CHAPTER 20

THE ECONOMICS OF PRIVACY

LAURA BRANDIMARTE AND
ALESSANDRO ACQUISTI

1. Introduction: Why an Economics of Privacy?

In a study published in the April 2010 issue of *Continuum: Journal of Media and Cultural Studies*, Dr. Brett Mills, a senior lecturer in the School of Film and Television Studies at the University of East Anglia, U.K., raises the issue of the negation of the right to privacy to *animals* that appear in wildlife documentaries (Mills, 2010). Those animals never gave consent to their being filmed! Dr. Mills suggests that, just as it happens for human activities, a distinction between what is public and what is private should be made in the animal world. Mating, giving birth, and dying are considered extremely private activities in the human realm, but nobody is surprised to see those same activities broadcasted in a documentary involving other animals.

It may seem odd to claim that animals might have a right to privacy, considering that such right is sometimes denied to humans. As it is commonly understood, privacy is an eminently human concept, even an inviolable aspect of human dignity (Bloustein, 1964). Yet the very nature of privacy—ambiguous and idiosyncratic—creates considerable challenges for scholars who attempt to define it and circumscribe this right to certain groups or categories of data subjects. But if that is the case, how can a concept so ambiguous and idiosyncratic be analyzed through a tool so dry and analytical as the lenses of economic theory? The reason,

as we argue in this chapter, is that those ambiguities and idiosyncrasies most often reflect *trade-offs* between the opposing needs of different parties. As Noam (1997) put it (referring in particular, to *informational* privacy), "[p]rivacy is an interaction, in which the information rights of different parties collide. The issue is of control over information flow by parties that have different preferences over information permeability." And where trade-offs are, there lie opportunities for economic analysis.

In this chapter, we highlight the economic roots and nuances of the current privacy debate. We discuss how economics can help cast a light on the apparent contradictions that characterize the nature of privacy and the debates surrounding it. We start by offering an overview of privacy definitions (section 2), noting how much contemporary scholarly research and public attention focuses on issues of informational privacy. We then introduce an economics approach to understanding privacy trade-offs, discussing costs and benefits associated with the protection and revelation of personal data (section 3). Then, we examine the economic theories of privacy—from the pioneer contributions by Chicago School economists, to contemporary micro-economic and macro-economic models (section 4). Next, we discuss the empirics of privacy—the current body of research that attempts to measure the actual consequences of privacy protection, or lack thereof (section 5). Finally, we present the current body of research on privacy valuations and decision making (section 6).[1]

Before commencing our analysis, however, we note that studying the economic dimensions of privacy does not imply that privacy concerns can be solely reduced to their tangible, monetary dimensions. Issues of privacy—and even privacy trade-offs—often involve intangible, immeasurable considerations. Those considerations are no less important than the measurable dimensions of privacy trade-offs, since they relate to the crucial linkages between privacy, on one hand, and human autonomy, dignity, and freedom on the other hand.

2. The Meanings of Privacy

The meaning of privacy has evolved over time and across cultures. As Zimmerman (1989) puts it, privacy "has almost as many meanings as Hydra had heads." Two young Boston lawyers, Samuel Warren and Louis Brandeis, defined privacy as "the right to be let alone" in a seminal 1890 *Harvard Law Review* article (Warren and Brandeis, 1890). They referred, quite literally, to the need for a physical space free of external intrusions. Warren and Brandeis' definition influenced the development of much Western scholarship on privacy—but was also one that, adapting to the modifications of the boundaries between private and public naturally occurring over time, has been both extended and narrowed several times since then.

For instance, where Warren and Brandeis (1890) found an organic, unified concept of (and legal ground for) privacy rights, Prosser (1960) saw instead

a heterogeneous mix of disparate interests: a right to be free from invasions into one's solitude; a right to prevent widespread publicity of embarrassing facts about oneself; a right to be free of publicity which casts one in a false light in the public eye; and a right to control the use of one's name or image for commercial purposes. Posner (1978) went even further, suggesting that the very term "privacy" may be a misnomer, a catch-all word with which we try to capture too many differing needs and wants, ultimately depriving the term itself of actual meaning.

On the opposite side of the spectrum, Bloustein (1964) saw privacy as an aspect of "inviolate personality," what he defined "the individual's independence, dignity and integrity; it defines man's essence as a unique and self-determining being [. . .] He would be less of a man, less of a master over his own destiny" were he denied the right to protect his privacy. An invasion of private life "would destroy individual dignity and integrity and emasculate individual freedom and independence." Accordingly, privacy protection has been deemed by legal, information, and psychology scholars as an essential necessity for both individual psychological well-being and for social harmony (Agre and Rotenberg, 1997; Bellotti, 1997; Scoglio, 1998).

So many are the facets of privacy that different scientific disciplines—and scholars within a discipline—have often used the same term to refer to rather distinct (albeit related) concepts: from autonomy to confidentiality; from liberty to secrecy; from solitude to anonymity. Not even the modern, cross-disciplinarian convergence of research focused on privacy as *control and protection of personal data* has resolved the issue. In 1967, Alan Westin described privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent *information about them* is communicated to others" (Westin, 1967; emphasis added). With Western economies' transition to service-oriented information societies, issues associated with the usage of personal data (instead of one's physical space) became prominent. Yet more than forty years later, the concept was still in such a state of "disarray" (Solove, 2006) that need arose to develop a "taxonomy" of privacy to guide legislators, scholars, and policy makers through the many meanings of privacy. Solove's (2006) taxonomy attempted to achieve that goal by distinguishing different types of "harmful activities" that can create privacy problems: information collection, information processing, information dissemination, and personal invasions.

Most of the economics research on privacy *is* about informational privacy—that is, personal information and the problems and opportunities created by its collection, its processing, its dissemination, and its invasion. As Posner (1978) noted, while it may be debatable whether the concepts of privacy as "freedom" and privacy as "quiet" have significant economic implications,[2] the concept of privacy as concealment of information certainly does. Information about a person is manifestly a *signal* about that person—a signal that the individual may rationally want to alternatively share or suppress in transactions with other parties.

In short, studying privacy implies facing semantic ambiguities and contradictions. To some people privacy has a positive value in and of itself, but to others it is an ethically neutral concept, which may therefore have both positive and negative

consequences. The meaning that a person attributes to privacy may evolve over the course of her life, or may vary across different situations at a certain point in time. Expectations regarding what should be kept private change depending on factors like age, culture, or personal experiences. The same individual may accept the fact that a telephone company keeps records of his phone calls without particular concerns, but may not so blithely accept that his Internet service provider can monitor the websites he visits. Given the multifaceted nature of privacy, characterized by so many conflicts and opposing interests, economics can offer an interesting angle and useful tool for its analysis. Indeed, one of the most general objects of economic theory is to understand how an agent's utility can be maximized, and as long as a need for privacy enters the agent's utility function—either affecting it positively or negatively—economics is a good candidate for the investigation. Another fundamental purpose of economics is to examine the trade-offs that may arise in a certain transaction and to solve for the possible equilibria that may result from balancing the opposing interests of the parties involved. Thus economics provides a useful framework to address privacy issues.

3. The Economics of Privacy: Individual and Organizational Trade-Offs

The economics of privacy may be a relatively recent research field (its first scholarly writing dating back to the late 1970s and early 1980s; see section 4), but economic trade-offs arising from privacy issues are by no means a novel phenomenon.[3] With the reduction in the cost of data collection, manipulation, and use, the trade-offs of opposing economic interests have become more evident. On the Internet, the information a user reveals may be used to make the web surfing experience more pleasant and efficient, but it may also be used to maximize profit through price-discrimination (tracking a consumer's online behavior allows the inference of her preferences and the prediction of her propensity to purchase a certain product; see Acquisti and Varian, 2005). Notorious for its negative rebound on the company's reputation was Amazon's attempt, in 2001, to use customers' personal information to differentiate its offers, applying differential prices to different customers for the same product. This attempt, soon uncovered by users, was harmful for Amazon's image, and pushed the company to return the resulting gains back to customers (Streifield, 2001).

This example illustrates a general point: The economics of privacy can highlight the costs and benefits associated with the changing boundaries between public and private spheres, and in particular, with the protection and revelation of personal information. Such costs and benefits can be tangible or intangible: from the immediate gratification one derives from posting a holiday photo on a social

networking site, to the monetary damage one can incur if their personal information is breached and their identity is compromised by criminals. The costs and benefits are experienced not just by the so-called data subject (the individual the data refers to), but also by the actual or potential data holder. For instance, a supermarket chain needs to decide how much to invest into developing customer relationship marketing strategies such as loyalty cards. In doing so, the chain must consider the benefits—from improved marketing to price discrimination—they may obtain from such programs, but also the costs they may suffer if the data gained through the cards is breached, or if customers perceive the program as intrusive and react negatively to it. Furthermore, decisions regarding the usage of personal data simultaneously comprise benefits and costs. Consider, for instance, the consumer who refuses to use the grocery loyalty card the supermarket has created. She will reduce the likelihood of being tracked across purchases. This carries direct (if intangible) benefits (for instance, the psychological satisfaction of not being tracked) as well as indirect ones (for instance, the decreased probability—and therefore reduced expected costs—that her data will be exploited for annoying marketing strategies). But those benefits come at the *opportunity* cost of giving up the discount at the checkout. Or consider another example: If personal information is neither demanded nor revealed during an online transaction, the consumer keeps her privacy protected and may prevent the seller from, say, price-discriminating her; but she won't be able to enjoy personalized services or discounts and may incur costs in order to protect her personal data. As regards the seller, she may build a reputation for not intruding customers' privacy, but she will have less data available to use for targeting and marketing purposes. On the other hand, if the consumer decides to reveal her personal information, she will have customized services or discounts, but may be subject to price discrimination and will be exposed to the future risks associated with the revelation of personal data, including unsolicited marketing, credit card fraud or identity theft. The seller, on her part, will be able to provide a better service to the customer and price-discriminate her, but will have to face consumers' privacy concerns, which may deteriorate the business relationship with them.

The economics of privacy attempts to understand those costs and benefits, whether there are particular "allocations" of personal information that maximize individual and aggregate welfare, and how economic agents make decisions about those trade-offs.

4. Economic Theories of Privacy

In the years following the end of World War II, information assets became one of the most important research focuses of economics. Harking back to Friedrich Hayek, some scholars began to interpret the whole theoretical framework of

microeconomics as economics of information, starting from the fundamentally informative value of price in a market economy. However, studies specifically addressing *personal* information (and related privacy issues) only appeared in the economics literature at the end of the 1970s. Economists and jurists of the Chicago School (such as Posner and Stigler) animated the debate with their utilitarian theories and laissez-faire positions; they saw their arguments opposed by other philosophers, law scholars, or economists (such as Hirshleifer), who found in privacy more than a marketable commodity.

Law and economics scholar Posner (1978) conceived privacy primarily as information *concealment*—an individual right that is in contrast with the opposing right, equally relevant, of others to *know*. According to Posner, one of the consequences of privacy (intended as control over information about oneself) is the possibility that the individual will untruthfully represent him or herself to society. Such opportunity clearly counters the interest of those who establish a relationship with that individual to receive accurate and reliable information about him or her. Privacy may therefore have counterproductive effects for society and cause inefficiencies. (In Posner's opinion, companies, not individuals, should be the main objects of legal protection, so that they can keep information of crucial importance to their competitiveness private.) Posner pushed this argument further, concluding that the tendency to increasingly protect consumer privacy, and impose transparency obligations on corporations, is an "example of perverse government regulation of social and economic life."

Stigler (1980) similarly claimed that government interference in privacy matters, directed to protect one of the parties involved in a voluntary transaction, was redundant and sometimes amiss. As long as the standard conditions of competition apply, the amount of personal information that is revealed in a transaction results from the trade-off between privacy protection and the need for information of each party. Indeed, people may have an interest in disclosing personal data when such data depict a positive image of themselves. For instance, when applying for a loan, an individual with a reputation of being a good debtor will want his credit history to be known. On the contrary, an individual with a bad credit report will likely prefer to keep this information concealed. Therefore, keeping this type of information private will be a signal of bad reputation for the debtor, inducing the other party to apply higher prices for the services provided—in this example, the price of credit.

Stigler concluded that the existence of laws that prevent the creditor from communicating information about the debtor to others favors the debtor himself. Thus, according to Stigler, privacy protection may lower the quality, and the level of detail, of the information that can be obtained regarding economic agents—for example regarding the productivity of a worker. Consequently, the economic result is inefficient and redistributive: resources will be inefficiently used, because information about their quality is lacking, and resources of different qualities will not be possibly rewarded accordingly—which will induce those who hold such resources to invest less in quality improvements. Moreover, the result will be redistributive

because if the differences across individuals cannot be easily measured, the treatment (e.g., salary) applied to individuals of different qualities will necessarily be more homogeneous. Income redistribution from higher to lower quality workers will follow.

Posner (1981) provides a similar analysis. Keeping people away from relevant information about an individual causes inefficiencies, because it transfers the cost of possible negative characteristics of the individual to another subject (such as an employer in the labor market, or a partner in the "marriage market"). It also contributes to retarding, rather than promoting, efficient equilibria. These delays may end up negatively affecting the most productive workers' market. At the same time though, revisiting Prosser (1960), Posner recognizes the valid economic rationale of certain forms of privacy protection that are based on tort law—such as protection from appropriation of others' name or image, from the diffusion of slanderous or tendentious information, or from intrusive methods of personal information acquisition, like spying and surveillance.

Contra the Chicago School's averse view of privacy as an inefficient and redistributive economic roadblock, and taking the perspective of the social planner that wants to maximize social welfare, Hirshleifer (1971) observed that investment in (private) information gathering may be inefficient. Hirshleifer showed that the use of private information may simply have redistributive effects, resulting in overinvestment in information gathering. Even in the case where consumer information may be acquired at zero cost, the seller's private incentive to maximize profit via consumer profiling may be in contrast with the public interest. If too much (but also if too little) information is available to the seller, some consumers may get priced out of the market, and not have access to items that social efficiency would require them to be able to consume (for this, see also Varian, 1985; Hart and Tirole, 1988; Thisse and Vives, 1988; Fudenberg and Villas-Boas, 2006). Hirshleifer (1980) more directly criticized Posner and Stigler's opinions, emphasizing how the study of market interactions under the assumption that economic agents are perfectly rational utility maximizers can be a useful simplification for modeling, but it cannot adequately describe all human exchanges, such as those related to privacy. (More recently, scholars have built on these premises to start the branch of research of behavioral economics of privacy, as we discuss in section 5).

After some years of relative disinterest, privacy became again a topic of economic investigation in the late 1990s. Progress in digital information technologies on multiple fronts (the proliferation of electronic databases and personal computers, improvements in cryptographic technologies, the advent of the Internet, the diffusion of electronic mail, and growth in secondary uses of personal information) attracted the attention of economists interested in information technology (for an extensive analysis of Internet security, see chapter 21 by Anderson and Moore in this volume). Among them, Varian (1996) observes that the development of low-cost technologies for data manipulation generated new concerns for personal information processing. Nonetheless, Varian argues that simply prohibiting the diffusion of personal data would not benefit the individual. In fact, the consumer

may be willing to reveal certain pieces of information, such as her commercial preferences (so as to receive news about the products that called her attention and to avoid those that regard disliked products), and hide other pieces of information, such as her willingness to pay for a certain good. Therefore, troubles may arise when not enough useful information is exchanged. This line of reasoning echoes Stigler and Posner's approach, but Varian adds on to that, specifying the role of secondary use of private information as an externality (later taken up by Hui and Png, 2006). Even if two parties reach an agreement for exchanging personal data with each other, one party may forward those data to others, for uses that were not initially agreed upon. Such secondary use of information may entail costs for the other party involved, costs that are not internalized by the party that shares the information.

Noam (1997) elaborates on the arguments of the Chicago School. According to the Coase theorem, in order to reach efficiency in a transaction with zero costs, but where externalities are present, the initial allocation of property rights is arbitrary and ineffectual, and does not influence the final equilibrium outcome. Applying this theorem to the case of privacy, Noam suggests that, regardless of the initial allocation of rights, the prevailing party between one agent, who has an interest in protecting her private information, and another party, who on the other hand is interested in acquiring that information, will be the one whose interests at stake are higher. That is the reason why the use of cryptography (or other technologies of data protection) cannot determine the final "outcome" of the transaction—that is, the party that will have control over personal data—but only the value exchanged between the two agents involved in the transaction process. Because consumers since the mid-Nineties have had at their disposal technologies of privacy protection, their counterparts, who may want to obtain their personal information, will have to offer a sufficient compensation in exchange of their data. Noam therefore concludes that cryptography, and by extension technologies that enhance consumer privacy, may be mainly considered as means to transfer wealth to consumers.

A similar combination of technological and economic analysis can be found in Laudon (1997), who proposes the creation of "a national information market" where individuals own their personal data and can transfer the rights on those data to others in exchange for money. As already pointed out by the economists of the Chicago School, Laudon believes that the mere legal protection of privacy is outdated. Following Varian, Laudon believes that a system based on property rights over personal information may satisfy the interests of both consumers and companies; he therefore suggests a "hybrid" solution that uses the market, technology and regulation.

The economics literature on privacy of more recent years is based on formal mathematical—often microeconomic—models that solve for equilibrium in the market for privacy. At the center of inquiry is, often, an individual's preferences and willingness to pay for goods, which are considered private information. However, even though privacy intended as data confidentiality remains the core of the investigation, modern studies also expand the analysis to include the costs of

intrusions into an individual's personal sphere (such as unsolicited mail or spamming; see for instance Hann et al., 2008) and personal preferences over privacy (see for instance Tang et al., 2008).

Taylor (2004a) focuses on the market for consumers' personal information, noting that the value of that information to a company depends on the ability of the company itself to infer consumers' preferences, and thus price discriminate, that is, offer "personalized" prices that the consumer would not reject. With technologies that allow for accurate statistical inferences of such customers' preferences, social welfare critically depends on the possibility for consumers to anticipate the use of their personal information by companies. If consumers are naïve and are not aware of the power of companies to infer from their choices their willingness to pay for a given good, then the surplus generated in a transaction will only end up in the company's pockets, unless privacy protection is guaranteed by law and the exchange of consumers' personal information between companies is prohibited. If, on the other hand, consumers are aware of the ways in which companies will use their data, legal protection becomes unnecessary, since it will be in the 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, may make the company's privacy-intrusive strategies counterproductive.

Similarly, Acquisti and Varian (2005) look at the interaction between consumers and companies in a market where the latter have access to technologies that identify the former, and where the former can use technologies that prevent companies from identifying them. Their model shows that technologies of consumer tracking (such as a website's cookies) increase a company's profits only if those same technologies provide customers with additional, personalized services.

Calzolari and Pavan (2006) explicitly consider the exchange of information regarding customers between two companies that are interested in discovering the customers' willingness to pay. The authors study the effects of privacy regulation on society's economic welfare, finding that transmission of personal data from one company to another in some cases reduces the market information distortions and increases social welfare. Information disclosure is therefore not always harming to the individual; sometimes it contributes to improving the welfare of all parties involved. Moreover, companies may find it optimal to autonomously protect customers' data, even without a normative intervention by the legislator.

One may conclude from these more recent findings that the 1980s privacy claims of the Chicago School are confirmed: the market will induce an efficient dissemination of private information, with no need for regulatory intrusions. But it would be a hasty deduction. First of all, some studies (e.g. Taylor, 2004b) show that market forces are often unable to produce efficient economic outcomes. In particular, even if consumers were perfectly rational, companies may have an incentive to collect a larger amount of data than would be socially optimal from a welfare perspective, resulting in too little trade in equilibrium (in which case it may be efficient for information to remain completely private, and for companies not to search for information at all). Moreover, it has been shown that in a competitive

market with different types of consumers—and specifically, those who draw no benefit from unsolicited marketing, and those who are interested in receiving information about new products—attempts to use technologies that prevent unsolicited marketing on one side, and sellers' efforts to use direct marketing on the other, are strategic complements: the higher the attempts of consumers to protect themselves from unsolicited marketing, the higher the use of direct marketing by sellers (Hann et al., 2008).

Furthermore, Hermalin and Katz (2006) develop a model (initially based on a monopoly or monopsony scenario, but later expanded to the case of a competitive market) in which two rational agents, respectively maximizing their own expected utilities, engage in a transaction, and each party is interested in collecting information about the other. Challenging Posner and Stigler, they find that, since the flow of information between transacting agents does not always lead to symmetrically or fully informed parties, privacy protection can lead to efficient allocation equilibria, even if privacy per se does not directly enter the individuals' utility function. Moreover, the authors find that simply allocating property rights over one's private information may not be an effective privacy policy—prohibiting information transmission may be necessary.

In addition—as the above-mentioned Taylor (2004a) shows—if information regarding consumers (in the form of customers' lists or profiles) can be resold to third parties, social efficiency may be reduced. On the one hand, social benefits will be lower because dynamic pricing (sellers varying their selling prices over time, depending on the information they are able to acquire) causes loss in trades and larger deadweight losses. Lower valuation consumers will decide not to buy. Higher valuation consumers, if they are strategic, anticipate the resale of their personal information, and will decide not to buy, if the price set by the seller is high. In this case, besides the inefficiency caused by lower social benefits, there will also be damage in the market for customer information, because the resulting customer list will be worthless. On the other hand, social costs will be higher, because sellers will have incentives to exert effort in order to gather private information about their customers.

Besides price discrimination and reduction in social welfare caused by resale to third parties, individuals have to include another cost into consideration when analyzing the trade-offs involved in information disclosure. As suggested by Hui and Png (2006), a third way in which private information may be used is for unsolicited marketing—in person, via mail or email, telephone or fax—which constitutes a direct externality to the advantage of companies and to the inconvenience of individuals. A recent study by Ferris Research estimated that in 2009 the cost of spam—use of electronic messaging systems to send unsolicited advertisement to a whole mailing list indiscriminately—was about $130 billion, $42 billion in the U.S. alone.[4] This estimate includes costs in terms of user productivity. Productivity is lowered and costs are increased by the need to divert time and effort to deleting spam, looking for false positives, using a help desk, or finding the software and hardware necessary to control spam. To these monetary costs one has to add the

psychological distress that stems from being spammed. In a related paper, Anderson and de Palma (2009) look at spamming as a problem of competition among senders (of messages) for the receiver's attention, which is a limited resource. Their model considers the costs that both parties have to incur in order to arrive to a transaction. These costs endogenously determine the number of messages sent by the sender and the number of messages read by the receiver. The authors find that if the cost of sending messages is too low, there will be a congestion problem, meaning that the receiver will only read some of the messages that she will get. In this case, a welfare-enhancing solution may be to add a small tax on the transmission of the message. Such a tax will increase total surplus, because senders who send messages of low quality will be crowded out (it would be too costly for them to send a message), therefore fewer messages will be sent and more will be actually read (a similar analysis can be found in Van Alstyne, 2007).

Targeted advertising is a form of unsolicited marketing. While spamming involves indiscriminate sending of advertisement, targeted advertising, as the name suggests, consists of contacting a selected group of recipients who, according to the information available to the sender, may be particularly interested in the advertised product or service. As Stone (2010) puts it, targeted ads "can be funny, weird or just plain creepy," especially if the recipient has no idea of the reason why she was targeted for that specific ad, or if the targeting is based on particularly sensible information. Targeted advertising can be very effective: according to a recent study by the Network Advertising Initiative, behaviorally targeted advertising generated on average almost 2.7 times the revenue per ad as non-targeted advertising in 2009.[5] 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, 2010).

Finally, some studies (e.g., Acquisti and Varian, 2005; Taylor, 2004a) suggest that if consumers are not fully rational, the market alone cannot guarantee privacy protection to individuals; companies will extract the entire surplus generated in a transaction in the absence of regulation. As we further discuss in section 6, to the companies' incentives to gather personal information one has to add the difficulties of the individual in making "optimal" decisions regarding privacy.

5. The Empirics of Privacy

In recent years, researchers' attention has been increasingly devoted to evaluating empirically the consequences of personal data disclosure and protection and to testing the explanatory power of the theories presented earlier. Empirical studies of privacy trade-offs have contributed to the debate on how to best "protect" privacy without halting the beneficial effects—for data subjects and third parties alike—of information sharing.

On one side of the debate, Gellman (2002) reports an estimate of $18 billion 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 paid by high value consumers, spam, and investments aimed at protecting data or preventing abuse). 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. For instance, targeted advertising gives consumers useful information, advertising revenues support new Internet services, and reducing online information use would ultimately be costly to consumers.

Clearly, the former side in the debate advocates regulatory solutions to privacy problems—also highlighting the complications that would arise from the interaction of different entities, each with a different privacy policy; see, for instance, Milberg et al. (2000)—while the latter privileges self-regulatory solutions. Recent recommendations to the U.S. Congress by the Federal Trade Commission (FTC, 2010), motivated by the delays with which companies have adopted appropriate privacy rules,[6] acknowledged the limitations of a self-regulatory approach. For instance, in the case of targeted advertising (or behavioral targeting), the FTC has suggested the introduction of a "do not track" mechanism, similar to the "do not call" list that became law after years of aggressive telemarketing by companies.[7] Such a do not track mechanism would be built into websites or web browsers, and would allow consumers to prohibit any data collection process about their online behavior with one click. On the one hand, currently available services that allow consumers to opt out of advertising networks (such as the Self-Regulatory Program for Online Behavioral Advertising),[8] prevent users from getting targeted ads but they do not stop advertisers or sites from collecting data. On the other hand, however, opinions differ on whether it is always improper for websites to monitor browsing behavior and target offers to visitors based on their previous behavior. The debate, therefore, is still open.

The empirical literature has focused not only on the impact of spam or targeted advertising, but also on occurrences of personal data breaches that resulted in identity theft and that, consequently, also imposed costs on companies. A data breach is an unauthorized acquisition of data, malicious or unintentional. It can be costly to both consumers and firms—especially when it leads to identity theft: in 2010, identity thefts resulted in corporate and consumer losses of around $37 billion dollars (Javelin Research, 2011). Using publicly available data, compiled byDataLossDB,[9] Romanosky et al. (2011) report that about 75 percent of recorded breaches between 2002 and 2007 were caused by hackers or external sources, and that almost 78 percent involved theft of social security numbers, a piece of personal information whose loss may lead to identity theft. The authors look at the effectiveness of data breach disclosure laws adopted by several states in America, and find that such laws have a small effect on the incidences of identity thefts and reduce the rate by just less than two percent on average. On the firms' side, Acquisti et al. (2006) try to calculate the cost to a company that suffers from a data breach using an event

study analysis. Concentrating specifically on privacy incidents—cases of exposure of personal information—due to security, policy or business failures on the side of the firm involved in the data breach event, they find that the stock market reacts negatively to the announcement of the breach. The effect of the announcement of a privacy breach on a firm's stock value is small (-0.6 percent one day after the announcement) but statistically significant. Campbell et al. (2003) find a significant and negative effect of the announcement of a data breach on stock price specifically for breaches caused by "unauthorized access of confidential information." Considering a time window of one day before and one day after the announcement of the breach, they calculate a cumulative effect of -5.4 percent. Cavusoglu et al. (2004) find that the disclosure of a security breach results in the loss of $1.65 billion of a firm's market valuation, corresponding to a cumulative effect of -2.1 percent over two days (the day of the announcement and the day after).

However, privacy breaches could occur even in absence of *data* breaches. Sometimes, voluntary self-disclosure presents unintended consequences that the individual may not have been aware of, or that she may have underestimated. This is becoming more frequent due to the popularity of Web 2.0 services, such as online social networks or blogs (section 6 analyzes the difficulties that individuals face when taking privacy-related decisions). In a recent article, Acquisti and Gross (2009) showed how apparently innocuous self-revelations made on the Internet—such as posting date and state of birth on one's social network profile—may have serious consequences in terms of privacy intrusion. The authors predicted with a margin of statistical error narrow ranges of values likely to contain individuals' social security numbers, using simply publicly available data.

6. Privacy Concerns and Decision Making

The potential risks associated with innocent online self-disclosures highlight the challenges of privacy decision making. Much recent research has dwelt upon how people value their privacy and how they make decisions about what to keep private and what to share.

Individuals' privacy preferences are profoundly affected by local customs: in the inns of many villages in Northern China, for example, it is still ordinary, just like centuries ago, to find a *kang*, or a communal brick bed, heated from underneath, that travelers share, all fully clothed and ignoring each other. Laws also play a critical role in defining what can be acceptably shared or not. For instance, privacy regulations in Europe and in the United States are vastly different. The American legislator adopts a much more decentralized approach, with rules that differ across sectors (e.g., the Health Insurance Portability and Accountability Act of 1996, regulating the health insurance sector; the Children's Online Privacy

Protection Act of 1998, regulating privacy of minors; and the Fair and Accurate Credit Transactions Act of 2003, regulating the usage of personal information in the credit sector), and with a strong tendency towards deregulation and laissez-faire. Regulations that are so different from one country to the other constitute a significant challenge for organizations that wish to operate internationally, as they will have to comply with the laws of each country in which they want to be active. One of them is Google. On November 3, 2010 Great Britain ruled that the company breached the UK law by amassing emails, Internet addresses, and passwords while collecting data for the Streetview maps service. Italy, France, Germany, Spain, and Canada started investigating the company for the same issue, while US regulators ended their probe in October 2010 after Google addressed their concerns.

What people consider private has also changed with time with the evolution of social customs and traditions, with culture and technology, and as progress modifies the boundaries between public and private. The article by Warren and Brandeis (1890) provides an example of how technological advancement modifies privacy standards. Recognizing the rotary press (a fast and efficient method of information dissemination) as a technological innovation which had the power to fundamentally modify the impact of information on society, Warren and Brandeis considered cases in which the inventions of their time could violate individuals' privacy, broadcasting details of their private life. The political, social and economic changes of American society at the time, together with fast technological progress, brought about evident benefits for the community, but also new risks, less obvious yet not negligible. That was the justification Warren and Brandeis provided for the introduction of specific laws protecting the right to privacy.

Not surprisingly, privacy expectations today are vastly different from those of 120 years ago. Carrying photo cameras around and taking pictures of strangers is ordinary nowadays, so it would not be startling at all to see oneself on the photo album of a friend's friend (not to mention how privacy expectations have changed for show business personalities, or VIPs in general). One can almost take for granted that people go around with photo shooting devices—from standard cameras to cellular phones, from watches to pens with embedded cameras—to the point that some companies have started to use this habit to their own advantage (for advertisement, for example). Walking around downtown Rome, Italy, it is not uncommon to read on billboards messages such as: "Come to our restaurant with a digital photo of this poster and you'll get 10 percent discount on your meal."

Privacy expectations have also changed as a consequence of the increasingly emphasized need for security (Trapp, 2009). The use of closed circuit video cameras in banks, museums, shops or other private properties is widespread—still, this does not seem to stop customers from going on about their business. Privacy intrusions in these cases are apparently well accepted, or at least justified by the greater good of higher perceived safety.

Furthermore, along with advancements that have made technologies more and more privacy intrusive, one can observe a recent trend involving a growing number of people willing to reveal personal information to strangers. Whether this is

due to a belief that going public makes people into celebrities, as being the object of gossip is a signal of people's interest, or that people can become rich and famous just by agreeing to have their lives constantly spied upon by the voracious eyes of the media, the success of Web 2.0 technologies such as online social networks and blogs demonstrates that people do find benefits in others (even strangers) knowing things (even embarrassing things) about them (Solove, 2007).

In some cases, there are strictly economic—and quite evident—benefits from revealing personal information. Often, online shops sell the same products at lower prices than standard offline shops, or sell products that cannot be found offline, so consumers may be willing to disclose personal information to online merchants in order to buy products at a discount or to get products with particular characteristics. Offline shops also offer products at discounted prices if customers accept to enroll in loyalty programs, which obviously require them to provide information to the seller. Moreover, providing information about one's preferences and tastes typically reduces the time and effort one has to invest in searching, allowing an easier, customized shopping experience. Whether this type of economic incentive is objectively large enough to *fairly* reward the consumer for the provision of sensible information is, however, harder to establish.

6.1. Privacy Concerns

Dinev and Hart (2003) have developed and empirically tested a model of privacy preferences, analyzing the trade-off between privacy costs and benefits of Internet transactions. The authors conclude that even though privacy concerns would tend to reduce willingness to complete transactions through the Internet, trust towards the seller and control over disclosed information contribute to generate a sense of security that may outweigh people's worries, and convince them to trade. By far outweighing the relevance of privacy statements, trust also appears to be the main driver in lowering privacy concerns when dealing with financial institutions (Tsarenko and Tojib, 2009). Consumer trust, in turn, is negatively affected by tracking mechanisms, such as cookie use, but negative reactions seem to be significantly reduced if the company discloses such usage beforehand (Miyazaki, 2008).

Focusing on the domain of direct marketing, Phelps et al. (2000) studied the trade-offs consumers face when they provide personal information in order to obtain shopping benefits. First of all, the authors find that privacy concerns strongly depend on the type of information requested, with concerns being higher for financial or purchase-related information, and lower for demographic or lifestyle interests information. Furthermore, they find that consumers' privacy concerns are highly correlated with their ability to control secondary use (and specifically, subsequent dissemination) of personal information.

Through an email survey, Sheehan and Hoy (2000) collected data regarding the dimensions and underlying factors of Internet users' privacy concerns, and confirm the result obtained by Phelps et al. (2000) that ability to control information

collection and use by third parties constitutes the primary concern among online consumers. The authors also find that, besides the FTC's core principles of fair information practices, two factors influence consumers' privacy online: "the relationships between entities and online users and the exchange of information for appropriate compensation."

Recognizing that the use of personal information by companies stimulates privacy concerns, and therefore affects purchasing intentions and behaviors, Taylor et al. (2009) show that higher perceived information control reduces the negative effect on customers' response of privacy concerns (thus increasing the likelihood of purchasing, spreading positive word-of-mouth, or expressing favorable opinions). In contrast, it seems as though the offer of compensation has no effect on the relationship between privacy concern and customers' response. However, compensation increases the salience of trust to privacy concerns, because it reinforces the seller's perceived benevolence.

Xu's (2007) has proposed a way to test whether self-regulatory or legislative solutions better satisfy individuals' privacy concerns. Her results suggest that the appropriate privacy protection device changes across individuals. Those who evaluate themselves as more independent prefer to use technology as a tool to maintain control of personal information. Those who evaluate themselves to be less independent and believe others to be powerful, influential, and responsible for events in their lives, prefer instead industry self-regulation and government legislation.

The representation of oneself as a more or less independent character may not be the only mediating factor in individuals' preferences of one type of privacy solution or the other. At least for technology-based self-regulation, computer self-efficacy (or an individual's perceptions of his or her ability to use computers in the accomplishment of a task; see Compeau and Higgins, 1995), also plays a central role, since individuals who report low self-efficacy in a certain domain will be less likely to approach that domain (Bandura, 1982; for a presentation of the theory of technology acceptance and its evolutions, see Venkatesh et al., 2003). Indeed, technology (and in particular, so-called privacy enhancing technologies; see Goldberg et al., 1997 and Goldberg, 2002) can do much to protect certain types of individuals' data while still allowing for others to be shared, with mutual benefit to data subjects and holders. However, such technologies have to be trustable and usable (Cranor and Garfinkel, 2005). Moreover, even if privacy enhancing technologies were widely accepted and properly used, they may not be effective if the individual has unstable preferences regarding privacy (see section 6.2 for an analysis of privacy decision making, and specifically, of the difficulty in defining the value of privacy).

6.2. Decision Making

Ward (2001) cautions that "measuring the value of consumer privacy may prove to be intractable," and the literature seems to confirm that, while the inferred value of private information can sometimes be very low, it varies widely with context, time, and across people—who may be more or less aware of the value of what

they are giving up. For instance, Beresford et al. (2010) find that a discount of one Euro on the online purchase of a DVD can be enough to convince students to provide date of birth and monthly income to the seller. Greenberg (2000) shows how online shoppers are typically willing to have their purchasing behavior tracked in exchange of a customized shopping experience. Citing a *Wall Street Journal* interview from 2000 with Austin Hill, then president of Zero-Knowledge Systems, a consulting company for privacy and security solutions, Shostack (2003) argues that people would also be willing to spend money in order to protect their privacy *if* the products available on the market were well understood and perceived to be effective. Indeed, the heterogeneous results obtained empirically indicate that it's problematical, if at all possible, to establish an objective value for privacy (see Acquisti and Grossklags, 2007 for an overview, and Acquisti, John, and Lowenstein, 2009 for empirical evidence of the impact of endowment effects on privacy valuations).

In other cases, the benefits from revealing personal information are not strictly economic in nature, but are still quite clear. When using a cell phone, we accept the fact that the service provider can monitor our conversations, but the convenience of being able to communicate from anywhere is worth the candle for many people. Similarly, the fact that Internet service providers can check which web pages we navigate through does not stop us from surfing the web.

There are also instances in which the benefits of giving up privacy are not so obvious. Why would people be willing to publish on the Internet embarrassing pictures of themselves? Or post compromising comments about their employer or romantic partners? It may be argued that humans are social beings by nature, so it's only natural that some feel the *need* to share and let others in, including on private things. Still, surveys administered by different organizations confirm that most people have serious concerns about online privacy protection (see Kumaraguru and Cranor, 2005 for an extensive review of publicly available Westin privacy surveys).

People's behavior may sometimes appear surprising. We may not feel comfortable talking about personal happenings to friends or relatives, but we may well end up revealing the story of our life to complete strangers (John et al., 2011). (Richard Rodriguez, a writer and public speaker, noted in his autobiography *Hunger of Memory* that "there are things so deeply personal that they can be revealed only to strangers," Rodriguez, 1982, p. 200.) Indeed, privacy scholars have uncovered an apparent paradox: a dichotomy between professed privacy attitudes and actual behavior. Consumers often voice concerns that their rights and ability to control their personal information in the marketplace are being violated.[10] However, despite those concerns, it seems as if they tend to freely provide personal data without too much alarm. For instance, Spiekerman et al., 2001 showed how even privacy privacy-conscious subjects in an experiment were generally willing to provide personal data for small discounts (see also Norberg et al., 2007). Attempting to explain the paradox, some studies have brought to light the diffuse lack of interest (or difficulties) of people in using privacy protection technologies, such as data security or Privacy Enhancing Technologies (PETs), or their apparent lack of interest in companies' privacy policies (see for example, Cranor and McDonald, 2008).[11]

Other studies underline the importance of the drives to self-disclose, which is psychologically and physically therapeutic (Pennebaker, 1997), helps strengthen human relationships (Altman and Taylor, 1973; Laurenceau et al., 1998), and satisfies exhibitionistic motivations (Miller and Shepherd, 2004; Calvert, 2000). Others have started challenging the rational agent model of privacy decision making—the premise that individuals rationally and with forethought take into account the trade-offs that are related to privacy. In the last decade, scholars have introduced new complications to the picture, coming from the realization that individuals may not always be canonically "rational." As noted by Acquisti and Grossklags (2004), decision-making processes regarding privacy are influenced and made difficult by a series of hurdles, such as incomplete information, bounded rationality (Simon, 1982), and several cognitive and behavioral biases that induce the individual to systematically deviate from a strategy that would be optimal (utility maximizing) for the theoretically rational economic agent.

As a matter of fact, the information available to individuals when making decisions regarding privacy is often incomplete, due to the externalities that Varian identified and issues of asymmetric information. (Information asymmetry in the privacy realm arises every time the data holder, who receives personal data about the data subject, knows more than the latter about the purposes and conditions of future use of those data.) Moreover, due to bounded rationality, the individual cannot obtain and retain all information necessary to make a perfectly rational decision. Even if she could access all that information, and even if she had unlimited capability of information storage and processing, her choices would nonetheless be influenced by several psychological biases and heuristics identified by psychologists and behavioral economists (see for instance Kahneman and Tversky, 2000; O'Donoghue and Rabin, 2000; Hoch and Loewenstein, 1991), such as ambiguity aversion, self-control problems, hyperbolic time discounting, illusion of control, optimism bias, default bias, and so on. All these factors influence the individual's privacy decision-making processes in such a way that even if she was willing, in theory, to protect her privacy, in practice she may not do so.

For example, when there is an immediate and certain benefit (such as a discount on the price of an item bought online, in exchange for private information of the buyer), even a privacy-conscious individual may decide to provide her personal data because the risk of any major costs arising from the disclosures (perhaps unsolicited marketing or price discrimination; or perhaps worse, credit card fraud and identity theft), is only future and uncertain.

Ultimately, even if the individual had complete control over the use of personal information, she may end up taking decisions that are contrary to her own stated preferences, or even her long-term interests. In order to help people make choices they do not stand to regret, one branch of this new literature is considering the possibility of applying "soft-paternalistic" approaches (Loewenstein et al., forthcoming) to privacy decision making (Acquisti, 2009). The idea is to guide individuals toward privacy balances that those individuals have claimed to prefer, without limiting their freedom to reveal (or to protect) more personal data.

7. Summary

When we think about privacy issues we may not necessarily and immediately associate them with economics. Privacy may be thought of as the protection of a personal sphere on which we do not want the public to intrude—something that has very little to do with money or economic choices. However, this chapter hopefully made evident that a link exists between privacy and economics. Informational privacy is, ultimately, about negotiating and harmonizing the contrasting needs of information concealment and information sharing. As we argued in our overview of the theories of economics and privacy, economics can help us understand trade-offs of a diverse nature: cost-benefit analysis, allocation of scarce resources among competing goods and services, utility maximization subject to budget constraints, profit maximization and cost minimization . . . and last but not least, privacy protection and disclosure.

At the same time, however, we have shown that standard assumptions that economists make in order to resolve these trade-offs may need to be revisited when it comes to analyzing privacy decision making. First of all, individual preferences regarding privacy are seldom well-defined, and it is not clear whether, or under which conditions, one choice is strictly better than another. Is it desirable to provide personal information to an airline in order to join their frequent flyer program and enjoy the benefits of a "preferred member?" Is it safe to provide one's credit card number to a website in order to enjoy online shopping and possibly obtain a discount? Is it appropriate to post highly personal stories or comments on a blog or an online social network that can be visited by the whole World Wide Web? Privacy preferences are not just heterogeneous across people, but often unstable for a given individual. They vary with time and context. This trait may induce apparently inconsistent behaviors or preference reversals that the standard assumption of economic rationality would have trouble explaining.

Moreover, even if privacy preferences were well-defined, privacy decision making is complex and intricate, because it involves forward-looking optimization and anticipation of future emotional states and self-control—capabilities in which human beings are notoriously limited. Regulatory or technological solutions may therefore assist individuals in making informed and, where possible, utility-maximizing decisions.

Notes

1. Related reviews of the economics literature on privacy can be found in Hui and Png (2006), as well as from one of the authors of this chapter (Acquisti 2005, 2007, and 2010 on which some of the present analysis is based).
2. Recent work on the economics of spam—unwanted advertising emails that reach the consumer's inbox: see, e.g. Hann et al., 2006—suggests that, in recent years, economists *have* started investigating issues of privacy as violation of someone's freedom or quiet.

3. For instance, as part of the 1799 U.S. Census efforts, federal agents were sent to verify the number and dimension of the windows of private citizens' homes. Public protests against the initiative focused on the issue of governmental intrusion into its citizens' private lives—but in fact what people were really contesting were the tax impositions those intrusions were designed to calculate (Smith, 2000). Even Warren and Brandeis' right to be left alone (highlighted in the previous section) is rooted in eminently economic issues: Warren and Brandeis' article was written as a reaction to the spreading practice of publishing photos of the Boston intelligentsia's social events in the evening papers. Newspapers published those photos because—in 1890 as much as today—they promised commercial success.
4. See http://www.ferris.com/2009/01/28/cost-of-spam-is-flattening-our-2009-predictions, last accessed on April 10, 2011.
5. See http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf, last accessed on April 10, 2011.
6. The report does not explicitly mention any company, but Facebook in particular has been vehemently criticized for the way it handles users' information, and specifically for transmission of user IDs to third parties. An article published on the Wall Street Journal in October 2010 uncovered a data-gathering firm, RapLeaf Inc., which had linked Facebook user ID information, obtained from Facebook applications, to its own database of Internet users, to be then re-sold.
7. The White House Privacy White Paper, released in February 2012 (White House, 2012), and concurrent announcements by Internet giants such as Google Inc. (Angwin, 2012), supporting a do not track mechanism, seem to make such a system a realistic expectation in the near future.
8. See http://www.iab.net/self-reg, last accessed on April 10, 2011.
9. See http://datalossdb.org/, last accessed on March 12, 2012.
10. The results of a Consumer Reports Poll published by the Consumer Reports National Research Center in September 2008 say that most Americans are very concerned about what is being done with their personal information online and want more control over how their information is collected and used. See http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html, last accessed on April 10, 2011.
11. Whether it is a consequence of the difficulty in correctly estimating return on investment in security (see for example "Why Invest in Security?," a study by Protegrity, a company in the market of Enterprise Data Security Management, available at http://www.protegrity.com/DataSecurityBusinessCase, last accessed on April 10, 2011), or it is a consequence of the managers' difficulties in correctly estimating risks (Romanosky, 2006), companies too may under- or over-invest in security.

References

Acquisti, A., 2005. Privacy. Rivista di Politica Economica V/VI, pp. 319–368.

Acquisti, A., 2007. Note sull' Economia della Privacy. In: Cuffaro, V., D'Orazio, R. Ricciuto, V. (Eds.), Il Codice del Trattamento dei Dati Personali, Giappichelli, pp. 907–920.

Acquisti, A., 2009. Nudging Privacy: The Behavioral Economics of Personal Information. IEEE Security and Privacy, November/December 2009, pp. 82–85.

Acquisti, A., 2010. The Economics of Personal Data and the Economics of Privacy. Background Paper for the Joint WPISP-WPIE Roundtable, "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines," OECD.

Acquisti, A., Friedman, A., Telang, R., 2006. Is There a Cost to Privacy Breaches? An Event Study. Fifth Workshop on the Economics of Information Security.

Acquisti, A., Gross, R., 2009. Predicting Social Security Numbers from Public Data. Proceedings of the National Academy of Science 106(27), pp. 10975–10980.

Acquisti A., Grossklags J., 2004. Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behaviors. In: Camp, J., Lewis, S. (Eds.), The Economics of Information Security, Springer, pp. 165–178.

Acquisti, A., Grossklags, J., 2007. When 25 Cents Is Enough: Willingness to Pay and Willingness to Accept for Personal Information. Workshop on the Economics of Information Security (WEIS).

Acquisti, A., John, L., Loewenstein, G., 2009. What is Privacy Worth? Workshop on Information Systems Economics (WISE).

Acquisti, A., Varian, H. R., 2005. Conditioning Prices on Purchase History. Marketing Science 24(3), pp. 1–15.

Agre, P. E., Rotenberg, M., 1997. Technology and Privacy: The New Landscape. MIT Press.

Altman, I., Taylor, D., 1973. Social Penetration: The Development of Interpersonal Relationships. Holt, Rinehart & Winston, New York.

Anderson, S. P., de Palma, A., 2009. Information Congestion. RAND Journal of Economics 40(4), pp. 688–709.

Angwin, J., 2012. Web Firms to Adopt 'No Track' Button. The Wall Street Journal, February 23. Available at: http://online.wsj.com/article/SB10001424052970203960804577239774264364692.html.

Bandura, A., 1982. Self-Efficacy Mechanisms in Human Agency. American Psychologist 37, pp. 122–147.

Bellotti, V., 1997. Design for Privacy in Multimedia Computing and Communications Environments. In: Agre P. E., Rotenberg, M. (Eds.), Technology and Privacy: The New Landscape, MIT Press, pp. 62–98.

Beresford, A., Kübler, D., Preibusch, S., 2010. Unwillingness to Pay for Privacy: A Field Experiment. IZA Discussion Paper No. 5017.

Bloustein, E. J., 1964. Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. New York University Law Review 39, pp. 962–1007.

Calvert, C., 2000. Voyeur Nation: Media, Privacy, and Peering in Modern Culture. Westview Press, Boulder, Colorado.

Calzolari, G., Pavan, A., 2006. On the Optimality of Privacy in Sequential Contracting. Journal of Economic Theory 30(1), pp. 168–204.

Campbell, K., Gordon, L. A., Loeb, M. P., Zhou, L., 2003. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. Journal of Computer Security 11, pp. 431–448.

Cavusoglu, H., Mishra, B., Raghunathan, S., 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), pp. 69–105.

Compeau, D. R., Higgins, C. A., 1995. Computer Self-Efficacy: Development of a Measure and Initial Test. MIS Quarterly 19(2), pp. 189–211.

Cranor, L. F., Garfinkel, S. (Eds.), 2005. Security and Usability: Designing Secure Systems that People Can Use. O'Reilly Media, Inc., Sebastopol, Calif.

Cranor, L. F., McDonald, A., 2008. The Cost of Reading Privacy Policies. ACM Transactions on Human-Computer Interaction 4(3), pp. 1–22.

Dinev, T., Hart, P, 2003. Privacy Concerns and Internet Use—A Model of Trade-off Factors. Academy of Management Meeting, Seattle.

FTC, 2010. Protecting Consumer Privacy in an Era of Rapid Change. Preliminary Staff Report.

Fudenberg, D., Villas-Boas, L. M., 2006. Behavior-based Price Discrimination and Customer Recognition. In: Hendershott, T. (Ed.), Handbooks in Information Systems (Volume 1), Economics and Information Systems, Elsevier, pp. 377–436.

Gellman, R., 2002. Privacy, Consumers, and Costs—How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete. The Digital Media Forum, Washington, D.C.

Goldberg, I., 2002. Privacy-Enhancing Technologies for the Internet, II: Five Years Later. Proceedings of the 2nd International Conference on Privacy Enhancing Technologies.

Goldberg, I., Wagner, D., Brewer, E., 1997. Privacy-Enhancing Technologies for the Internet. Proceedings of the 42nd IEEE International Computer Conference.

Greenberg, P. A., 2000. E-Shoppers Choose Personalization over Privacy. e-Commerce Times, January 4.

Hann I.H., Hui, K.L., Lee, T.S., Png, I. 2008. Consumer Privacy and Marketing Avoidance: A Static Model. Management Science 54(6), pp. 1094–1103.

Hann, I., Hui, K., Lai, Y., Lee, S. Y. T., Png, I., 2006. Who Gets Spammed? Communications of the ACM 49(10), pp. 83–87.

Hart, O. D., Tirole, J., 1988. Contract Renegotiation and Coasian Dynamics. Review of Economic Studies 55(4), pp. 509–540.

Hermalin, B., Katz, M., 2006. Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy. Quantitative Marketing and Economics 4(3), pp. 209–239.

Hirshleifer, J., 1971. The Private and Social Value of Information and the Reward to Inventive Activity. American Economic Review 61, pp. 561–574.

Hirshleifer, J., 1980. Privacy: Its Origins, Function and Future. Journal of Legal Studies 9(4), pp. 649–664.

Hoch, S. J., Loewenstein, G., 1991. Time-Inconsistent Preferences and Consumer Self-Control. Journal of Consumer Research: An Interdisciplinary Quarterly 17(4), pp. 492–507.

Hui, K., Png, I. P. L., 2006. The Economics of Privacy. In: Hendershott, T. (Ed.), Handbook on Economics and Information Systems, Elsevier, Amsterdam, The Netherlands, pp. 471–498.

Javelin Research, 2011.2011 Identity Fraud Survey Report. Javelin Strategy & Research.

John, L., Acquisti, A., Loewenstein, G., 2011. Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. Journal of Consumer Research 37(5), pp. 858–873.

Kahneman, D., Tversky, A., 2000. Choices, Values, and Frames. University Press, Cambridge.

Kumaraguru, P., Cranor, L. F., 2005. Privacy in India: Attitudes and Awareness. Proceedings of the 2005 Workshop on Privacy Enhancing Technologies.

Laudon, K. C., 1997. Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information. In: U.S. Dept. of Commerce, Privacy and Self-Regulation in the Information Age.

Laurenceau, J., Barrett, L.F., Pietromonaco, P.R., 1998. Intimacy as an Interpersonal Process: The Importance of Self-Disclosure, Partner Disclosure, and Perceived Partner Responsiveness in Interpersonal Exchanges. Journal of Personality and Social Psychology 74, pp. 1238–1251.

Loewenstein, G., John, L., Volpp, K., forthcoming. Protecting People from Themselves: Using Decision Errors to Help People Help Themselves (and Others). In: Shafir, E. (Ed.), Behavioral Foundations of Policy, Russell Sage Foundation and Princeton University Press.

Milberg, S.J., Smith, H. J., Burke, S. J., 2000. Information Privacy: Corporate Management and National Regulation. Organization Science 11, pp. 35–37.

Miller, C. R., Shepherd, D., 2004. Blogging as Social Action: A Genre Analysis of the Weblog. In: Gurak, L., Antonijevic, S., Johnson, L., Ratliff, C., Reyman, J. (Eds.), Into the Blogosphere. Available at: http://blog.lib.umn.edu/blogosphere/introduction.html.

Mills, B., 2010. Television wildlife documentaries and animals' right to privacy. Continuum: Journal of Media and Cultural Studies 24 (2), pp. 193–202.

Miyazaki, A., 2008. Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. Journal of Public Policy and Marketing 27(1), pp. 19–33.

Noam, E., 1997. Privacy and Self-Regulation: Markets for Electronic Privacy. In: U.S. Dept. of Commerce, Privacy and Self-Regulation in the Information Age.

Norberg, P. A., Horne, D. R., Horne, D. A., 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs 41(1), pp. 100–126.

O'Donoghue, T., Rabin, M., 2000. The Economics of Immediate Gratification. Journal of Behavioral Decision Making 13(2), pp. 233–250.

Pennebaker, J.W., 1997. Writing About Emotional Experiences as a Therapeutic Process. Psychological Science 8, pp. 162–166.

Phelps, J., Nowak, G. J., Ferrell, E, 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy and Marketing 19(1), pp. 27–41.

Posner, R. A., 1978. The Right of Privacy. Georgia Law Review 12(3), pp. 393–422.

Posner, R. A., 1981. The Economics of Privacy. American Economic Review 71(2), pp. 405–409.

Prosser, W., 1960. Privacy. California Law Review 48(3), pp. 383–423.

Rodriguez, R., 1982. Hunger of Memory—The Education of Richard Rodriguez. Bantam Dell, New York.

Romanosky, S., 2006. Private Sector: When It Comes to Data Security, Sweat the Little Things. Pittsburgh Post-Gazette, August 22. Available at: http://www.post-gazette.com/pg/06234/715217-28.stm.

Romanosky, S., Telang, R., Acquisti, A., 2011. Do Data Breach Disclosure Laws Reduce Identity Theft? Journal of Policy Analysis and Management 30(2), pp. 256–286.

Rubin, P. H., Lenard, T. M., 2001. Privacy and the Commercial Use of Personal Information. Kluwer Academic Publishing.

Scoglio, S., 1998. Transforming Privacy: A Transpersonal Philosophy of Rights. Praeger, Westport.

Sheehan, K., Hoy, M., 2000. Dimensions of Privacy Concern among Online Consumers. Journal of Public Policy and Marketing 19, pp. 62–75.
Shostack, A., 2003. Paying for Privacy: Consumers and Infrastructures. 2nd Annual Workshop on Economics and Information Security, Maryland.
Simon, H.A., 1982. Models of Bounded Rationality. Cambridge, Mass.: MIT Press.
Smith, R. E., 2000. Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet. Sheridan Books.
Solove, D.J., 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review 154(3), pp. 477–560.
Solove, D. J., 2007. The Future of Reputation—Gossip, Rumor, and Privacy on the Internet. New Haven & London: Yale University Press.
Spiekerman, S., Grossklags, J., Berendt, B., 2001. E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. Proceedings of the 3rd ACM Conference on Electronic Commerce.
Stigler, G. J., 1980. An Introduction to Privacy in Economics and Politics. Journal of Legal Studies 9, pp. 623–644.
Stone, B., 2010. Ads Posted on Facebook Strike Some as Off-key. New York Times, March 3.
Streifield, D., 2001. On the Web Price Tags Blur: What You Pay Could Depend on Who You Are. The Washington Post.
Tang, Z., Hu, Y.J., Smith, M., 2008. Gaining Trust through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. Journal of Management Information System 24(4), pp. 153–173.
Taylor, C. R., 2004a. Consumer Privacy and the Market for Customer Information. RAND Journal of Economics 35(4), pp. 631–650.
Taylor, C.R., 2004b. Privacy and Information Acquisition in Competitive Markets. Berkeley Program in Law and Economics, Working Paper Series.
Taylor, D.G., Davis, D.F., Jillapalli, R., 2009. Privacy Concern and Online Personalization: The Moderating Effects of Information Control and Compensation. Electronic Commerce Research 9(3), pp. 203–223.
Thisse, J., Vives, X., 1988. On the Strategic Choice of Spatial Price Policy. American Economic Review 78(1), pp. 122–137.
Trapp, R., 2009. The Debatabase Book: a Must-Have Guide for Successful Debate. New York: International Debate Education Association.
Tsarenko, Y., Tojib, D. R., 2009. Examining Customer Privacy Concerns in Dealings with Financial Institutions. Journal of Consumer Marketing 26(7), pp. 468–476.
Tucker, C., 2010. Social Networks, Personalized Advertising, and Privacy Controls. NET Institute Working Paper n. 10–07.
Van Alstyne, M.W., 2007. Curing Spam: Rights, Signals & Screens. The Economists' Voice 4(2), pp. 1–4.
Varian, H. R., 1985. Price Discrimination and Social Welfare. American Economic Review 75(4), pp. 870–875.
Varian, H. R., 1996. Economic Aspects of Personal Privacy. In: Privacy and Self-Regulation in the Information Age. National Telecommunications and Information Administration, US Department of Commerce. Available at: http://www.ntia.doc.gov/report/1997/privacy-and-self-regulation-information-age.
Venkatesh, V., Morris, M. G., Davis, G. B., Davis, F. D., 2003. User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly 27(3), pp. 425–478.

Ward, M.R., 2001. The Economics of Online Retail Markets. In: Madden, G., Savage, S. (Eds.), The International Handbook on Emerging Telecommunications Networks. Cheltenham, U.K.: Edward Elgar Publishers, pp. 92–106.

Warren, S.D., Brandeis, L.D., 1890. The Right to Privacy. Harvard Law Review 4(5), pp. 193.

Westin, A., 1967. Privacy and Freedom. Atheneum, New York.

White House, 2012. Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Available at: http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf.

Xu, H., 2007. The Effects of Self-Construal and Perceived Control on Privacy Concerns. Proceedings of 28th Annual International Conference on Information Systems, Montréal, Canada.

Zimmerman, D. L., 1989. False Light Invasion of Privacy: The Light that Failed. New York University Law Review 64, pp. 375–383.