to restrict this kind of "corporate family" trading of personal information. There are also several other exemptions under the GLB Act that can permit information sharing despite a consumer's objection. For instance, if a financial institution wishes to engage the services of a separate company, they can transfer personal information to that company by arguing that the information is necessary to the services that the company will perform. A financial institution can transfer information to a marketing or sales company to sell new products or jointly offered products. Once this unaffiliated third party has a consumer's personal information, they can share it within their own "corporate family." However, they themselves cannot likewise transfer the information to further companies through this exemption. In addition, financial institutions can disclose users' information to credit reporting agencies to comply with any other laws or regulations.

For lenders, the extension of credit to borrowers depends on the acquisition and possibly the exchange of personal information among market participants. Jentzsch (2006) develops a financial privacy index to quantify the extent of information protection across different regimes, demonstrating that the United States grants less data protection than EU members. The primary concern is that more stringent data protection regulations may lead to reduced access to credit, thus creating a trade-off with consumer privacy. In line with this work, Pagano and Jappelli predict that if banks share information about their customers, they would increase lending to safe borrowers, thereby decreasing default rates (Pagano and Jappelli 1993; Jappelli and Pagano 2002). Relatedly, Einav, Jenkins, and Levin (2013) find that credit scoring provides the ability to target more generous loans to lower-risk borrowers among individuals with lower income. Other empirical studies tend to focus on the effects of credit bureaus and creditor rights using data from a cross section of countries (see, e.g., Djankov, McLiesh, and Shleifer 2007; Qian and Strahan 2007).

States and local municipalities may enact legislation and local ordinances that exceed the protections in the GLB Act.[25] They may

[25] However, in *ABA v. Brown*, banks were partially successful in preempting state restrictions on sharing of affiliate info and credit reporting info. See, e.g., https://epic.org/privacy/preemption/ABABrown-SG-Brief.pdf.

require, for instance, opt-in consent, as is the case in a subset of the Bay Area counties examined in Kim and Wagman (2015). In a study that directly bridges the theoretical and empirical analyses of privacy, Kim and Wagman incorporate information acquisition and privacy regulation—through restrictions on information trade—into a model of consumer screening. In their model, firms, such as mortgage lenders, compete in prices. Lower prices, however, entail more stringent screening of applicants. The authors show that, in equilibrium, consumers apply to obtain loans from firms posting the lowest prices, despite anticipating more stringent loan approval processes. They then demonstrate that enabling firms to sell applicant data to interested downstream parties, such as insurers, can lead to even lower prices, higher screening intensities, and higher rejection rates of applicants; however, social welfare, overall, increases.

One of the main criticisms of the GLB Act's privacy provisions has been that most consumers do not (and likely will not) take advantage of the *opt-out* option to request that a firm ceases trade in their information. In 2002, three out of five counties in the San Francisco–Oakland–Fremont, California, Metropolitan Statistical Area enacted a local ordinance (effective January 1, 2003) that is more protective than then-current practices by pursuing an *opt-in* approach. Specifically, the local ordinance would require financial institutions to seek a written waiver before sharing consumer information with both affiliates and nonaffiliates. The variation in the adoption of the ordinance—adopted in three of the five counties—led to simple policy differences in local financial-privacy statutes. Exploiting this variation, and using Census tract-level and individual loan-level data on mortgage and refinancing applications, Kim and Wagman demonstrate that the opt-in ordinance had a statistically significant negative effect on loan denial rates (that is, approval rates increased), consistent with their theoretical model's predictions. They further provide some suggestive evidence that foreclosure start rates during the financial crisis of 2007–08 were higher in the counties that adopted the privacy ordinance, possibly indicative of looser underwriting standards following the ordinance, also in line with their model's predictions.

3.6 *Markets for Privacy and Personal Data*

Databases of consumer data or consumer reports have existed throughout the twentieth century (Smith 2000). The progress of information technology and the advent of the Internet have, however, vastly increased the scope and reach of those databases, ultimately giving rise to a market ecosystem of organizations that gather, merge, clean, analyze, buy, and sell consumer data. This ecosystem, although dominated by a decreasing number of players (Krishnamurthy and Wills 2009), is still rather complex and decentralized (Olejnik, Minh-Dung, and Castelluccia 2014). There is no single, unified market for personal data. Rather, there are multiple markets in which data is traded, and multiple markets in which privacy is sought or purchased (cf. Lane et al. 2014). These include markets where data aggregators buy and sell data to other organizations (data subjects generally do not participate directly in these markets, and are in fact often unaware that reports on their names may exist); markets in which consumers exchange personal information for "free" products or services (for instance, search engines and social media); markets where consumers actively attempt to purchase protection for their data and/or against the negative consequences of privacy intrusions (for instance, identity theft, insurance services); and markets where consumers attempt to explicitly trade their data in exchange for money (such as services provided by "personal data vault" firms, akin to the proposal for privacy markets in Laudon 1996).

One particular type of database that has attracted the attention of economists is the National "Do-Not-Call" Registry, a database established by the Do-Not-Call Implementation Act of 2003. It allows US residents, by registering, to disallow telemarketers to call their phone numbers with promotional offers. Within twenty-four hours of its opening on June 27, 2003, over 10 million telephone numbers were registered; by February 2007, registrations exceeded 139 million. Some studies have delineated the demographic characteristics of those likely to opt out using Do-Not-Call, and estimated consumers' benefit from doing so. Varian, Wallenberg, and Woroch (2005) calculate consumers' value for telemarketing privacy to range from $0.55 to $33.21 per household per year, while Png (2010), using state-level registries, estimates it to be between $13.19 to $98.33 per household per year. Goh, Hui, and Png (2015) use data from the federal registry (and previously established state-level registries) to investigate externalities arising from consumers opting out via the Do-Not-Call registry. Consumers who opt out prefer privacy to the benefits associated with targeted advertisements. Their decision reduces the pool of consumers available for sellers to solicit. In response, sellers redirect some of their marketing efforts to those consumers who are still available for solicitation. As these consumers experience an increase in solicitations, some of them respond by opting out as well. As more consumers opt out, sellers continue to adjust their solicitation. In a sense, sellers face a form of a prisoner's dilemma: individually, sellers wish to intensify their targeting of the pool of consumers who did not opt out; collectively, they would be better off holding back to keep this pool of consumers from shrinking further. Consumers, on the one hand, benefit from having the option of not being targeted with advertisements; on the other hand, consumers who opt out lose the benefits of targeted advertising, and those who do not opt out are likely to be excessively targeted with advertisements. The conclusions of these works may extend to the ongoing debate over a "do-not-track" policy for online markets.

3.7 *Privacy and Information Security*

While privacy and information security are distinct concepts, they can overlap. By "information security" we refer to the processes designed to protect data assets. Poor information security can lead to what Solove (2006) refers to as "insecurity," or carelessness in protecting (personal) information from leaks and improper access. While the economics of information security has become a field of research in its own right, covering subjects as diverse as the optimal timing for patching operating systems or markets for software vulnerabilities,[26] a number of topics are of interest to both privacy and security researchers, such as spam, identity theft, and data breaches.

Although spam messages are not entirely random (Hann et al. 2006), the term "spam" is used to refer to the indiscriminate use of electronic messaging systems for unsolicited advertisement to consumers. A study by Ferris Research estimates that in 2009, the cost of spam, accounting for decreased user productivity, was about $130 billion, with $42 billion in the United States alone. These estimates, however, should be taken with caution: in 2012, Rao and Reiley (2012) estimated a much lower overall societal cost of spam, $20 billion.

While every Internet user receives spam, the cost per user is low, primarily due to users' reliance on filtering technologies. On the other hand, identity theft may affect fewer individuals, but at larger individual costs.

[26] For a review of the literature on the economics of information security, see Anderson and Moore (2006).

The 1998 US Identity Theft and Assumption Deterrence Act (ITADA) defines identity theft as the knowing transfer, possession, or usage of any name or number that identifies another person with the intent of committing, aiding, or abetting a crime. Advances in information technology have allowed identity thieves to combine information taken from a variety of sources to open accounts in the names of others' identities (Cheney 2005; Coggeshall 2007). Anderson, Durbin, and Salinger (2008) report 30 mentions of "identity theft" in US newspapers in 1995; 2,000 in 2000; and 12,000 in 2005. In 2006, identity theft resulted in corporate and consumer losses of $61 billion, with 30 percent of known identity thefts caused by corporate data breaches. By 2012, the Bureau of Justice estimated that 16.6 million US residents ages sixteen and older (or about 7 percent of the population in that age group) had been victims of at least one incident of identity theft. By 2014, the number of US victims was estimated at 17.6 (Harrell 2015). It is further estimated that 75 percent of recorded breaches between 2002 and 2007 were caused by hackers or external sources, with over 77 percent involving the theft of Social Security numbers (Anderson, Durbin, and Salinger 2008; Romanosky, Telang, and Acquisti 2011; Harrell 2015).

Miller and Tucker (2011b) study the impact of data encryption laws on data breach incidences. Their study highlights the risks associated with internal security threats (e.g., those by employees authorized to access a corporate database). In particular, policies that focus on outside threats may paradoxically redirect efforts away from protecting against internal risks. However, as noted by Mann (2015), "information lost may not be information abused." That is, the probability distributions of data breach occurrences, and of actual abuse of stolen information conditional on a breach, are, if not unknown, extremely uncertain. This makes it harder to devise (or agree upon) sound framework for data security policy.

For instance, Roberds and Schreft (2009) argue that the loss of privacy due to identity theft is outweighed by gains from the relative ease of gaining access to available credit. Kahn and Roberds (2008) model the incidence of identity theft as a trade-off between the desire to avoid costly or invasive monitoring of individuals on the one hand, and the need to control transaction fraud on the other. They suggest that this trade-off will prevail despite any technological advances. Kahn, McAndrews, and Roberds (2005) examine the role of money in its provision of privacy and anonymous transactions, wherein a credit purchase may identify the purchaser. In a simple trading economy with moral hazard, the authors compare the efficiency of money and credit, and find that money may indeed be useful as a means of preserving anonymity toward sellers. More recently, the emergence of Bitcoin has provided a vehicle for doing just that—facilitating increased anonymity when transacting online (see, e.g., Böhme et al. 2015).

In response to increasing concerns regarding identity theft, many US states have adopted data-breach disclosure laws. By and large, these laws require firms to notify consumers if their personal information has been lost or stolen. Romanosky, Telang, and Acquisti (2011) use FTC data to estimate the impact of data-breach disclosure laws on identity theft over the years 2002 to 2007. They find that the adoption of data-breach disclosure laws has a marginal effect on the incidence of identity theft and reduces their average rate by under 2 percent. At the same time, state disclosure laws may have other benefits, such as reducing an average victim's loss and improving firms' security and operational practices (Schwartz and Janger 2007).

In some sense, whether or not state laws require firms to disclose information about data breaches could be interpreted as firms'

own level of privacy, which may pose its own set of trade-offs. Ideally, firms should be induced by strict disclosure laws to secure their customers' data. However, several studies that examine the financial impact of such disclosures on firms have come up with mixed and primarily mild results. Campbell et al. (2003), for instance, find only limited evidence of a negative reaction by the stock market to news of security breaches, although they do find a significant and negative effect on stock price for breaches caused by unauthorized access of confidential information. Using an event-study methodology, and considering a time window of one day before and one day after the announcement of a breach, they calculate a cumulative effect of −5.4 percent. Cavusoglu, Mishra, and Raghunathan (2004) find that the disclosure of a security breach results in the loss of 2.1 percent of a firm's market valuation over two days (the day of the announcement and the day after). Telang and Wattal (2007) find that software vendors' stock prices suffer when vulnerability information about their products is announced. Acquisti, Friedman, and Telang (2006) focus on the announcements of *privacy* breaches. They find a negative and significant, but temporary, reduction of 0.6 percent in the stock market price of affected firms on the day of the breach. Ko and Dorantes (2006) find that, while a firm's overall performance is lower in the four quarters following a breach, the breached firm's sales increase significantly relative to firms that incurred no breach. These findings suggest that a strict disclosure policy alone may not be, by itself, the solution to aligning the interests of firms, in terms of data security, with those of their customers.

3.8 *Consumer Attitudes and Behaviors*

Although privacy concerns seem to vary decidedly with context as well as personal traits (Acquisti, Brandimarte, and Loewenstein 2015), surveys of US respondents have repeatedly highlighted privacy as one of the most significant concerns of Internet users. In a 2009 study, Turow et al. (2009) find that 66 percent of Americans do not want marketers to tailor advertisements to their interests, and 86 percent of young adults do not want tailored advertising if it were the result of following their behaviors across websites. In a 2013 survey, the Pew Research Center finds that 68 percent of US adults believed that current laws are insufficient in protecting individuals' online privacy (Rainie et al. 2013).[27] A 2015 report, also by the Pew Research Center, finds that an overwhelming majority of US adults (93 percent) believe that being in control of who can get information about them is important; but only 9 percent of them think that they have, in fact, "a lot" of control over how much information is collected about them and how it is used (Madden and Rainie 2015). At the same time as they profess their need for privacy, most consumers remain avid users of information technologies that track and share their personal information with unknown third parties. If anything, the adoption of privacy-enhancing technologies (for instance, Tor,[28] an application for browsing the Internet anonymously) lags vastly behind the adoption of sharing technologies (for instance, online social networks such as Facebook).

The apparent dichotomy between privacy attitudes, privacy intentions, and actual privacy behaviors has caught the attention of scholars (e.g., Berendt, Gunther, and Spiekermann 2005), leading to a debate over the so-called privacy paradox (Norberg, Horne, and Horne 2007) and the value people assign to their privacy. Is the dichotomy real or imaginary? Do people actually care

[27] For analyses of privacy complaints submitted by consumers to the FTC, see https://ashkansoltani.files.wordpress.com/2013/01/knowprivacy_final_report.pdf.

[28] See www.torproject.org.

about privacy? If they do, how much exactly do they value the protection of their personal data?

Perhaps anticlimactically, a first possible resolution to the paradox is that it may not actually exist. Attitudes are often expressed generically (for instance, the seminal categorization by Harris and Westin (1992) of individuals into privacy pragmatists, fundamentalists, and unconcerned relied on broad and general survey questions), whereas behaviors (or behavioral intentions) are specific and contextual. Thus, it should not be surprising that the former may not correlate with or predict the latter (Fishbein and Ajzen 1975).

A second resolution is that people routinely and expertly engage in mental trade-offs of privacy concerns and privacy benefits (Milberg et al. 1995), or a so-called privacy calculus (Laufer and Wolfe 1977; Culnan and Armstrong 1999; Dinev and Hart 2006). This context-dependent calculus naturally leads to situations in which consumers will choose to protect their data, and other situations in which protection will be seen as too costly or ineffective and sharing is preferred. Privacy is, after all, a process of negotiation between public and private, a modulation of what a person wants to protect and what she wants to share at any given moment and in any given context. Therefore, neither does the sharing of certain information with others imply, per se, a loss of privacy, nor is the complete hiding of data necessary for the protection of privacy. In fact, the observation that people seem not to protect their privacy online very aggressively does not justify the conclusion that they never do so. Tsai et al. (2011) find that consumers *are*, sometimes, willing to pay a price premium to purchase goods from more privacy-protective merchants; Goldfarb and Tucker (2012b) use surveys to measure respondents' implied concern for privacy by their willingness to disclose information about income, and find evidence of privacy concerns increasing over an eight-year period; Stutzman, Gross, and Acquisti (2012) find evidence of increasing privacy-seeking behavior among a sample of over 4,000 early Facebook members; Kang, Brown, and Kiesler (2013) document Internet users' attempts to maintain anonymity online; and Boyd and Marwick (2011) discuss various alternative strategies teenagers adopt to protect their privacy while engaging in online sharing.

That noted, evidence of dichotomies between specific attitudes or preferences and actual behaviors have also been uncovered. Consider, for instance, Acquisti and Gross (2006), in the context of social networking sites; or consider Turow et al. (2009), who find that 66 percent of Americans do not wish for marketers to tailor advertisements to their interests—while the vast majority of them use search engines and social-networking sites, which operate based on enabling advertisers to target advertisements.

Thus, it is more likely that the purported dichotomy between privacy attitudes and privacy behaviors is actually the result of many, coexisting, and not mutually exclusive different factors. Among them, a role is likely played by various decision-making hurdles consumers face when dealing with privacy challenges, especially online, such as asymmetric information, bounded rationality, and various heuristics. For instance, some individuals may not be aware of the extent to which their personal information is collected and identified online (many Internet users are substantially unaware of the extent of behavioral targeting, and many believe that there is an implied duty of confidentiality and law that protects their data despite disclosure; see, e.g., McDonald and Cranor 2010; Hoofnagle and Urban 2014). Or, some individuals may not be aware of possible alternative solutions to their privacy concerns (such as privacy-enhancing technologies). Furthermore, some individuals'

privacy-sensitive decision making—even that of well-informed and privacy-sensitive subjects—may be affected by cognitive and behavioral biases, such as immediate gratification or status quo bias (Acquisti 2004; John, Acquisti, and Loewenstein 2011).

Because of those hurdles, it is difficult to pinpoint reliably the valuations that consumers assign to their privacy or to their personal data. Certainly, there is no shortage of studies that do attempt to quantify the value of data for both organizations and for end-users. For instance, Olejnik, Minh-Dung, and Castelluccia (2014) find that elements of users' browsing histories are being traded among Internet advertising companies for amounts lower than $0.0005 per person. Hann et al. (2007) quantify the value that US subjects assign to protection against errors, improper access, and secondary uses of personal information online to an amount between $30.49 and $44.62. Similarly, Savage and Waldman (2013) find that consumers may be willing to make a one-time payment of $2.28 to conceal their browser history, $4.05 to conceal their contacts list, $1.19 to conceal their location, $1.75 to conceal their phone's identification number, $3.58 to conceal the contents of their text messages, and $2.12 to eliminate advertising. However, privacy outcomes are uncertain (Knight 1921) and privacy concerns and expectations are remarkably context dependent (Nissenbaum 2004). Thus, small changes in contexts and scenarios can lead to widely differing conclusions regarding consumers' willingness to pay to protect their data. For instance, in a lab experiment, Tsai et al. (2011) find that a substantial proportion of participants were willing to pay a premium (roughly half a dollar, for products costing about $15) to purchase goods from merchants with more protective privacy policies; Jentzsch, Preibusch, and Harasser (2012) find that (only) a third of participants were willing to pay a similar premium to purchase cinema tickets from a merchant that requests less personal information than a competing, but cheaper, merchant; and Preibusch, Kubler, and Beresford (2013) find that a vast majority of participants chose to buy a DVD from a cheaper but more privacy-invasive merchant, than from a costlier (1 euro more) but less invasive merchant. In fact, behavioral and cognitive heuristics may also play a significant role in affecting privacy valuations.[29]

4. *The Evolving Privacy Debate*

Both the theoretical and the empirical studies we have examined in the previous sections of this article suggest that the path towards optimally balancing privacy protection and benefits from disclosure is, at the very least, uncertain. And yet, those studies also make the following clear: (1) different stakeholders—including businesses, consumers, and governments—each have different, multilayered, and often conflicting objectives; (2) information technologies, privacy concerns, and the economics of privacy evolve constantly, with no single study or policy intervention being able to fully account for future (and even some present) concerns; and (3) rather than a uniform piece of regulation to address contemporary privacy issues, a nuanced approach—dynamic and individualized to specific markets, contexts, and scenarios—may be necessary. In this section, we point out a number of privacy issues that have started and continue to attract a lively debate involving economics, technology, and policy. We also propose a number of directions for future research.

[29] For instance, applying the endowment effect to the study of privacy, Acquisti, John, and Loewenstein (2013) identify a discrepancy of up to five times the value individuals assign to the protection of personal information merely depending on the framing of the trade-offs, as opposed to actual changes in the trade-offs.

4.1 *Regulation versus Self-Regulation*

Empirical studies of privacy trade-offs have contributed to a debate over how to best protect privacy without harming the beneficial effects of information sharing. Much of this debate has juxtaposed the relative benefits of regulation and self-regulation (Bennett and Raab 2006; Koops et al. 2006). On one side of the debate, Gellman (2002) estimates that in 2001, $18 billion were lost by companies in Internet retail sales due to buyers' privacy concerns, and appraises at even larger amounts the costs that consumers bear when their privacy is not protected (the costs include losses associated with identity theft, higher prices, spam, and investments aimed at protecting data). This side of the debate advocates regulatory solutions to privacy problems (Solove 2003). One of the highlighted advantages of such solutions would be the avoidance of the complexity for data subjects to interact with different entities, each with different privacy policies (cf. Milberg, Smith, and Burke 2000).

On the opposite side of the debate, Rubin and Lenard (2001) suggest that the costs of privacy *protection* are much higher for both firms and consumers alike than the costs that may rise from privacy violations. For instance, according to the authors, targeted advertising gives consumers useful information, advertising revenues support new Internet services, and reducing the use of online information would ultimately be costly to consumers. This side of the debate advocates self-regulation. Self-regulatory solutions may work, for instance, when concerns over adverse consumer response limit advertisers' usage of invasive targeting of ads (Lohr 2010); website operators choose to comply with their published policies rather than engage in spam (Jamal, Maier, and Sunder 2003); and firms refrain from engaging in certain forms of price discrimination so as not to antagonize consumers (Anderson and Simester 2010).

The United States and the European Union have taken different positions in this debate. The European Union has focused on regulatory solutions, establishing principles that govern use of data across multiple sectors, including the need for individuals' consent for certain data processing activities. By contrast, the United States has taken a more limited, sectorial, and ad hoc regulatory approach, often opting for providing guidelines rather than enforcing principles. For instance, recommendations to the US Congress by the Federal Trade Commission (Federal Trade Commission 2012), motivated by the delays with which companies have adopted appropriate privacy rules, included the introduction of a do-not-track mechanism, similar to the Do-Not-Call list that became law in 2003. Such a mechanism would be built into websites and web browsers, and would allow people to signal to websites (and their commercial partners) that they do not want to be tracked. Limitations with respect to verification and enforcement would undoubtedly exist. Currently available services that allow consumers to opt out of advertising networks (such as the Self-Regulatory Program for Online Behavioral Advertising, and Google's opt-out settings) prevent users from receiving certain types of targeted ads, but they do not stop advertisers or sites from collecting data.

Self-regulatory solutions often rely on transparency and control (also known as "notice and consent"), and are therefore predicated around individuals' ability to be informed about, and properly manage, privacy settings and privacy concerns. However, numerous empirical studies have highlighted the limitations of transparency mechanisms. These include the failure of privacy policies to properly inform consumers about how their data will be used (Jensen and Potts 2004); the large opportunity costs associated with frameworks that rely on consumers reading privacy policies

(McDonald and Cranor 2008); and the fact that the same policy can nudge individuals to disclose varying amounts of personal data simply by manipulating the format in which the policy itself is presented to users (Adjerid et al. 2013). Control mechanisms have also been critiqued. For instance, while research in the information system literature has suggested that providing users with control over their information can reduce privacy concerns (Culnan and Armstrong 1999; Tucker 2014; Malhotra, Kim, and Agarwal 2004), the protection afforded by that control may be illusory. To that effect, Brandimarte, Acquisti, and Loewenstein (2013) highlight how the mere provision of more perceived control over personal information can paradoxically lead users to take more risks with their personal information, increasing their willingness to share sensitive data with other parties. As a result, doubts have been expressed about the viability of self-regulated transparency and control mechanisms in adequately protecting consumers' privacy (Acquisti, John, and Loewenstein 2013; Solove 2013; Zuiderveen Borgesius 2015). The limitations of notice and consent mechanisms as viable instruments of privacy policy were also acknowledged in a 2014 report by the US President's Council of Advisors on Science and Technology (Executive Office of the President—President's Council of Advisors on Science and Technology 2014).

An alternative approach to privacy protection relies on the propertization (Laudon 1996; Varian 1997; Schwartz 2004) or licensing (Samuelson 2000) of personal information. As noted in section 2.2 and in section 3.6, various authors have proposed the establishment of markets where individuals can trade (rights over) their personal information. With the advent of social media, a number of startups began offering services along those lines. However, it is not clear that such markets for personal data could ever be successful. First, when interacting with services that offer trade and protection for their data, consumers face similar hurdles as those that arise when dealing with transparency and consent in the presence of traditional privacy policies—including the hurdle of estimating the fair value of their personal information. Second, in the absence of regulatory frameworks that enforce protection of traded data, the possibility of secondary usage of personal information (after the subject has traded it to another party) may run counter to the very idea of protecting consumer data. Third, much of consumer data that is of value to advertisers is nonstatic information that is dynamically generated as part of the interaction of the individual with other online services, such as search engines or online social networks. These services would be unlikely to relinquish control over the personal information that their technologies help generate. An additional alternative proposed in the literature is the application of soft paternalistic solutions (designed by governments, organizations, or data subjects themselves as self-control mechanisms) to "nudge" individuals towards personal information practices they have claimed to prefer (Wang et al. 2013).

As noted in section 2.2, market-based solutions and regulatory approaches to privacy protection are not polar opposites. They are better perceived as points on a spectrum of solutions—from regimes that rely entirely on firms' self-regulation and consumers' responsibility (even in the absence of clearly defined and assigned property rights over personal data), to regimes with strict regulatory protection of data. Similarly, as pointed out in section 3.4, an understanding is emerging that the economic impact of privacy regulation is heterogeneous and context dependent: privacy regulation may have both positive and negative effects on economic growth and efficiency, depending on the specific *attributes* of the laws. Thus,

a potentially worthwhile direction of future research will aim at focusing on the specific features of regulation (and their differential effects on economic outcomes), rather than on simpler binary models contrasting regulation with its absence.

4.2 *From Big Data to Privacy-Enhancing Technologies*

As the amount of personal information produced and gathered about individuals continues to increase, so does the ability to utilize data mining to infer more sensitive information about them. For instance, Sweeney (1997) has highlighted the possibility of reidentifying supposedly anonymous health data, and Acquisti and Gross (2009) have shown how seemingly innocuous self-revelations made on the Internet—such as making available one's date and state of birth in a social network profile—may have serious consequences in terms of privacy intrusion. With evolving data mining and analytics tools being applied to expanding sets of personal data (the so called "big data" phenomenon) and with new technologies—from facial recognition to smart thermostats, from activity and health trackers to the Internet of Things—the portions of our personal and professional lives that are not monitored and quantified are further reduced. On the one hand, granular personal data may be used to provide even more precisely targeted services and to ensure that advertising is shown only to those consumers who stand to gain most from it (Tucker 2012). On the other, opportunities for abuse may abound. For instance, algorithmic discrimination may take subtle forms (Sweeney 2013 documents cases in which advertising technologies employed by a search engine can expose racial bias). And personal data may be used to influence individual decision making in subtle, targeted, and hidden manners (Calo 2014), raising questions over the limits of a person's autonomy and self-determination in a world where so much personal data can be gathered and used to influence the individual.[30]

The trade-offs arising from the intersection of big data and privacy suggest several fruitful directions for research. For instance: to what extent will the combination of sophisticated analytics and massive amounts of consumer data will lead to an increase in aggregate welfare, and to what extent will it lead to mere changes in the allocation of wealth? A related open question concerns the role of privacy-enhancing technologies (Goldberg 2003) in affecting how personal information will be used and with what economic consequences. Privacy-enhancing technologies, or PETs, can allow the protection of sensitive data without entirely disrupting commercially valuable flows of consumer information. They are, however, computationally intensive, and reduce the granularity of individual information available to others (consider, for instance, differential privacy, as in Dwork 2006). Thus, they may diminish its economic value. Therefore, how costly will those privacy-enhancing technologies ultimately be? Will their implementation costs, as well as the opportunity costs they may cause, be offset by gains in privacy protection? And, importantly, who will bear those costs—the data subjects or data holders? Finally, the contrast between the potential value of (big) data, and its privacy costs, raises questions about optimal retention policies. For instance, do larger quantities of consumer historical data provide competitive advantages to Internet search firms (Chiou and Tucker 2014)? And could a so-called "right to be forgotten," suggested

[30] For instance, Kramer, Guillory, and Hancock (2014) show that it is possible to influence the emotional states of users of a social networking site in the form of an emotional "contagion" by suppressing information containing positive or, alternatively, negative emotions.

by the European Commission,[31] support individuals' privacy rights without hampering the societal benefits of data sharing?

4.3 *Open Data, Government Records, and Surveillance*

The topic of this survey is the economics of privacy, and we have, therefore, naturally focused on the commercial acquisition and exploitation of personal data. It would be remiss of us, however, not to mention a no-less important facet of the privacy debate, one with potentially even greater impact on individuals and societies—namely the role and value of open access to data and governmental records, as well as the covert governmental collection of personal information.

Access to personal data (from governmental administrative records, to researchers' results arising from experiments and surveys, to firms' collections of consumers' data) is of great importance to empirical economists and social scientists. And once again, trade-offs arise between the utility of sharing publicly (or with other researchers) personal records and files and the privacy risks associated with granting access to third parties. Essentially, data utility and risks of disclosure are correlated (Duncan and Stokes 2004). Even statistical techniques meant to protect data (such as the technique of differential privacy, which attempts to minimize the risks of reidentification of records in a statistical database while maximizing the accuracy of queries from such database) still face risk/utility trade-offs (Fienberg, Rinaldo, and Yang 2010), not just for firms but also for researchers (Komarova, Nekipelov, and Yakovlev 2015). Furthermore, even protected (or anonymized, or deidentified) data may still be exposed (Ohm 2010; Heffetz and Ligett 2013). For instance, a portion of anonymized movie ratings data made available by Netflix as part of a competition to improve its ratings algorithms could be reidentified using Internet Movie Database (IMDB) data (Narayanan and Shmatikov 2008). These trade-offs apply both to government databases (the Census uses a variety of mechanisms and procedures to balance researchers' needs to access Census data with considerations for Census respondents' privacy) and to the private sector.[32] How to best balance researchers' and society's needs to access granular data with the need to protect individuals' records is a question that simultaneously involves economists and scholars in other disciplines, such as statisticians and computer scientists.

As for the topic of government surveillance, the US PATRIOT Act was enacted in 2001 and extended in 2011. It superseded, among others, the Foreign Intelligence Surveillance Act, the Electronic Communications Privacy Act, and the National Security Letter statutes. It facilitates the US government's collection of more information, from a greater number of sources, than had previously been authorized in criminal or foreign intelligence investigations. The PATRIOT Act enables greater access to records showing an individual's spending and communications, including e-mail and telephone conversations.[33] Beginning in June 2013, a series of disclosures by former CIA employee and

[31] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) COM(2012) 11 final, 2012/0011 (COD), January 25, 2012.

[32] Similarly, the problems of data breaches and identity theft discussed in section 3.7 do not arise only in the context of firms' databases, but also governmental ones: in the last few years, a number of large-scale data breaches involved governmental data, such as the loss of 26.5 million records of veterans, their spouses, and active-duty military personnel in 2006, or the recent IRS data breach that has put as many as 724,000 taxpayers at risk of identity theft (http://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/).

[33] See Congress CRS Report, 2011, at http://www.fas.org/sgp/crs/intel/R40980.pdf.

contractor Edward Snowden of thousands of classified documents involving data collection by the National Security Agency triggered a massive wave of public concern about privacy and governmental overreach (Marthews and Tucker 2015). The report of the US Administration's Review Group on Intelligence and Communication Technologies in December 2013 states that "excessive surveillance and unjustified secrecy can threaten civil liberties, public trust, and the core processes of democratic self-government," whereas in "an era increasingly dominated by technological advances in communication technologies, the United States must continue to collect signals intelligence globally in order to assure the safety of our citizens."[34] Together, the report states, the US government "must protect, at once, two different forms of security: national security and personal privacy." The report concludes that the "government should base its decisions on a careful analysis of consequences, including both benefits and costs (to the extent feasible)." Surveillance does not only have implications with respect to civil liberties, but also with respect to economic interests, from those of firms to those of other nations. These implications can give rise to disputes, including a 2016 legal dispute between Apple Inc. and the FBI regarding bypassing security mechanisms to gain access to a terrorist's cellphone, and the European Union's Court of Justice ruling in 2015 that the Safe Harbor agreements are invalid in response, at least in part, to the Snowden revelations (Finley 2015). These Safe Harbor agreements had thus far enabled US companies to comply with privacy laws protecting EU citizens by regulating the way US companies would handle their data. The loss of confidence in US firms from EU consumers may end up materially affecting US businesses. How to devise strategies that balance privacy protection, benefits from information sharing, business interests, and national security will likely remain a thorny and yet vital subject of research for years to come.

[34] See https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

4.4 *Conclusions*

One of the themes emerging from this review is that both the sharing and the protecting of personal data can have positive and negative consequences at both the individual and societal levels. On the one hand, personal information has both private and commercial value, and the sharing of data—as highlighted by both theoretical models and empirical studies—may reduce frictions in the market and facilitate transactions. On the other hand, the claimed societal benefits of data sharing have not always been vetted and confirmed. For instance, the ability of Google Flu Trends to correctly estimate influenza activity—which has often been heralded as an example of the power of big data (Goel et al. 2010), and which we cited in the introduction of this review—was later challenged (Butler 2013). Researchers have mentioned "Big Data Hubris" (Lazer et al. 2014) in reference to the "implicit assumption that big data are a substitute for, rather than a supplement to, traditional data collection and analysis." In fact, exploiting the commercial value of data can often entail a reduction in private utility, and sometimes even in social welfare overall. Thus, consumers have good reasons 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. Personal data—like all information—

is easily stored, replicated, and transferred, and regulating its acquisition and dissemination is a challenging undertaking for individuals and governments alike.

Given the fundamentally sensitive nature of personal data, it is not surprising that advancements in information technology and increased globalization of trade, investment, information flows, and security threats have brought concerns over the erosion of personal privacy to the forefront of public debate. Numerous Internet firms have collected large amounts of data from their users and either sell this data or use it to enable advertisers to target and personalize ads. While consumers can and do benefit from targeted product recommendations (Anand and Shachar 2009), they also can and do incur substantial monetary costs and disutilities from violations of their privacy (Stone 2010). Such concerns have led to new regulations across world governments, some protecting privacy (e.g., the EU Data Protection Directive, the US Children's Online Privacy Protection Act), some legalizing its erosion (for instance, by allowing trade in personal information under certain circumstances; see, e.g., the US Gramm–Leach–Bliley Act of 1999), and some suggesting the implementation of additional opt-in and opt-out controls for users (e.g., the US Federal Trade Commission's 2012 online privacy guidelines[35]).

With regulations struggling to keep pace, industry competition has been behind both new privacy-enhancing and privacy-invasive technologies. New search engines, social networks, ecommerce websites, web browsers, and individualized controls for privacy-conscious consumers have emerged. Concurrently, social media services have facilitated a culture of disclosure: disclosure of one's activities, location, emotions, work history, and political opinions. While, overall, these technologies seemingly leave privacy choices in the hands of consumers, many (if not most) consumers, in practice, lack the awareness and technical sophistication required to protect and regulate the multiple dimensions of their personal information. Privacy-invasive technological services have become integral to every-day communications, job searches, and general consumption. At the same time, privacy-protecting services require additional levels of user effort and know-how, which limits their efficacy, especially within some of the most vulnerable segments of the population.

As noted in section 3.4, extracting economic value from data and protecting privacy do not need to be antithetical goals. The economic literature we have examined clearly suggests that the extent to which personal information should be protected or shared to maximize individual or societal welfare is not a one-size-fits-all problem: the optimal balancing of privacy and disclosure is very much context dependent, and it changes from scenario to scenario. In fact, privacy guarantees may be most needed precisely when the goal is to extract benefits from the data. In the health-care realm, for instance, if privacy risks are not addressed, public concern might end up outweighing public support for initiatives that rely on extensive collection of patients' medical records (Kohane 2015). Thus, it stands to reason that, case by case, diverse combinations of regulatory interventions, technological solutions, and economic incentives could ensure the balancing of protection and sharing that increases individual and societal welfare.

We have, in this article, attempted to survey and rationalize the extant research on the economics of privacy. Because privacy is a multifaceted concept, our survey has delved into numerous literatures across a variety of disciplines and fields, from marketing to economics to computer science. While this

[35] See http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

study is certainly not exhaustive, we believe it highlights some of the most relevant historical and current research on the topic. It is, however, abundantly evident that protection of personal privacy is rapidly emerging as one of the most significant public policy issues, and research on the economics of privacy will, therefore, continue to expand and evolve in coming years.

References

Acquisti, Alessandro. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification." In *EC '04: Proceedings of the 5th ACM Conference on Electronic Commerce*, 21–29. New York: Association for Computing Machinery.

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2015. "Privacy and Human Behavior in the Age of Information." *Science* 347 (6221): 509–14.

Acquisti, Alessandro, and Christina M. Fong. 2013. "An Experiment in Hiring Discrimination via Online Social Networks." Paper presented at the Twelfth Workshop on the Economics of Information Security, Washington, DC, June 12.

Acquisti, Alessandro, Allan Friedman, and Rahul Telang. 2006. "Is There a Cost to Privacy Breaches? An Event Study." Presented at the Twenty-Seventh International Conference on Information Systems, Milwaukee 2006 and Workshop on the Economics of Information Security 2006.

Acquisti, Alessandro, and Ralph Gross. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." *Privacy Enhancing Techniques* 4258: 36–58.

Acquisti, Alessandro, and Ralph Gross. 2009. "Predicting Social Security Numbers from Public Data." *Proceedings of the National Academy of Sciences* 106 (27): 10975–80.

Acquisti, Alessandro, Leslie K. John, and George Loewenstein. 2013. "What Is Privacy Worth?" *Journal of Legal Studies* 42 (2): 249–74.

Acquisti, Alessandro, and Hal R. Varian. 2005. "Conditioning Prices on Purchase History." *Marketing Science* 24 (3): 367–81.

Adjerid, Idris, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2013. "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency." In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 1–11. New York: Association for Computing Machinery.

Adjerid, Idris, Alessandro Acquisti, Rahul Telang, Rema Padman, and Julia Adler-Milstein. Forthcoming. "The Impact of Privacy Regulation and Technology Incentives: The Case of Health Information Exchanges." *Management Science*.

Akerlof, George A. 1970. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *Quarterly Journal of Economics* 84 (3): 488–500.

Altman, Irwin. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Pacific Grove, CA: Brooks/Cole Publishing.

Anand, Bharat N., and Ron Shachar. 2009. "Targeted Advertising as a Signal." *Quantitative Marketing and Economics* 7 (3): 237–66.

Anderson, Eric T., and Duncan I. Simester. 2010. "Price Stickiness and Customer Antagonism." *Quarterly Journal of Economics* 125 (2): 729–65.

Anderson, Keith B., Erik Durbin, and Michael A. Salinger. 2008. "Identity Theft." *Journal of Economic Perspectives* 22 (2): 171–92.

Anderson, Ross, and Tyler Moore. 2006. "The Economics of Information Security." *Science* 314 (5799): 610–13.

Anderson, Simon P., and Andre de Palma. 2012. "Competition for Attention in the Information (Overload) Age." *RAND Journal of Economics* 43 (1): 1–25.

Ariès, P. 1987. *A History of Private Life*. Cambridge, MA: Harvard University Press.

Armstrong, Mark, John Vickers, and Jidong Zhou. 2009. "Consumer Protection and the Incentive to Become Informed." *Journal of the European Economic Association* 7 (2–3): 399–410.

Armstrong, Mark, and Jidong Zhou. 2010. "Conditioning Prices on Search Behaviour." Munich Personal RePEc Archive Paper 19985.

Arrow, Kenneth J. 1962. "The Economic Implications of Learning By Doing." *Review of Economic Studies* 29 (3): 155–73.

Asplund, Marcus, Rickard Eriksson, and Niklas Strand. 2008. "Price Discrimination in Oligopoly: Evidence from Regional Newspapers." *Journal of Industrial Economics* 56 (2): 333–46.

Athey, Susan, Emilio Calvano, and Joshua Gans. 2013. "The Impact of the Internet on Advertising Markets for News Media." University of Toronto Rotman School of Management Working Paper 2180851.

Athey, Susan, and Joshua S. Gans. 2010. "The Impact of Targeting Technology on Advertising Markets and Media Competition." *American Economic Review* 100 (2): 608–13.

Bapna, Ravi, Jui Ramaprasad, Galit Shmueli, and Akhmed Umyarov. Forthcoming. "One-Way Mirrors in Online Dating: A Randomized Field Experiment." *Management Science*.

Baumer, David L., Julia B. Earp, and J. C. Poindexter. 2004. "Internet Privacy Law: A Comparison between the United States and the European Union." *Computers and Security* 23 (5): 400–412.

Baye, Michael R., and John Morgan. 2001. "Information Gatekeepers on the Internet and the Competitiveness of Homogeneous Product Markets." *American Economic Review* 91 (3): 454–74.

Bendrath, Ralf, and Milton Mueller. 2011. "The End of the Net as We Know It? Deep Packet Inspection and Internet Governance." *News Media & Society* 13 (7): 1142–60.

Bennett, Colin J., and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global*

Perspective. Cambridge, MA: MIT Press.
Berendt, Bettina, Oliver Gunther, and Sarah Spiekermann. 2005. "Privacy in e-Commerce: Stated Preferences vs. Actual Behavior." *Communications of the ACM* 48 (4): 101–06.
Bergemann, Dirk, and Alessandro Bonatti. 2011. "Targeting in Advertising Markets: Implications for Offline versus Online Media." *RAND Journal of Economics* 42 (3): 417–43.
Bergemann, Dirk, and Alessandro Bonatti. 2015. "Selling Cookies." *American Economic Journal: Microeconomics* 7 (3): 259–94.
Berners-Lee, Tim. 2000. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*. New York: HarperCollins Publishers.
Berthold, Stefan, and Rainer Böhme. 2010. "Valuating Privacy with Option Pricing Theory." In *Economics of Information Security and Privacy*, edited by Tyler Moore, David Pym, and Christos Ioannidis, 187–209. New York: Springer.
Bertrand, Marianne, and Sendhil Mullainathan. 2004. "Are Emily and Greg More Employable than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination." *American Economic Review* 94 (4): 991–1013.
Blake, Thomas, Chris Nosko, and Steven Tadelis. 2015. "Consumer Heterogeneity and Paid Search Effectiveness: A Large-Scale Field Experiment." *Econometrica* 83 (1): 155–74.
Blanchette, Jean-Francois, and Deborah G. Johnson. 2002. "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness." *Information Society* 18 (1): 33–45.
Blattberg, Robert C., and John Deighton. 1991. "Interactive Marketing: Exploiting the Age of Addressability." *MIT Sloan Management Review* 33 (1): 5–14.
Blumstein, Alfred, and Kiminori Nakamura. 2009. "Redemption in the Presence of Widespread Criminal Background Checks." *Criminology* 47 (2): 327–59.
Board, Simon, and Jay Lu. 2015. "Competitive Information Disclosure in Search Markets." Unpublished.
Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives* 29 (2): 213–38.
Bottero, Margherita, and Giancarlo Spagnolo. 2013. "Limited Credit Records and Market Outcomes." Bank of Italy Working Paper 903.
Boyd, Danah, and Alice Marwick. 2011. "Social Steganography: Privacy in Networked Publics." Paper presented at the International Communication Association Conference, Boston, MA, May 28.
Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. 2013. "Misplaced Confidences: Privacy and the Control Paradox." *Social Psychological and Personality Science* 4 (3): 340–47.
Burke, Jeremy M., Curtis R. Taylor, and Liad Wagman. 2012. "Information Acquisition in Competitive Markets: An Application to the US Mortgage Market." *American Economic Journal: Microeconomics* 4 (4): 65–106.
Burton, Paul R., et al. 2007. "Genome-Wide Association Study of 14,000 Cases of Seven Common Diseases and 3,000 Shared Controls." *Nature* 447 (7145): 661–78.
Bushway, Shawn D. 2004. "Labor Market Effects of Permitting Employer Access to Criminal History Records." *Journal of Contemporary Criminal Justice* 20 (3): 276–91.
Butler, Declan. 2013. "When Google Got Flu Wrong." *Nature* 494 (7436): 155.
Calo, Ryan. 2011. "The Boundaries of Privacy Harm." *Indiana Law Journal* 86 (3): 1131–62.
Calo, Ryan. 2014. "Digital Market Manipulation." *George Washington Law Review* 82 (4): 995–1051.
Calzolari, Giacomo, and Alessandro Pavan. 2006. "On the Optimality of Privacy in Sequential Contracting." *Journal of Economic Theory* 130 (1): 168–204.
Campbell, James, Avi Goldfarb, and Catherine Tucker. 2015. "Privacy Regulation and Market Structure." *Journal of Economics and Management Strategy* 24 (1): 47–73.
Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market." *Journal of Computer Security* 11 (3): 431–48.
Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 2004. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers." *International Journal of Electronic Commerce* 9 (1): 69–104.
Chellappa, Ramnath K., and Shivendu Shivendu. 2010. "Mechanism Design for 'Free' but 'No Free Disposal' Services: The Economics of Personalization under Privacy Concerns." *Management Science* 56 (10): 1766–80.
Chen, Yongmin. 1997. "Paying Customers to Switch." *Journal of Economics and Management Strategy* 6 (4): 877–97.
Chen, Yuxin, and Ganesh Iyer. 2002. "Consumer Addressability and Customized Pricing." *Marketing Science* 21 (2): 197–208.
Chen, Yuxin, Chakravarthi Narasimhan, and Z. John Zhang. 2001. "Individual Marketing with Imperfect Targetability." *Marketing Science* 20 (1): 23–41.
Chen, Yuxin, and Z. John Zhang. 2009. "Dynamic Targeted Pricing with Strategic Consumers." *International Journal of Industrial Organization* 27 (1): 43–50.
Cheney, Julia S. 2005. "Identity Theft: Do Definitions Still Matter?" Federal Reserve Bank of Philadelphia Payments Cards Center Discussion Paper 05-10.
Chiou, Lesley, and Catherine Tucker. 2014. "Search Engines and Data Retention: Implications for Privacy and Antitrust." Massachusetts Institute of Technology Sloan School Working Paper 5094-14.
Coase, Ronald H. 1960. "The Problem of Social Cost." *Journal of Law and Economics* 3: 1–44.
Coggeshall, Stephen. 2007. "ID Theft Knows No Boundaries." http://www.technewsworld.com/story/56864.html.

Conitzer, Vincent, Curtis R. Taylor, and Liad Wagman. 2012. "Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases." *Marketing Science* 31 (2): 277–92.

Cowan, Simon. 2007. "The Welfare Effects of Third-Degree Price Discrimination with Nonlinear Demand Functions." *RAND Journal of Economics* 38 (2): 419–28.

Culnan, Mary J., and Pamela K. Armstrong. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization Science* 10 (1): 104–15.

Daughety, Andrew F., and Jennifer F. Reinganum. 2010. "Public Goods, Social Pressure, and the Choice between Privacy and Publicity." *American Economic Journal: Microeconomics* 2 (2): 191–221.

de Corniere, Alexandre. Forthcoming. "Search Advertising." *American Economic Journal: Microeconomics*.

de Corniere, Alexandre, and Romain De Nijs. 2014. "Online Advertising and Privacy." http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2191124.

Diamond, Peter. 1971. "A Model of Price Adjustment." *Journal of Economic Theory* 3 (2): 156–68.

Dinev, Tamara, and Paul Hart. 2006. "An Extended Privacy Calculus Model for e-Commerce Transactions." *Information Systems Research* 17 (1): 61–80.

Djankov, Simeon, Caralee McLiesh, and Andrei Shleifer. 2007. "Private Credit in 129 Countries." *Journal of Financial Economics* 84 (2): 299–329.

Dugas, Andrea Freyer, et al. 2012. "Google Flu Trends: Correlation with Emergency Department Influenza Rates and Crowding Metrics." *Clinical Infectious Diseases* 54 (4): 463–69.

Duncan, George T., and S. Lynne Stokes. 2004. "Disclosure Risk vs. Data Utility: The R–U Confidentiality Map as Applied to Topcoding." *Chance* 17 (3): 16–20.

Dwork, Cynthia. 2006. "Differential Privacy." In *Automata, Languages and Programming*, edited by Michele Bugliesi et al., 1–12. Berlin: Springer.

Dziuda, Wioletta, and Ronen Gradwohl. 2015. "Achieving Cooperation under Privacy Concerns." *American Economic Journal: Microeconomics* 7 (3): 142–73.

Edelman, Benjamin, and Michael Luca. 2014. "Digital Discrimination: The Case of Airbnb.com." Harvard Business School, Negotiation, Organizations & Markets Unit Working Paper 14-054.

Einav, Liran, Mark Jenkins, and Jonathan Levin. 2013. "The Impact of Credit Scoring on Consumer Lending." *RAND Journal of Economics* 44 (2): 249–74.

Evans, David S. 2009. "The Online Advertising Industry, Economics, Evolution, and Privacy." *Journal of Economic Perspectives* 23 (3): 37–60.

Executive Office of the President, President's Council of Advisors on Science and Technology. 2014. "Report to the President: Big Data and Privacy: A Technological Perspective." Washington, DC: Executive Office of the President.

Farahat, Ayman, and Michael Bailey. 2012. "How Effective Is Targeted Advertising?" In *Proceedings of the 21st International Conference on World Wide Web*, 111–20. New York: Association for Computing Machinery.

Farrell, Joseph. 1987. "Information and the Coase Theorem." *Journal of Economic Perspectives* 1 (2): 113–29.

Farrell, Joseph. 2012. "Can Privacy Be Just Another Good?" *Journal on Telecommunications and High Technology Law* 10 (2): 251–64.

Federal Trade Commission. 2012. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers." https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

Feri, Francesco, Caterina Giannetti, and Nicola Jentzsch. 2016. "Disclosure of Personal Information under Risk of Privacy Shocks." *Journal of Economic Behavior and Organization* 123: 138–48.

Fienberg, Stephen E., Alessandro Rinaldo, and Xiaolin Yang. 2010. "Differential Privacy and the Risk-Utility Tradeoff for Multi-dimensional Contingency Tables." *Privacy in Statistical Databases* 6344: 187–99.

Finley, Klint. 2015. "Thank (or Blame) Snowden for Europe's Big Privacy Ruling." *Wired*. http://www.wired.com/2015/10/tech-companies-can-blame-snowden-data-privacy-decision/.

Fishbein, Martin, and Icek Ajzen. 1975. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA and London: Addison–Wesley Publishing Company.

Friedman, Eric J., and Paul Resnick. 2001. "The Social Cost of Cheap Pseudonyms." *Journal of Economics and Management Strategy* 10 (2): 173–99.

Fudenberg, Drew, and Jean Tirole. 1998. "Upgrades, Tradeins, and Buybacks." *RAND Journal of Economics* 29 (2): 235–58.

Fudenberg, Drew, and Jean Tirole. 2000. "Customer Poaching and Brand Switching." *RAND Journal of Economics* 31 (4): 634–57.

Garrie, Daniel B., and Rebecca Wong. 2006. "Demystifying Clickstream Data: A European and U.S. Perspective." *Emory International Law Review* 20 (2): 563–89.

Gehrig, Thomas, and Rune Stenbacka. 2007. "Information Sharing and Lending Market Competition with Switching Costs and Poaching." *European Economic Review* 51 (1): 77–99.

Gellman, Robert. 2002. "Privacy, Consumers, and Costs—How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete. https://epic.org/reports/dmfprivacy.html.

Goel, Sharad, Jake M. Hofman, Sebastien Lahaie, David M. Pennock, and Duncan J. Watts. 2010. "Predicting Consumer Behavior with Web Search." *Proceedings of the National Academy of Sciences* 107 (41): 17486–90.

Goh, Khim-Yong, Kai-Lung Hui, and Ivan P. L. Png. 2015. "Privacy and Marketing Externalities: Evidence from Do Not Call." *Management Science* 61 (12): 2982–3000.

Goldberg, Ian. 2003. "Privacy-Enhancing Technologies for the Internet, II: Five Years Later." In *Privacy Enhancing Technologies*, edited by Roger Dingledine and Paul Syverson, 1–12. New York: Springer.

Goldfarb, Avi, and Catherine E. Tucker. 2011a. "Online Display Advertising: Targeting and Obtrusiveness." *Marketing Science* 30 (3): 389–404.
Goldfarb, Avi, and Catherine E. Tucker. 2011b. "Privacy Regulation and Online Advertising." *Management Science* 57 (1): 57–71.
Goldfarb, Avi, and Catherine E. Tucker. 2012a. "Privacy and Innovation." *Innovation Policy and the Economy* 12 (1): 65–90.
Goldfarb, Avi, and Catherine E. Tucker. 2012b. "Shifts in Privacy Concerns." *American Economic Review* 102 (3): 349–53.
Goldin, Claudia, and Cecilia Rouse. 2000. "Orchestrating Impartiality: The Impact of 'Blind' Auditions on Female Musicians." *American Economic Review* 90 (4): 715–41.
Gottlieb, Daniel, and Kent Smetters. 2011. "Grade Non-disclosure." National Bureau of Economic Research Working Paper 17465.
Gradwohl, Ronen. 2014. "Voting in the Limelight." Unpublished.
Gradwohl, Ronen. 2015. "Privacy in Implementation." Unpublished.
Gradwohl, Ronen, and Omer Reingold. 2010. "Partial Exposure in Large Games." *Games and Economic Behavior* 68 (2): 602–13.
Gradwohl, Ronen, and Rann Smorodinsky. 2014. "Perception Games and Privacy." http://arxiv.org/abs/1409.1487.
Grossman, Gene M., and Carl Shapiro. 1984. "Informative Advertising with Differentiated Products." *Review of Economic Studies* 51 (1): 63–81.
Grossman, Sanford J. 1981. "The Informational Role of Warranties and Private Disclosure about Product Quality." *Journal of Law and Economics* 24 (3): 461–83.
Hagiu, Andrei, and Bruno Jullien. 2011. "Why Do Intermediaries Divert Search?" *RAND Journal of Economics* 42 (2): 337–62.
Hann, Il-Horn, Kai Lung Hui, Yee-Lin Lai, Sang-Yong Tom Lee, and Ivan P. L. Png. 2006. "Who Gets Spammed?" *Communications of the ACM* 49 (10): 83–87.
Hann, Il-Horn, Kai Lung Hui, Sang-Yong Tom Lee, and Ivan P. L. Png. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach." *Journal of Management Information Systems* 24 (2): 13–42.
Hann, Il-Horn, Kai Lung Hui, Sang-Yong Tom Lee, and Ivan P. L. Png. 2008. "Consumer Privacy and Marketing Avoidance: A Static Model." *Management Science* 54 (6): 1094–1103.
Harrell, Erika. 2015. "Victims of Identity Theft, 2014." Washington, DC: US Department of Justice Bureau of Justice Statistics.
Harris, Louis, and Alan F. Westin. 1992. "The Equifax Canada Report on Consumers and Privacy in the Information Age." Anjou, Quebec: Equifax Canada.
Hayek, Friedrich A. 1945. "The Use of Knowledge in Society." *American Economic Review* 35 (4): 519–30.
Heffetz, Ori, and Katrina Ligett. 2013. "Privacy and Data-Based Research." National Bureau of Economic Research Working Paper 19433.
Hermalin, Benjamin E., and Michael L. Katz. 2006. "Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy." *Quantitative Marketing and Economics* 4 (3): 209–39.
Hillestad, Richard, et al. 2005. "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs." *Health Affairs* 24 (5): 1103–17.
Hirshleifer, Jack. 1971. "The Private and Social Value of Information and the Reward to Inventive Activity." *American Economic Review* 61 (4): 561–74.
Hirshleifer, Jack. 1980. "Privacy: Its Origin, Function, and Future." *Journal of Legal Studies* 9 (4): 649–64.
Hitsch, Gunter J., Ali Hortaçsu, and Dan Ariely. 2010. "Matching and Sorting in Online Dating." *American Economic Review* 100 (1): 130–63.
Hoffmann, Florian, Roman Inderst, and Marco Ottaviani. 2014. "Persuasion through Selective Disclosure: Implications for Marketing, Campaigning, and Privacy Regulation." Unpublished.
Hoofnagle, Chris Jay, Ashkan Soltani, Nathaniel Good, and Dietrich J. Wambach. 2012. "Behavioral Advertising: The Offer You Cannot Refuse." *Harvard Law & Policy Review* 6: 273.
Hoofnagle, Chris Jay, and Jennifer M. Urban. 2014. "Alan Westin's Privacy Homo Economicus." *Wake Forest Law Review* 49 (261).
Hui, Kai-Lung, and Ivan P. L. Png. 2006. "The Economics of Privacy." In *Handbooks in Information Systems: Volume 1: Economics and Information Systems*, edited by Terrence Hendershott, 471–98. Bingley, UK: Emerald.
Jamal, Karim, Michael Maier, and Shyam Sunder. 2003. "Privacy in e-Commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market." *Journal of Accounting Research* 41 (2): 285–309.
Jappelli, Tulio, and Marco Pagano. 2002. "Information Sharing, Lending and Defaults: Cross-Country Evidence." *Journal of Banking and Finance* 26 (10): 2017–45.
Jensen, Carlos, and Colin Potts. 2004. "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 471–78. New York: Association for Computing Machinery.
Jentzsch, Nicola. 2006. *The Economics and Regulation of Financial Privacy*. New York: Springer.
Jentzsch, Nicola, Soren Preibusch, and Andreas Harasser. 2012. "Study on Monetising Privacy: An Economic Model for Pricing Personal Information." Berlin: European Network and Information Security Agency.
Jeong, Yuncheol, and Masayoshi Maruyama. 2009. "Commitment to a Strategy of Uniform Pricing in a Two-Period Duopoly with Switching Costs." *Journal of Economics* 98 (1): 45–66.
Jernigan, Carter, and Behram F. T. Mistree. 2009.

"Gaydar: Facebook Friendships Expose Sexual Orientation." *First Monday* 14 (10).

Jing, Bing. 2011. "Pricing Experience Goods: The Effects of Customer Recognition and Commitment." *Journal of Economics and Management Strategy* 20 (2): 451–73.

John, Leslie K., Alessandro Acquisti, and George Loewenstein. 2011. "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information." *Journal of Consumer Research* 37 (5): 858–73.

Johnson, Eric J., and Daniel G. Goldstein. 2004. "Defaults and Donation Decisions." *Transplantation* 78 (12): 1713–16.

Johnson, Justin P. 2013. "Targeted Advertising and Advertising Avoidance." *RAND Journal of Economics* 44 (1): 128–44.

Kahn, Charles M., James McAndrews, and William Roberds. 2000. "A Theory of Transactions Privacy." Federal Reserve Bank of Atlanta Working Paper 2000-22.

Kahn, Charles M., James McAndrews, and William Roberds. 2005. "Money Is Privacy." *International Economic Review* 46 (2): 377–99.

Kahn, Charles M., and William Roberds. 2008. "Credit and Identity Theft." *Journal of Monetary Economics* 55 (2): 251–64.

Kang, Ruogu, Stephanie Brown, and Sara Kiesler. 2013. "Why Do People Seek Anonymity on the Internet? Informing Policy and Design." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2657–66. New York: Association for Computing Machinery.

Kearns, Michael, Mallesh M. Pai, Aaron Roth, and Jonathan Ullman. 2014. "Mechanism Design in Large Games: Incentives and Privacy." *American Economic Review* 104 (5): 431–35.

Kim, Byung-Cheoi, and Jay Pil Choi. 2010. "Customer Information Sharing: Strategic Incentives and New Implications." *Journal of Economics and Management Strategy* 19 (2): 403–33.

Kim, Jin-Hyuk, and Liad Wagman. 2015. "Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis." *RAND Journal of Economics* 46 (1): 1–22.

Kim, Jin-Hyuk, Liad Wagman, and Abraham Wickelgren. 2016. "The Impact of Access to Consumer Data on the Competitive Effects of Horizontal Mergers." http://ssrn.com/abstract=2728378.

Knight, Frank H. 1921. *Risk, Uncertainty, and Profit*. New York: Hart, Schaffner and Marx.

Ko, Myung, and Carlos Dorantes. 2006. "The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation." *Journal of Information Technology Management* 17 (2): 13–22.

Kohane, Isaac S. 2015. "Ten Things We Have to Do to Achieve Precision Medicine." *Science* 349 (6243): 37–38.

Komarova, Tatiana, Denis Nekipelov, and Evgeny Yakovlev. 2015. "Estimation of Treatment Effects from Combined Data: Identification versus Data Security." In *Economic Analysis of the Digital Economy*, edited by Avi Goldfarb, Shane Greenstein, and Catherine Tucker, 279–308. Chicago and London: University of Chicago Press.

Koops, B.-J., et al. 2006. "Should Self-Regulation Be the Starting Point?" In *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, edited by B.-J. Koops et al., 121. The Hague: TMC Asser Press.

Kramer, Adam D. I., Jamie E. Guillory, and Jeffrey T. Hancock. 2014. "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks." *Proceedings of the National Academy of Sciences* 111 (24): 8788–90.

Krishnamurthy, Balachander, and Craig Wills. 2009. "Privacy Diffusion on the Web: A Longitudinal Perspective." In *Proceedings of the 18th International Conference on World Wide Web*, 541–50. New York: Association for Computing Machinery.

Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. 2013. "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries." Presented at the Twelfth Workshop on the Economics of Information Security, Washington, DC, June 11.

Lambrecht, Anja, and Catherine Tucker. 2013. "When Does Retargeting Work? Information Specificity in Online Advertising." *Journal of Marketing Research* 50 (5): 561–76.

Lane, Julia, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, eds. 2014. *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge and New York: Cambridge University Press.

Laudon, Kenneth C. 1996. "Markets and Privacy." *Communications of the ACM* 39 (9): 92–104.

Laudon, Kenneth C. 1997. "Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information." New York University Stern School of Business Working Paper IS-97-4.

Laufer, Robert S., and Maxine Wolfe. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory." *Journal of Social Issues* 33 (3): 22–42.

Lazer, David, Ryan Kennedy, Gary King, and Alessandro Vespignani. 2014. "The Parable of Google Flu: Traps in Big Data Analysis." *Science* 343 (6176): 1203–05.

Levin, Jonathan, and Paul Milgrom. 2010. "Online Advertising: Heterogeneity and Conflation in Market Design." *American Economic Review* 100 (2): 603–07.

Lewis, Kevin. 2013. "The Limits of Racial Prejudice." *Proceedings of the National Academy of Sciences* 110 (47): 18814–19.

Lewis, Randall A., and David H. Reiley. 2014. "Online Ads and Offline Sales: Measuring the Effect of Retail Advertising via a Controlled Experiment on Yahoo!" *Quantitative Marketing and Economics* 12 (3): 235–66.

Litman, Jessica. 2000. "Information Privacy/Information Property." *Stanford Law Review* 52.

Lohr, Steve. 2010. "Privacy Concerns Limit Online Ads, Study Says." http://bits.blogs.nytimes.com/2010/04/30/privacy-concerns-limit-online-ads-study-says/.

Madden, Mary, and Lee Rainie. 2015. "Americans'

Attitudes about Privacy, Security and Surveillance." http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15 (4): 336–55.

Mann, Catherine L. 2015. "Information Lost: Will the 'Paradise' That Information Promises, to Both Consumer and Firm, Be 'Lost' on Account of Data Breaches? The Epic Is Playing Out." In *Economic Analysis of the Digital Economy*, edited by Avi Goldfarb, Shane Greenstein, and Catherine Tucker, 309–51. Chicago and London: University of Chicago Press.

Marthews, Alex, and Catherine Tucker. 2015. "Government Surveillance and Internet Search Behavior." Available at SSRN: http://dx.doi.org/10.2139/ssrn.2412564.

Mayer, Jonathan R., and John C. Mitchell. 2012. "Third-Party Web Tracking: Policy and Technology." In Proceedings of the 2012 IEEE Symposium on Security and Privacy, 413–27. Piscataway, NJ: Institute of Electrical and Electronics Engineers.

McDonald, Aleecia, and Lorrie Faith Cranor. 2008. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society* 4 (3): 540–65.

McDonald, Aleecia, and Lorrie Faith Cranor. 2010. "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising." Paper presented at the 2010 TPRC—43rd Research Conference on Communication, Information and Internet Policy, Arlington, VA, October 2.

Mikians, Jakub, Laszlo Gyarmati, Vijay Erramilli, and Nikolaos Laoutaris. 2012. "Detecting Price and Search Discrimination on the Internet." In *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*, 79–84. New York: Association for Computing Machinery.

Mikians, Jakub, Laszlo Gyarmati, Vijay Erramilli, and Nikolaos Laoutaris. 2013. "Crowd-Assisted Search for Price Discrimination in e-Commerce: First Results." In *Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*, 1–6. New York: Association for Computing Machinery.

Milberg, Sandra J., Sandra J. Burke, H. Jeff Smith, and Ernest A. Kallman. 1995. "Values, Personal Information Privacy, and Regulatory Approaches." *Communications of the ACM* 38 (12): 65–74.

Milberg, Sandra J., H. Jeff Smith, and Sandra J. Burke. 2000. "Information Privacy: Corporate Management and National Regulation." *Organization Science* 11 (1): 35–57.

Milgrom, Paul R. 1981. "Good News and Bad News: Representation Theorems and Applications." *Bell Journal of Economics* 12 (2): 380–91.

Milgrom, Paul R., and John Roberts. 1986. "Relying on the Information of Interested Parties." *RAND Journal of Economics* 17 (1): 18–32.

Miller, Amalia R., and Catherine E. Tucker. 2007. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." Paper presented at the 2007 Workshop on the Economics of Information Security, Pittsburgh, PA, June 7.

Miller, Amalia R., and Catherine E. Tucker. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." *Management Science* 55 (7): 1077–93.

Miller, Amalia R., and Catherine E. Tucker. 2011a. "Can Health Care Information Technology Save Babies?" *Journal of Political Economy* 119 (2): 289–324.

Miller, Amalia R., and Catherine E. Tucker. 2011b. "Encryption and the Loss of Patient Data." *Journal of Policy Analysis and Management* 30 (3): 534–56.

Miller, Amalia R., and Catherine E. Tucker. 2014a. "Electronic Discovery and the Adoption of Information Technology." *Journal of Law, Economics, and Organization* 30 (2): 217–43.

Miller, Amalia R., and Catherine E. Tucker. 2014b. "Privacy Protection, Personalized Medicine and Genetic Testing." http://ssrn.com/abstract=2411230.

Murphy, Richard S. 1995. "Property Rights in Personal Information: An Economic Defense of Privacy." *Georgetown Law Journal* 84: 2381.

Nagin, Daniel, and Joel Waldfogel. 1995. "The Effects of Criminality and Conviction on the Labor Market Status of Young British Offenders." *International Review of Law and Economics* 15 (1): 109–26.

Narayanan, Arvind., and Vitaly Shmatikov. 2008. "Robust De-anonymization of Large Sparse Datasets." In *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 111–25. Los Alamitos, CA: IEEE Computer Society.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79: 101–39.

Noam, Eli M. 1997. "Privacy and Self-Regulation: Markets for Electronic Privacy." In *Privacy and Self-Regulation in the Information Age*. Washington, DC: US Department of Commerce, National Telecommunications and Information Administration.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs* 41 (1): 100–126.

Nuffield Council on Bioethics. 2015. "The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues." Nuffield: Nuffield Council on Bioethics.

Odlyzko, Andrew. 2003. "Privacy, Economics, and Price Discrimination on the Internet." In *Economics of Information Security*, edited by L. Jean Camp and Stephen Lewis, 187–212. Norwell, MA: Kluwer Academic Publishers.

Ohm, Paul. 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* 57: 1701–77.

Olejnik, Lukasz, Tran Minh-Dung, and Claude Castelluccia. 2014. "Selling Off Privacy at Auction." Paper presented at ISOC Network and Distributed System Security Symposium, San Diego, CA, February 23–26.

Oster, Emily, Ira Shoulson, Kimberly Quaid, and E. Ray Dorsey. 2010. "Genetic Adverse Selection: Evidence

from Long-Term Care Insurance and Huntington Disease." *Journal of Public Economics* 94 (11–12): 1041–50.

Pagano, Marco, and Tullio Jappelli. 1993. "Information Sharing in Credit Markets." *Journal of Finance* 48 (5): 1693–1718.

Pancras, Joseph, and K. Sudhir. 2007. "Optimal Marketing Strategies for a Customer Data Intermediary." *Journal of Marketing Research* 44 (4): 560–78.

Pavan, Alessandro, and Giacomo Calzolari. 2009. "Sequential Contracting with Multiple Principals." *Journal of Economic Theory* 144 (2): 503–31.

Png, Ivan P. L. 2010. "On the Value of Privacy from Telemarketing: Evidence from the 'Do Not Call' Registry." Unpublished.

Posner, Richard A. 1978. "The Right of Privacy." *Georgia Law Review* 12 (3): 393–422.

Posner, Richard A. 1981. "The Economics of Privacy." *American Economic Review* 71 (2): 405–09.

Posner, Richard A. 1993. "Blackmail, Privacy, and Freedom of Contract." *University of Pennsylvania Law Review* 141 (5): 1817–47.

Preibusch, Soren, Dorothea Kubler, and Alastair R. Beresford. 2013. "Price versus Privacy: An Experiment into the Competitive Advantage of Collecting Less Personal Information." *Electronic Commerce Research* 13 (4): 423–55.

Qian, Jun, and Philip E. Strahan. 2007. "How Laws and Institutions Shape Financial Contracts: The Case of Bank Loans." *Journal of Finance* 62 (6): 2803–34.

Rainie, Lee, Sara Kiesler, Ruogu Kang, and Mary Madden. 2013. "Anonymity, Privacy, and Security Online." Washington, DC: Pew Research Center.

Rao, Justin M., and David H. Reiley. 2012. "The Economics of Spam." *Journal of Economic Perspectives* 26 (3): 87–110.

Roberds, William, and Stacey L. Schreft. 2009. "Data Security, Privacy, and Identity Theft: The Economics behind the Policy Debates." *Federal Reserve Bank of Chicago Economic Perspectives* First Quarter: 22–30.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management* 30 (2): 256–86.

Rosen, Jeffrey. 2012. "The Right to Be Forgotten." *Stanford Law Review Online* 64: 88.

Rubin, Paul H., and Thomas M. Lenard. 2001. *Privacy and the Commercial Use of Personal Information*. New York: Springer, Kluwer Academic.

Rust, Roland T., P. K. Kannan, and Na Peng. 2002. "The Customer Economics of Internet Privacy." *Journal of the Academy of Marketing Science* 30 (4): 455–64.

Samuelson, Pamela. 2000. "Privacy as Intellectual Property." *Stanford Law Review* 52: 1125–73.

Savage, Scott J., and Donald M. Waldman. 2013. "The Value of Online Privacy." Unpublished.

Schenk, Eric, and Claude Guittard. 2011. "Toward a Characterization of Crowdsourcing Practices." *Journal of Innovation Economics and Management* 7: 93–107.

Schoeman, Ferdinand David, ed. 1984. *Philosophical Dimensions of Privacy: An Anthology*. Cambridge and New York: Cambridge University Press.

Schoeman, Ferdinand David. 1992. *Privacy and Social Freedom*. Cambridge and New York: Cambridge University Press.

Schwartz, Paul M. 1997. "Privacy and the Economics of Personal Health Care Information." *Texas Law Review* 76 (1): 1–75.

Schwartz, Paul M. 2004. "Property, Privacy, and Personal Data." *Harvard Law Review* 117: 2056–2128.

Schwartz, Paul M., and Edward J. Janger. 2007. "Notification of Data Security Breaches." *Michigan Law Review* 105: 913–84.

Shaffer, Greg, and Z. John Zhang. 1995. "Competitive Coupon Targeting." *Marketing Science* 14 (4): 395–416.

Shaffer, Greg, and Z. John Zhang. 2002. "Competitive One-to-One Promotions." *Management Science* 48 (9): 1143–60.

Shy, Oz, and Rune Stenbacka. Forthcoming. "Customer Privacy and Competition." *Journal of Economics and Management Strategy*.

Smith, Richard M. 1999. "The Web Bug FAQ." https://w2.eff.org/Privacy/Marketing/web_bug.html.

Smith, Robert Ellis. 2000. *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Privacy Journal.

Solove, Daniel J. 2003. "Identity Theft, Privacy, and the Architecture of Vulnerability." *Hastings Law Journal* 54: 1227–75.

Solove, Daniel J. 2006. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (3): 477–560.

Solove, Daniel J. 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven and London: Yale University Press.

Solove, Daniel J. 2013. "Introduction: Privacy Self-management and the Consent Dilemma." *Harvard Law Review* 126 (7): 1880–903.

Spence, Michael. 1973. "Job Market Signaling." *Quarterly Journal of Economics* 87 (3): 355–74.

Spiegel, Yossi. 2013. "Commercial Software, Adware, and Consumer Privacy." *International Journal of Industrial Organization* 31 (6): 702–13.

Stigler, George J. 1961. "The Economics of Information." *Journal of Political Economy* 69 (3): 213–25.

Stigler, George J. 1962. "Information in the Labor Market." *Journal of Political Economy* 70 (5): 94–105.

Stigler, George J. 1980. "An Introduction to Privacy in Economics and Politics." *Journal of Legal Studies* 9 (4): 623–44.

Stone, Brad. 2010. "Ads Posted on Facebook Strike Some as Off-Key." *New York Times*, March 4, B1.

Stone, E. F., and D. L. Stone. 1990. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms." *Research in Personnel and Human Resources Management* 8 (3): 349–411.

Strahilevitz, Lior Jacob. 2008. "Privacy versus Antidiscrimination." *University of Chicago Law Review* 75 (1): 363–81.

Stutzman, Fred, Ralph Gross, and Alessandro Acquisti. 2012. "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook." *Journal of Privacy and*

Confidentiality 4 (2): 7–41.
Sweeney, Latanya. 1997. "Weaving Technology and Policy Together to Maintain Confidentiality." *Journal of Law, Medicine and Ethics* 25 (2–3): 98–110.
Sweeney, Latanya. 2013. "Discrimination in Online Ad Delivery: Google Ads, Black Names and White Names, Racial Discrimination, and Click Advertising." *ACM Queue* 11 (3): 10.
Swire, Peter P., and Robert E. Litan. 1998. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington, DC: Brookings Institution Press.
Tamir, Diana I., and Jason P. Mitchell. 2012. "Disclosing Information about the Self Is Intrinsically Rewarding." *Proceedings of the National Academy of Sciences* 109 (21): 8038–43.
Tang, Zhulei, Y. U. Hu, and Michael D. Smith. 2008. "Gaining Trust through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor." *Journal of Management Information Systems* 24 (4): 153–73.
Taylor, Curtis R. 2004. "Consumer Privacy and the Market for Customer Information." *RAND Journal of Economics* 35 (4): 631–50.
Taylor, Curtis R., and Liad Wagman. 2014. "Consumer Privacy in Oligopolistic Markets: Winners, Losers, and Welfare." *International Journal of Industrial Organization* 34: 80–84.
Telang, Rahul, and Sunil Wattal. 2007. "An Empirical Analysis of the Impact of Software Vulnerability Announcements on firm Stock Price." *IEEE Transactions on Software Engineering* 33 (8): 544–57.
Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *Information Systems Research* 22 (2): 254–68.
Tucker, Catherine E. 2012. "The Economics of Advertising and Privacy." *International Journal of Industrial Organization* 30 (3): 326–29.
Tucker, Catherine E. 2014. "Social Networks, Personalized Advertising, and Privacy Controls." *Journal of Marketing Research* 51 (5): 546–62.
Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. 2009. "Americans Reject Tailored Advertising and Three Activities That Enable It." http://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers.
Valentino-Devries, Jeremy Singer-Vine, and Ashkan Soltani. 2012. "Websites Vary Prices, Deals Based on Users' Information." *Wall St. Journal*, December 24.
Van Alstyne, Marshall W. 2007. "Curing Spam: Rights, Signals & Screens." *The Economists' Voice* 4 (2).
Van Zandt, Timothy. 2004. "Information Overload in a Network of Targeted Communication." *RAND Journal of Economics* 35 (3): 542–60.
Varian, Hal R. 1997. "Economics Aspects of Personal Privacy." In *Privacy and Self-Regulation in the Information Age*. Washington, DC: US Department of Commerce, National Telecommunications and Information Administration.
Varian, Hal R. 2010. "Computer Mediated Transactions." *American Economic Review* 100 (2): 1–10.
Varian, Hal R., Fredrik Wallenberg, and Glenn Woroch. 2005. "The Demographics of the Do-Not-Call List." *IEEE Security and Privacy* 3 (1): 34–39.
Villas-Boas, J. Miguel. 1999. "Dynamic Competition with Customer Recognition." *RAND Journal of Economics* 30 (4): 604–31.
Villas-Boas, J. Miguel. 2004. "Price Cycles in Markets with Customer Recognition." *RAND Journal of Economics* 35 (3): 486–501.
Vissers, Thomas, Nick Nikiforakis, Nataliia Bielova, and Wouter Joosen. 2014. "Crying Wolf? On the Price Discrimination of Online Airline Tickets." Paper presented at the 7th Workshop on Hot Topics in Privacy Enhancing Technologies, Amsterdam, Netherlands, July 18.
Wagman, Liad. 2014. "Good News or Bad News? Information Acquisition and Applicant Screening in Competitive Labor Markets." http://ssrn.com/abstract=2377849.
Wagman, Liad, and Vincent Conitzer. 2014. "False-Name-Proof Voting with Costs over Two Alternatives." *International Journal of Game Theory* 43 (3): 599–618.
Waldfogel, Joel. 1994. "The Effect of Criminal Conviction on Income and the Trust 'Reposed in the Workmen'." *Journal of Human Resources* 29 (1): 62–81.
Wang, Yang, et al. 2013. "The Second Wave of Global Privacy Protection: From Facebook Regrets to Facebook Privacy Nudges." *Ohio State Law Journal* 74 (6): 1307–34.
Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193–203.
Wathieu, Luc. 2002. "Privacy, Exposure and Price Discrimination." http://neumann.hec.ca/cref/sem/documents/031111.pdf.
Westin, Alan. 1967. *Privacy and Freedom*. New York: Atheneum Publishers.
White, Ryen W., Nicholas P. Tatonetti, Nigam H. Shah, Russ B. Altman, and Eric Horvitz. 2013. "Web-Scale Pharmacovigilance: Listening to Signals from the Crowd." *Journal of the American Medical Informatics Association* 20: 404–08.
White, Tiffany Barnett, Debra L. Zahay, Helge Thorbjørnsen, and Sharon Shavitt. 2008. "Getting too Personal: Reactance to Highly Personalized Email Solicitations." *Marketing Letters* 19 (1): 39–50.
Wickelgren, Abraham L. 2015. "An Economic Analysis of Internet Privacy Regulation." Unpublished.
Wilson, Kumanan, and John S. Brownstein. 2009. "Early Detection of Disease Outbreaks Using the Internet." *Canadian Medical Association Journal* 180 (8): 829–31.
Xie, Yinglian, Fang Yu, and Martin Abadi. 2009. "De-anonymizing the Internet Using Unreliable IDs." *Computer Communication Review* 39: 75–86.
Zhang, Juanjuan. 2011. "The Perils of Behavior-Based Personalization." *Marketing Science* 30 (1): 170–86.
Zuiderveen Borgesius, Frederik J. 2015. *Improving Privacy Protection in the Area of Behavioural Targeting*. New York: Wolter Kluwer Law and Business.

This article has been cited by:

1. Caleb S. Fuller. 2018. Privacy law as price control. *European Journal of Law and Economics* **45**:2, 225-250. [Crossref]
2. Ronen Gradwohl. 2018. Privacy in implementation. *Social Choice and Welfare* **50**:3, 547-580. [Crossref]
3. Chantal Lidynia, Ralf Philipsen, Martina Ziefle. The Sky?s (Not) the Limit - Influence of Expertise and Privacy Disposition on the Use of Multicopters 270-281. [Crossref]
4. Florian Morath, Johannes Münster. 2018. Online Shopping and Platform Design with Ex Ante Registration Requirements. *Management Science* **64**:1, 360-380. [Crossref]
5. Leyla Dogruel, Sven Joeckel, Jessica Vitak. 2017. The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. *Computers in Human Behavior* **77**, 230-239. [Crossref]
6. Oliver Budzinski. 2017. Wettbewerbsregeln für das Digitale Zeitalter?. *List Forum für Wirtschafts- und Finanzpolitik* **43**:3, 221-249. [Crossref]
7. Chao Li, Daniel Yang Li, Gerome Miklau, Dan Suciu. 2017. A theory of pricing private data. *Communications of the ACM* **60**:12, 79-86. [Crossref]
8. Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian, Asuman Ozdaglar. 2017. Privacy-constrained network formation. *Games and Economic Behavior* **105**, 255-275. [Crossref]
9. Steven Schmeiser. 2017. Online advertising networks and consumer perceptions of privacy. *Applied Economics Letters* **49**, 1-5. [Crossref]
10. Alessandro Acquisti, Manya Sleeper, Yang Wang, Shomir Wilson, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub. 2017. Nudges for Privacy and Security. *ACM Computing Surveys* **50**:3, 1-41. [Crossref]
11. Samant Khajuria, Knud Erik Skouby. 2017. Privacy and Economics in a 5G Environment. *Wireless Personal Communications* **95**:1, 145-154. [Crossref]
12. Alexia Gaudeul, Caterina Giannetti. 2017. The Effect of Privacy Concerns on Social Network Formation. *Journal of Economic Behavior & Organization* . [Crossref]
13. Ronen Gradwohl, Rann Smorodinsky. 2017. Perception games and privacy. *Games and Economic Behavior* **104**, 293-308. [Crossref]
14. Evert Van den Broeck, Karolien Poels, Michel Walrave. 2017. A Factorial Survey Study on the Influence of Advertising Place and the Use of Personal Data on User Acceptance of Facebook Ads. *American Behavioral Scientist* **33**, 000276421771756. [Crossref]
15. 2017. Book Reviews. *Journal of Economic Literature* **55**:2, 662-663. [Abstract] [View PDF article] [PDF with links]
16. 2017. Book Reviews. *Journal of Economic Literature* **55**:2, 644-663. [Citation] [View PDF article] [PDF with links]
17. 2017. Book Reviews. *Journal of Economic Literature* **55**:2, 660-662. [Abstract] [View PDF article] [PDF with links]

18. Oliver Budzinski, Sonja Schneider. 2017. Smart Fitness: ?konomische Effekte einer Digitalisierung der Selbstvermessung. *List Forum f?r Wirtschafts- und Finanzpolitik* **43**:2, 89-124. [Crossref]
19. Yann Balgobin, David Bounie, Martin Quinn, Patrick Waelbroeck. 2017. Payment Instruments, Financial Privacy and Online Purchases. *Review of Network Economics*, ahead of print. [Crossref]
20. Malte Dold, Tim Krieger. Informationelle Selbstbestimmung aus ordnungsökonomischer Sicht 181-198. [Crossref]
21. Grazia Cecere, Fabrice Le Guel, Matthieu Manant, Nicolas Soulié. The Economics of Privacy 1-11. [Crossref]
22. Kallia Anastasopoulou, Spyros Kokolakis, Panagiotis Andriotis. Privacy Decision-Making in the Digital Era: A Game Theoretic Review 589-603. [Crossref]
23. Sophia Kununka, Nikolay Mehandjiev, Pedro Sampaio, Konstantina Vassilopoulou. **10303**, 135. [Crossref]
24. Grazia Cecere, Fabrice Le Guel, Matthieu Manant, Nicolas Soulié. The Economics of Privacy 1-11. [Crossref]
25. Muhammad Rizwan Asghar, Gyorgy Dan, Daniele Miorandi, Imrich Chlamtac. 2017. Smart Meter Data Privacy: A Survey. *IEEE Communications Surveys & Tutorials* **19**:4, 2820-2835. [Crossref]
26. Paul Belleflamme, Wouter Vergote. 2016. Monopoly price discrimination and privacy: The hidden cost of hiding. *Economics Letters* **149**, 141-144. [Crossref]
27. Christopher Griffin, Sarah Rajtmajer, Anna Squicciarini. Invited Paper: A Model of Paradoxical Privacy Behavior in Online Users 206-211. [Crossref]