Terrence Hendershott, Ed., *Handbooks in Information Systems, Vol. 1*

Chapter 9

The Economics of Privacy

Kai-Lung Hui
Department of Information Systems, City University of Hong Kong, Hong Kong

I.P.L. Png
Department of Information Systems, National University of Singapore, Singapore

Abstract

This chapter reviews economic analyses of privacy. We begin by scrutinizing the "free market" critique of privacy regulation. Welfare may be non-monotone in the quantity of information; hence, there may be excessive incentive to collect information. This result applies to both non-productive and productive information. Over-investment is exacerbated to the extent that personal information is exploited across markets. Further, the "free market" critique does not apply to overt and covert collection of information that directly causes harm. We then review research on property rights and challenges in determining their optimal allocation. We conclude with insights from recent empirical research and directions for future research.

1 Introduction

Information privacy has been defined as the individual's ability to control the *collection* and *use* of personal information (Westin, 1967; Stigler, 1980). The invention and development of computing technologies led to widespread concern about collection of personal information in various contexts, including employment, finance, marketing, and government. In response to these concerns, the US Congress passed the Privacy Act of 1974, the Organization for Economic Co-operation and Development (OECD) published guidelines on privacy protection and transborder data flow (OECD, 1980), and the European Union (EU) adopted Directive

95/46/EC on data protection. The EU directive prohibits transfer of information to jurisdictions that do not accord adequate protection.

The development of the Internet and the advent of e-commerce have amplified public concern about privacy. With every web site visit, a browser leaves an electronic trace which can later be retrieved to analyze the consumers' online browsing and shopping behavior. Another technology—the cookie—stores identifying information about consumers. Using clickstream and identifying information, web sites can profile visitors. Such profiling could benefit consumers by more precisely identifying their needs.[1] However, it can also be used to effect price discrimination or exclude individuals with less attractive characteristics.[2] Some organizations even sell customer information to third parties, which subject their customers to further privacy intrusion.[3,4]

Clearly, technology has significantly changed business practices, but new opportunities present new concerns. Westin (2001) concludes "There has been a well-documented transformation in consumer privacy attitudes over the past decade, moving concerns from a modest matter for a minority of consumers in the 1980s to an issue of high intensity expressed by more than three-fourths of American consumers in 2001."

Within the United States, the Federal Trade Commission (FTC) oversees personal information privacy in consumer transactions. In the 1990s, the FTC emphasized fair information practices (FIPs) in its policy toward consumer privacy. Subsequently, however, the FTC revised its thinking and considered that the cost of obtaining consumers' consent for information sharing and use would far exceed the potential benefit (Muris, 2003). According to this view, the FIPs were inefficient and the FTC should follow the approach under the Fair Credit Reporting Act of 1970. This approach generally allows the use of personal information, while focusing on enforcement against misuses. Specifically, "the most important objective of a privacy agenda should be stopping practices that can harm consumers" (Muris, 2003).

The other major privacy issue identified by Muris (2003) was spam: "Spam is one of the most daunting consumer protection problems that the

[1]See, for instance, Moe and Fader (2001, 2004), Bucklin and Sismeiro (2003), Montgomery et al. (2004), and Sismeiro and Bucklin (2004).

[2]"Giving the web a memory cost its users privacy," *New York Times*, September 4, 2001. Amazon.com's application of dynamic pricing illustrates consumers' privacy dilemma ("On the web, price tags blur; what you pay could depend on who you are," *Washington Post*, September 27, 2000).

[3]For instance, Amazon.com's privacy policy states: "As we continue to develop our business, we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets … in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets."

[4]The U.S. Federal Trade Commission (2005a) has taken enforcement action against an online shopping cart provider that rented customer information to third-party marketers, in violation of the disclosure policies published to consumers using the shopping cart.

Commission has ever faced.'' Muris worried whether legislation and legal sanctions could resolve the problem of spam.

Clearly, privacy is an important policy and business issue. What has been the contribution of academic scholarship, and in particular, economics, to the issue? Academic discourse on individual privacy dates back at least to the seminal *Harvard Law Review* article of Warren and Brandeis (1890). Privacy is a multi-disciplinary issue that has been and should be analyzed from multiple perspectives—law, psychology, sociology, political science, and economics.[5] Economics is an especially appropriate discipline as it provides a framework to appreciate the key trade-offs in policy toward privacy.

The earliest economic analyses of privacy focused on the efficiency of markets for personal information. Since the Privacy Act of 1974 regulated only government records, the immediate issue was whether the collection and use of personal information by private sector entities should be regulated. The ''Chicago School'' (Posner, 1978, 1979, 1981; Stigler, 1980) contended that regulation is not needed—markets for personal information would work as well as markets for conventional goods and services.

However, the Chicago School's argument ignored the ways in which personal information is collected. Realistically, accurate personal information does not come from nowhere; resources must be expended to collect the information, and the collection could have undesirable consequences on consumer welfare.

For the most part, the Chicago School focused on just one dimension of privacy, *viz.*, secrecy, and overlooked two other dimensions—autonomy and seclusion (Hirshleifer, 1980; Camp and Osorio, 2003). While *secrecy* concerns privacy of information, *autonomy* concerns freedom from observation and *seclusion* concerns the right to be left alone. Besides markets for secrecy, we are also interested to know whether markets for autonomy and seclusion work well.[6,7]

From an economic standpoint, governments, businesses, and other organizations use personal information about individuals in three ways. First, they use personal information to customize goods and services, discriminate more effectively between people with differing willingness to pay

[5]See, for example, Culnan and Bies (2003), Eddy et al. (1999), Goodwin (1992), Hirshleifer (1980), Laudon (1996), Petty (2000), Posner (1978, 1979, 1981), Schwartz (1968), Smith (2001), Stigler (1980), Stone and Stone (1990), Tolchinsky et al. (1981), and Woodman et al. (1982).

[6]Hirshleifer (1980) cited telemarketing as an example of violation of autonomy. Actually, telemarketing requires personal information, *viz.*, a telephone number, and involves an intrusion into the right to be left alone, hence it involves violation of secrecy and seclusion. An example that more clearly exemplifies autonomy is nude sunbathing. A peep does not need the subject's personal information to intrude on the subject's autonomy.

[7]Posner (1981) did acknowledge the definition of privacy as peace and autonomy, but he dismissed these aspects by saying ''to affix the term privacy to human freedom and autonomy (as in Jack Hirshleifer) is simply to relabel an old subject—not to identify a new area for economic research … the range of economic applications in this area seems limited.'' (p. 405)

or differing reservation wage, and sort more effectively among people with different personal characteristics (Mussa and Rosen, 1978; Katz, 1984; Moorthy, 1984; Varian, 1985; Hart and Tirole, 1988; Tirole, 1988, Chapter 3; Png, 1998, Chapter 9). The Chicago School posits that these uses of personal information lead to socially efficient outcomes and require no government regulation.

However, the use of personal information to profile individual persons imposes an *indirect* or *consequential* externality as some suffer from paying relatively higher price, receiving a relatively lower wage, or being excluded from enjoying a particular good or service. Hence, the exploitation of personal information could lead to *ex post* inefficiencies. Hirshleifer's (1971) classic analysis shows that the result of such information might simply be re-distribution, and so, from a social viewpoint, there might be over-investment in information. Even if consumer information is costless, the seller's private incentive to maximize profit may be inconsistent with maximizing social welfare. Some consumers may get priced out of the market when more information is available to the seller, even though it is socially efficient for them to consume the item (Varian, 1985; Hart and Tirole, 1988; Thisse and Vives, 1988; Fudenberg and Villas-Boas, 2006).

Second, a seller may collect personal information in one market for use by itself or others in another market. Then, the seller may have an excessive incentive to collect consumer information, at the expense of some of its own potential consumers (Taylor, 2004).[8] That is, the option of selling consumer information for extra revenue may further reduce social efficiency both from benefit (loss in trades and increase in deadweight losses) and cost (the effort in compiling the information) perspectives.

The third way in which organizations use personal information about potential clients is to direct unsolicited promotions, in person, by mail, telephone and fax, and electronically. These solicitations impose costs of intrusion on recipients and are a *direct* externality. Unsolicited marketing is one type of intrusion against seclusion (Camp and Osorio, 2003). A preference for seclusion is like a taste for privacy in that intrusions cause a direct externality, unrelated to any effect on the terms of any transaction or trading relationship (Laudon, 1996). Computing technologies have facilitated a flood of unsolicited promotions, which cause annoyance and affect productivity. However, most privacy research has ignored the implications of these uses of personal information.

Finally, opposing views on privacy and information use have led to different suggestions on whether property rights in personal information should be established and how they should be assigned. The Chicago School supports free collection and use of information; hence the issue of

[8]European Union Directive 2001/29/EC grants copyright protection to compilers of databases even if they did not create the information compiled. This right would further encourage sellers to develop consumer databases.

property rights is moot. Hermalin and Katz (2006) suggest that individuals might voluntarily reveal their personal information to trading partners anyway. Therefore, it does not matter how property rights are assigned. However, others argue that exclusive rights should be granted to individuals so that they can control the collection and subsequent use of their information (Noam, 1995b; Laudon, 1996). Marketers would then internalize the privacy costs that they impose on consumers. We examine each of these arguments and highlight some challenges in determining the optimal allocation of property rights.

This chapter reviews economic analyses of privacy. Section 2 begins with the free market approach. Sections 3 and 4 discuss the indirect consequential externality that arises from the use of personal information. Section 5 reviews direct externalities. Then, Sections 6 and 7 discuss the possible resolution of privacy through property rights and regulations. Section 8 reports some empirical findings, while Section 9 concludes with directions for future research.

2 "Free market" approach

The Chicago School (Posner, 1978, 1979, 1981; Stigler, 1980) resolutely affirms that markets for personal information would work as well as markets for conventional goods and services. Government regulation would impede economic efficiency. For instance, unskilled workers would suffer relatively more than skilled workers from restrictions on employers in the collection and use of personal information about workers. Likewise, low-income borrowers would suffer relatively more than wealthy borrowers from restrictions on lenders in the collection and use of personal information about borrowers.

The "free market" approach to privacy may not work efficiently, however, for several reasons. First, the Chicago School focuses on *ex post* efficiency, but overlooks that open and perfect information may destroy the basis for some markets with risk and asymmetric information (Hermalin and Katz, 2005). Take the insurance market as an example. If an insurer cannot distinguish persons with different health, it may offer medical insurance to healthy and unhealthy persons at the same premium. Then, what the Chicago School views as an inefficient cross-subsidy from healthy to unhealthy persons in an *ex post* sense could also be viewed as insurance against bad health in an *ex ante* sense. However, if the insurer can use personal information to distinguish persons by health level, then it would differentiate policies according to the person's health. Then, information collection would have undermined the market for insurance against bad health. The same argument applies to other markets where the "quality" on one side is private information. Examples include human resources, investments, and betting on sports.

Second, and more fundamentally, within the context of *ex post* efficiency, the Chicago School's argument works only when sellers have *perfect* information about consumers. However, welfare may not be monotone in the quantity of personal information (Hermalin and Katz, 2005). In a setting of "second-best," an increase in the quantity of personal information might reduce welfare, and accordingly, protection of privacy might raise welfare. This issue is further complicated when personal information is collected in one market for use in another.

Third, the Chicago School critique overlooks various direct externalities associated with the collection and use of personal information. These include direct marketing solicitations that overtly intrude into personal seclusion as well as covert intrusions into personal secrecy and autonomy.

The first issue (*ex ante* vs. *ex post* efficiency) is fairly trivial and we shall not elaborate it here. The second and third issues concern non-trivial production and exploitation of personal information, which are at the heart of many ongoing privacy debates. We survey recent economic advances on these two issues below.

Most economic analyses focus on *overt* collection and use of personal information, where the subject is aware that her personal information is being collected and used. Following the literature, our review will emphasize overt collection and use. Where relevant, we will also discuss covert collection and use.

3 Within-market consequential externalities

In this section, we consider how the collection and use of personal information within a single market affects the efficiency of market outcomes. The collection and use impose a consequential (rather than direct) externality. For the most part, within-market consequential externalities apply to the secrecy dimension of privacy.

Personal information is widely used to devise customized offers (products, prices, employment contracts, insurance, etc.) that better suit the tastes or characteristics of particular individuals.[9] To evaluate whether such customization promotes exchange and hence market efficiency, many economic analyses draw from the literature of asymmetric information (Akerlof, 1970; Spence, 1973; Stiglitz, 1975) and product differentiation (Mussa and Rosen, 1978; Katz, 1984; Moorthy, 1984).

In the following review, we adopt the classification of Hermalin and Katz (2006) and distinguish two classes of situation where privacy might matter. In one, personal information is *not productive*—the costs of the uninformed

[9]See, for instance, Chen et al. (2001), Chen and Iyer (2002), Acquisti and Varian (2005), Calzolari and Pavan (2005), Ghose and Chen (2003), Odlyzko (2003), Taylor (2004a) and (2004b), Wathieu (2002), Chellappa and Sin (2005), and Wattal et al. (2004).

party do not depend on the personal characteristics of the informed party as, for instance, in the case of pure price discrimination. In the other class, personal information is *productive*—the costs of the uninformed party do depend on the personal characteristics of the informed party as, for instance, in the case of an employer recruiting workers of differing skill or an insurer covering persons with differing health.

3.1 Non-productive information

Hermalin and Katz (2006) provide the simplest model of the issue. Consider a monopoly that has asymmetric information about consumers, where the consumers have either high or low valuation for some item. The marginal cost of the item is sufficiently low that it is efficient to provide to both consumer types. Generally, the seller's pricing strategy depends on its information about the consumer population. It provides a set of consumption levels from which consumers choose and thereby self-select.

Suppose that, originally, the seller sold only to the high-type consumers. Additional information would enable the seller to better sort between high and low types. If it leads the seller to sell to both types, then welfare would rise. However, suppose that, originally, the seller sold to a pool of both high and low types. If the additional information leads the seller to reduce the quantity provided to the low types, it would reduce welfare. Accordingly, privacy regulation (which would reduce the availability of personal information) might raise or reduce social welfare.

Bulow and Klemperer (2006) apply the auction theory concept of affiliation to analyze situations where competing sellers acquire different pieces of information about a consumer. While a seller will raise price against consumers with a relatively high willingness to pay for its product, it would reduce price toward consumers with relatively low willingness to pay. Other sellers would respond to the price cuts, and overall, the expected price to the consumer would be lower.

The implications of privacy regulation are more complex in a setting that unfolds over time, where consumers may make repeat purchases and sellers can condition price on the consumer's purchase history. Research into this aspect overlaps quite closely with the economics of "behavior-based price discrimination" (Fudenberg and Tirole, 2000), which is reviewed by Fudenberg and Villas-Boas (2006) in this *Handbook*. The pioneering analysis is due to Hart and Tirole (1988).

For simplicity, we present the analyses of Acquisti and Varian (2005) and Taylor (2004). As in the static case, there are two types of consumer, with the high type willing to pay more for the item than low-type consumers. Also, the marginal cost of the item is sufficiently low that it is efficient to provide it to both the types. The difference with the static case is that there are two periods.

The seller's pricing strategy depends on its information about the consumer population. With privacy regulation that prevents collection of personal information, the seller would set the same price over time, which price depends on the composition of the consumer population. In particular, if the proportion of low-type consumers is high enough (or, more generally, the demand is sufficiently elastic), the seller would set a price low enough so that both consumer types buy the item, and such that the high-type consumers enjoy a positive surplus. This equilibrium is efficient.

Now, suppose that the seller can infer the consumer types from their purchase history. Specifically, in the first period, the seller can set a sufficiently high price that only high types buy, and the remaining consumers (who do not buy) are revealed to be low types. Then, the seller can condition prices in subsequent periods on first-period purchase behavior, and so, perfectly price discriminate (Acquisti and Varian, 2005 call this "price conditioning").

Accordingly, if personal information collection is feasible, the seller faces a trade-off: by charging a high price in the first period, it forgoes profit from the low-type consumers, but it gains from identifying the high-type consumers and price discriminating against them in subsequent periods. From the viewpoint of social welfare, the low-type consumers suffer a deadweight loss from not consuming in the first period.

It is easy to predict what increases the seller's incentives to collect consumer information. In the stylized example above, a wider gap between the high- and low-type consumers' valuations, a higher proportion of high-type consumers, a longer time horizon (i.e., more future repurchases), and more precise addressing of the consumer segments, would increase the seller's incentive to use a high price to screen the consumer segments in the first period.

Note that the collection of personal information could also *raise* welfare. This arises when, absent the ability to record transaction information (and thereby discriminate), the seller chooses to sell only to high-type consumers. By enabling discrimination, the collection of purchase history then leads the seller to sell to low-type consumers as well, and so, raises welfare.[10]

Another consideration is that consumers might also act strategically. Suppose again that, when unable to record transaction information, the seller sells only to high-type consumers. If low-type consumers can credibly reveal their personal characteristics,[11] they would also produce information and so persuade the seller to offer them the item at a lower price.[12] The efforts of the seller and low-type consumers to produce information are strategic substitutes (Bulow et al., 1985).

[10]Generally, price discrimination might raise or reduce welfare (Varian, 1985).

[11]Students may produce school or university identity cards and seniors may show proof of age to qualify for lower prices. In the employment context, job seekers may produce reference letters from past employers, professional certificates, and school transcripts to prove their ability.

[12]Hermalin and Katz (2006) also make this point in discussing property rights.

Now, if privacy regulation increased the seller's cost of information collection, then the seller would collect less information. In turn, this would lead low-type consumers to produce *more* information. If the response of the low-type consumers is sufficiently vigorous, the net result might be paradoxical—the total amount of information produced and social welfare could both increase (Gould, 1980). Similarly, relaxing privacy regulation, which reduces the cost of information production, could lead to less information being produced and reduce welfare.

The implications of privacy regulation are subtler still in a setting with competition among multiple sellers. As reviewed by Fudenberg and Villas-Boas (2006) in this *Handbook*, even if each seller would gain individually by being the only one to engage in price conditioning, if all sellers engage in the practice, then it might intensify competition and thereby reduce the sellers' combined profits. Further, as in the monopoly case, privacy regulation may raise or lower social welfare. However, by contrast with the monopoly case, the use of price conditioning among competitive sellers may raise consumer surplus.[13]

Wathieu (2004) addresses a different issue—the impact of privacy regulation on the cost of product variety. Consider a setting where consumers have specific tastes for different products. *Ex ante*, a seller cannot distinguish the consumer types, and it incurs an advertising cost to address each individual consumer with a product. The advertising cost must be repeated for each product that the seller markets to a particular consumer. If the seller acquires and uses consumers' personal information to segment the demand, it can reduce advertising costs because the advertisements are more accurately directed. In this context, by hindering segmentation, "privacy" may increase the sellers' advertising costs.

However, despite the saving in advertising costs, when production is characterized by economies of scale, allowing the seller to gain access to consumer information could lead to excessive product variety. With the information, the seller will have excessive incentive to price discriminate and extract surplus from mainstream consumers. In this case, mainstream consumers would prefer information privacy, and so avoid being identified and hence avoid a higher price.

Generally, the collection and use of non-productive personal information may redistribute surplus among sellers and consumers, but it does not necessarily generate more exchange (Hirshleifer, 1971). Specifically, the collection and use of customer purchase histories has private value to sellers, but need not create social value. In fact, it may diminish social welfare by reducing the consumption of the low-type consumers. In the monopoly

[13]See also Choudhury et al. (2005) for a related analysis on competition between firms that employ personalized pricing technologies, and Bouckaert and Degryse (2006) for an analysis of the differing impacts of opt in and opt out privacy policies on firm entry and social welfare.

setting, consumer concerns about price discrimination seem to be well justified. On the other hand, in competitive settings, price conditioning may benefit consumers. Further, sellers may use personal information to reduce marketing costs (Wathieu, 2004). Finally, changes in privacy regulation to adjust the cost of collecting or producing personal information may lead to conflicting adjustments in the production of information. Clearly, the social value of privacy regulation is ambiguous.

3.2 Productive information

Hermalin and Katz (2006) provide a simple model of the issue.[14] Competitive employers face a heterogeneous population of workers, some of whom have high productivity while others have low productivity. Each employer needs just one worker. In the economic efficient allocation, both types of worker would be employed.

Suppose that the original equilibrium pools high and low types at a common wage. Since both types of worker are employed, this equilibrium is efficient. Now, divide the worker population into two pools. With additional information, employers can more accurately identify high-type workers. If the proportion of high types in the "good" pool is sufficiently large (and that in the other "bad" pool is low), then in competitive equilibrium, employers will employ all workers in the "good" pool at a common wage, but pay a low wage to the bad pool. The low wage would attract only low types; hence, the high-type workers in the bad pool would be unemployed. This would reduce welfare relative to the original equilibrium.

By contrast, suppose that the original equilibrium included only low types. This adverse selection equilibrium is not efficient. Again, divide the worker population into two pools, and suppose that additional information enables employers to more accurately identify high-type workers. If the proportion of high types in a "good" pool is sufficiently large, then in competitive equilibrium, employers will employ all workers in the "good" pool at a common wage. This would raise welfare relative to the original equilibrium.

Taylor (2005) also addresses the issue of over/under-investment in productive personal information in a competitive setting, but using a somewhat different setting. Each employer seeks a worker, who has either high or low productivity. The worker does not know her own productivity. In the economic efficient allocation, only the high-type worker would be employed. The employer can invest in information about the worker. When the information about high-type workers is perfect but information about low-type workers is subject to error, the employer will *over*-invest in

[14]Their setting is not quite the simplest possible, as it supposes there to be competition on the seller side. An even simpler setting would have just a monopoly seller.

information. However, when the information about high-type workers is subject to error but information about low-type workers is perfect, the employer will *under*-invest in information.

The analyses of Hermalin and Katz (2006) and Taylor (2005) imply that there is no simple rule: whether privacy of personal information raises or reduces welfare depends on the circumstances.

A separate stream of research has considered the role of personal information privacy in tax policy. In this setting, the less-informed party is the government. The government uses income tax to re-distribute income from high- to low-income earners. If the government sets tax rates after individuals have decided their investment in something that increases their future earnings, say education, a time consistency problem arises. Fearing that the government will set high tax rates in the future, taxpayers will under-invest in education (Boadway et al., 1996).

In this context, a privacy policy is an effective way by which the government can commit to lower tax rates in the future (Konrad, 2001): the privacy policy limits the government's ability to collect information and hence to levy high tax rates. Accordingly, the privacy policy serves to encourage taxpayers' investment in activities that increase their future earnings.

Dodds (2003) considers a different setting, where individuals of two types benefit from a public good. The socially efficient quantity of the public good depends on the number of high-productivity persons. The high-productivity persons are reluctant to reveal themselves as they must then contribute relatively more toward the public good. The issue is closely related to that of taxpayer compliance where taxpayers must report their income subject to government auditing. As in the taxpayer compliance analyses (Mookherjee and Png, 1989), Dodd's key result is that 100% auditing does not maximize welfare. He interprets this to mean that some degree of privacy is socially efficient.

Generally, in competitive settings, an improvement in the accuracy of productive personal information may lead the less informed party (seller or employer) to include more or exclude some marginal persons (consumers or workers). This is a consequential externality on some members of the better-informed side of the market. The consequential externality might be positive or negative. It is surprising that the grounds for privacy do not seem to be weaker with respect to productive as contrasted with non-productive personal information.

4 Cross-market consequential externalities

In this section, we consider how the collection of personal information in one market for use in another market affects the efficiency of market

outcomes.[15] The collection and use impose a consequential (rather than direct) externality. For the most part, cross-market consequential externalities apply to the secrecy dimension of privacy.

Marketers may compile customer databases for sale to third parties. For example, e-mail portals may pass personal details of account holders to third parties who then use the information to promote their goods and services. The policy implications with respect to the third-party "information buyers" are similar to those in the cases that we have reviewed in the preceding section. Hence, we consider only the actions of the "information sellers."

The central theme is that the marketer may have even more incentive to collect consumer information in a cross-market than in a within-market setting. Recall the monopoly model of within-market collection and use of non-productive information over time. As analyzed in Section 3.1, the seller has an excessive incentive to price high in the first period and so identify the high-type consumers.

This incentive is *reinforced* if the seller can sell the personal information collected to third parties—the revenue from selling customer information would raise the marginal return from the price experiment (Taylor, 2004). Hence, the seller is more likely to set a high first-period price. When demand is somewhat elastic (i.e., the seller would sell to all consumers absent the opportunity to sell information), the option to sell consumer information would lead the seller to restrict output, and hence, reduce welfare.

Addressing a similar problem, Calzolari and Pavan (2005) develop a very sophisticated model that considers interaction between two different uninformed parties, say sellers, with a single informed party, say a buyer whose characteristics are private information, over time. They identify conditions under which the early seller will transfer information about the buyer to the later seller. In particular, when the early seller is not interested in the exchange between the buyer and later seller, the buyer's valuations toward the two sellers' products are positively correlated, and the buyer's preferences in the two sellers' products are separable, then the early seller may prefer to protect the buyer's privacy.

By contrast, when any one of these conditions is not met, the early seller can capture additional rents arising from information or contractual externalities. The effect of privacy on welfare is ambiguous—privacy may promote the exchange between the buyer and later seller, but it could also introduce new distortions in the buyer's exchange with the early seller.

Overall, it seems that the selling of personal information benefits "information buyers" (secondary sellers). As for social welfare in secondary markets, it could increase or decrease depending on the composition of the

[15]Cross-market externalities imply "secondary use" of personal information. Secondary use can also occur within the same market. For instance, a marketer might use a delivery address submitted for an online purchase to promote related items.

consumer population (as discussed in Section 3). However, in the primary market, where the personal information is collected, welfare may decrease because sellers have greater incentive to raise price in order to classify consumers (Taylor, 2004; Calzolari and Pavan, 2005). The primary sellers can then compile customer information for sale to secondary sellers. Therefore, a cross-market externality may emerge when sale of consumer information is allowed.

In general, sale of consumer information is more likely to be beneficial when the potential of such information is high, e.g., when the classification of consumers can help to match seller offers and interested consumers. If the information does not lead to more efficient exchange in secondary markets, then it may be worthwhile to discourage its sale, which would in turn discourage primary sellers from collecting the information.

5 Direct externalities

In this section, we consider direct externalities arising from the collection and use of personal information within the same market and across markets. Direct externalities apply to the secrecy, autonomy, and seclusion dimensions of privacy.

A major use of personal information is to direct unsolicited promotions by mail, telephone, e-mail, and in person. To the extent that such solicitations impose costs on consumers that marketers ignore, they generate a negative externality (Petty, 2000).

Van Zandt (2004) analyzes a setting where heterogeneous sellers send messages to promote different items. Consumer attention is a scarce resource—each consumer can process a limited number of messages. Hence, consumers incur costs to "open" marketing messages. They respond to sellers and purchase if and only if they have read the messages and are interested in the item. Sellers have private information on consumer interests, and they decide strategically how many messages to send, and which consumers to target. Sellers may over-promote their products. Accordingly, measures that inhibit solicitations (e.g., that increase communication cost or a tax on solicitations) may help sellers to focus their marketing effort and hence improve social welfare.[16]

In a similar setting, Anderson and de Palma (2005) show that over-promotion by sellers could even lead to market failure—the quality of messages may become so low that consumers choose not to read any messages. Such market failure is reminiscent of the well-known "lemons"

[16]However, the sellers' profits would increase only if they have sufficiently accurate data on consumer interest (Van Zandt, 2004). To this extent, consistent with the Chicago School's view, privacy (or more specifically, secrecy) of personal information may not be desirable.

problem (Akerlof, 1970). Evidently, increasing solicitation cost could well raise welfare, and therefore regulation may play a positive role.[17]

Akcura and Srinivasan (2005) consider the cross-market collection and use of information. Sellers may collect personal information about consumers in a primary market and use it in a secondary market. In deciding how much personal information to reveal, consumers balance the benefit from consuming the primary item against direct privacy costs.[18] The higher the rate at which consumers expect sellers to cross-sell personal information, the less information consumers would reveal. Accordingly, sellers may choose to limit the extent to which they cross-sell personal information, and so, persuade consumers to provide more information in the primary market.

Hann et al. (2006a) analyze direct marketing in a setting with two types of consumer—one with a high value for the item being marketed and the other with a low value. Each direct marketing solicitation causes some harm, but a consumer can get the item only through the solicitation. Consumers can take actions to reduce the harm (''marketing avoidance''). For instance, to avoid telemarketing solicitations, consumers can conceal (e.g., by registering with do-not-call lists) or deflect (e.g., by screening incoming telephone calls). Sellers cannot distinguish the consumer types *ex ante*. Ideally, they would promote only to high-type consumers. Instead, they incur costs to solicit the entire consumer population, and then discover consumer types *ex post*.

Seller solicitations are a strategic complement (Bulow et al., 1985) with concealment by low-type consumers. If the cost of concealment measures were to fall, low-type consumers would raise concealment, and sellers would *increase* marketing. Indeed, since 2003, the US enforcement of a nationwide ''do not call list'' may have led to an increase in the return on investment from telemarketing (Direct Marketing Association, 2004). However, from a welfare perspective, consumer concealment is less favorable than deflection, because it concentrates seller solicitations on a smaller number of consumers (Hann et al., 2006a). A consumer needs only one solicitation to enjoy the product, and additional solicitations add to harm. Accordingly, concentrating the solicitations raises the expected harm relatively more than the benefit.

Although the scenarios of hacking and eavesdropping appear to be quite different from that of direct marketing, the formal analysis is quite closely related. Consumers who provide information to vendors or use communication services may be subject to *covert* intrusions into their privacy,

[17]Further, Gantman and Spiegel (2004) consider the trade-off in software that incorporates advertising banners (''adware'') between the benefit to consumers of receiving targeted information which improves their choice of product against the privacy cost.

[18]Akcura and Srinivasan (2005) do not specify the nature of these costs, but they could presumably encompass the inconvenience from receiving unsolicited direct marketing and the harm from possible intrusion into the seller's database.

which impose direct and indirect costs. In response, consumers could take defensive actions like encoding and encryption, which are costly and might also diminish the benefit from consumption (Noam, 1995a). The strategic impact of such defensive actions could be analyzed in the same way as marketing avoidance (Hann et al., 2006a) and, more generally, private security (Koo and Png, 1994).

The research just reviewed emphasizes externalities from one side of a market to another. Another important class of direct externalities is that of peer-to-peer externalities. August and Tunca (2004) study the incentives of end users to patch security flaws in computer systems. Computer viruses exploit flaws in one computer system to penetrate others, and are more likely to succeed the fewer users patch flaws. The key policy implication is that, where users differ in their value from use of the system, mandatory patching is not optimal.

Although August and Tunca focus on computer viruses, their analysis may apply more generally to applications in which consumers reveal the personal information of others. Examples of such applications include instant messaging services and online communities (e.g., friends.com), where users are asked to refer their peers to service providers. In some cases, service providers may even covertly traverse the e-mail boxes of users to recruit new potential users (much like the way computer viruses infect other systems). Despite the risks of such privacy invasion, August and Tunca's analysis suggests that mandating users to protect privacy need not be optimal.

Overall, it is clear that, in circumstances involving direct externalities, privacy of personal information would increase social welfare. However, sweeping solutions, such as disallowing the collection and use of personal information, would not be optimal—they would prevent interested consumers from enjoying the items being promoted (Van Zandt, 2004; Anderson and de Palma, 2005; Hann et al., 2006a) or cause consumers to forego some implicit benefits (Akcura and Srinivasan, 2005).

6 Property rights

Will the appropriate assignment of property rights (self-regulation) resolve the issue of privacy? The Chicago School posits that a free market for information yields social efficiency. Hence, an explicit allocation of property rights may shift society away from a socially efficient equilibrium and reduce welfare. For instance, granting workers property rights to their personal information may cause an employer to reduce employment.

In their analyses of both non-productive and productive information, Hermalin and Katz (2006) show that the market outcome is identical regardless of how property rights over personal information are assigned. Specifically, in the case of non-productive information, the monopoly seller

can compel customers to reveal their type. In the case of competition with productive information, high-type workers will identify themselves, thus revealing the low types. Similarly, Kahn et al. (2000) show that, if there is sufficient flexibility in contracting, information would be revealed to an efficient degree. The outcome obeys the Coase Theorem—it does not matter whether or how property rights to personal information are initially assigned.[19]

However, the analyses of Hermalin and Katz (2006) and Kahn et al. (2000) apply to situations where the collection and use of personal information take place within the same (primary) market. What if the relatively uninformed party uses the information in secondary contexts as, for instance, when a marketer sells consumer information gathered at one web site to third-party spammers? Then a cross-market externality will arise. The parties with personal information will certainly consider the cross-market externality when deciding how much personal information to reveal (Akçura and Srinivasan, 2005).

The impact of the allocation of property rights to personal information in the primary market may well depend on the relation between the party's positions in the primary and secondary markets. Will a high-type worker in the primary market also be a high-type worker in the secondary market? When the secondary use of the information is uncertain, property rights may have a role.

Further, in the case of direct externalities, property rights would clearly help to resolve the harms that sellers impose on consumers, and also peer-to-peer harms among consumers.

Therefore, it may be worthwhile to attach a value to personal information, at least in terms of restricting future uses of the information. The challenge then lies in how such a value is determined.

The first issue is that the parties with property right over their personal information may not fully take account of the potential benefit of the information to uninformed parties. For instance, a common regulatory remedy for unsolicited promotions is the "do not contact" list. However, potential consumers may ignore sellers' profit when deciding to register with "do not contact" lists, and hence may tend to over-register relative to the welfare optimum (Anderson and de Palma, 2005).[20]

It is quite natural to expect that allowing consumers to set their own values for personal information may lead them to over-value data (Schwartz, 2004). Hence, the second issue is that consumers may attach too high a price to their personal information, which might excessively raise the barrier to potential buyers of the information. Specifically, economic experiments have repeatedly shown that people demand a higher price for a

[19]See also Chellappa and Shivendu (2003).

[20]In 2003, the US government established a nationwide "do not call" registry. By August 18, 2005, the registry has recorded 100 million entries (Federal Trade Commission, 2005b).

property when another person seeks to use it than the price that they would offer to protect the property from being used (see, e.g., Boyce et al., 1992).

In the context of personal information, individuals' "willingness to accept" (WTA) for use of their personal information (when they have explicit property rights over the information) may exceed their "willingness to pay" (WTP) for protection of their information from exploitation (when no property right is granted). Granting property rights to individuals and allowing them to name their own price may lead to under-usage of information, whereas allowing the free use of personal information could lead to over-usage.

The difference between WTA and WTP for personal information could help explain the disparate findings from opinion polls (e.g., Harris Interactive, 2001, 2003) and behavioral experiments (e.g., Ackerman et al., 1999; Hann et al., 2003; Hui, 2006; Hui et al., 2006). Specifically, when polled for their opinions on or attitudes toward privacy, people may assume they "own" their personal information and hence demand a high price for use of their information. By contrast, when confronted with actual information requests and when they realize that protecting their personal information may be "costly" (e.g., they may not be able to use a web site or complete a transaction if they do not supply the information), they demand less compensation. The behavioral experiments cited above have shown that people provide their information in exchange for even small rewards or incentives.

Clearly, it would be misleading to judge the importance of privacy from opinion polls alone. Rigorous experiments are necessary to gauge the actual value that people attach to their personal information under various circumstances. Perhaps the Becker–DeGroot–Marschak (BDM) mechanism (Becker et al., 1964) can be employed to elicit the incentive-compatible reservation prices that people place on their personal information. It would be important to recognize the likely gap between WTA and WTP, and assess the benefits of allocating property rights accordingly.

7 Regulation

Assignment of property rights will resolve privacy issues only in contexts where the collectors and users of personal information and their subjects of the information can enter into contractual arrangements. But what about contexts where such arrangements are inconvenient or even impractical, for instance, widespread peer-to-peer externalities in the decision of computer users whether to patch security vulnerabilities? In law, this is the domain of tort law and regulation as contrasted with contract law.

Tang et al. (2005) consider a setting where intrusion of privacy imposes a direct cost on consumers. Consumers differ in their sensitivity to intrusion, while sellers differ in their cost of protecting privacy. When few consumers

are sensitive, welfare is maximized with a regime of "caveat emptor," as businesses avoid the cost of protecting privacy. By contrast, when many consumers are sensitive, welfare is maximized with mandatory privacy regulation, as consumers avoid the cost of comprehending each business' privacy policy. In the intermediate case, welfare is maximized with privacy seals—the low-cost businesses choose to purchase the seal, while the high-cost businesses do not.[21]

A key reason in favor of regulation is that it may be a more effective form of commitment than contractual arrangements. Our review above (Sections 3–5) has pointed to various situations of both consequential and direct externalities where commitment to protect privacy increases welfare. Specifically, analyses of behavior-based price discrimination in competitive settings show that businesses may benefit from privacy of personal information (Fudenberg and Villas-Boas, 2006).

Ironically, business interests oppose proposals to tighten privacy regulation. The US national cost of complying with these legislative proposals has been estimated to be US$9–36 billion (Hahn, 2001). For just catalog and Internet clothing retailers, the Direct Marketing Association estimated that opt-in restrictions to use of demographic information by third parties would raise costs by US$1 billion (Turner, 2001).

The economic analysis of consequential externalities suggests that whether and how privacy increases welfare depends on the particular circumstances. Consequently, there will be no magic "one size fits all" solution, but rather, regulation should be tailored to the circumstances. For instance, communication between persons with a particular relationship, including husband–wife, penitent–clergy, patient–doctor, attorney–client, citizen–census taker is commonly protected by "privilege." The patient–doctor privilege encourages an uninhibited exchange of information and so, enhances overall community health (Noam, 1995a).

Muris (2003) had proposed to generally allow free use of personal information, while focusing enforcement against misuse. The focus on information use is consistent with consumer preferences (Wathieu and Friedman, 2005). However, in the studies that we reviewed in Sections 3 and 4, welfare could be reduced by apparently legitimate uses of information that did not cause direct harms. Hence, requirements for consumer consent to collection and use of personal information (as stipulated in the FIPs) could raise social welfare. Accordingly, the key issue is how to balance the interests of sellers and consumers, and obviously a sweeping "use" or "no use" solution would not work across all contexts. Wherever it is feasible to ascertain the benefits and costs of information use, the obvious solution is industry-specific regulation, as in the Fair Credit Reporting Act of 1970.

[21]Information providers could also commit to privacy protection through service-level agreements with their users (Pau, 2005).

Regulation must be tailored even with regard to direct externalities, for which it is unambiguous that privacy would raise welfare. As mentioned earlier, a common regulatory remedy for unsolicited promotions is the "do not contact" list. While a "do not call" list may resolve telemarketing, a similar "do not spam" list might be counterproductive. Illicit spammers account for the bulk of spam, and they might well spam addresses on the "do not spam" list (Hahn, 2003; Muris, 2003). With regard to spam, a tax appears to be the most promising solution (Kraut et al., 2002; Van Zandt, 2004; Anderson and de Palma, 2005), and generally, deflection is to be preferred over concealment (Hann et al., 2006a).

8 Empirical evidence

To gauge the economic significance of privacy as a public policy issue, it is vital to know how much people value their privacy. Polls and surveys have repeatedly shown that people are concerned about privacy (Westin, 2001). However, the key policy issue is not whether individuals value privacy. It is obvious that people value privacy. What is not known is *how much* people value privacy and the extent to which people differ in their valuations.

Despite tremendous debate and policy interest, there has, to date, been little research into this question (Hahn, 2001). Indeed, it has been conjectured that "measuring the value of consumer privacy may prove to be intractable" (Ward, 2001).

Recent opinion surveys and experimental research provide some insights into this question. In November 1998, among 381 US respondents to an online survey, most were willing to reveal personal information but would not reveal personal identifying information (Ackerman et al., 1999). For instance, 58% would report income, investments, and investment goals to obtain customized investment advice, but only 35% would also reveal their name and address.

In May–June 2000, the Pew Internet and American Life Project found that, among 1,017 American Internet users, 54% would provide personal information in order to use a web site, whereas only 27% were hard-core privacy protectionists who would never provide their personal information to web sites (Fox et al., 2000). In February–March 2003, the Annenberg Public Policy Center of the University of Pennsylvania found that, among a sample of 1,200 respondents aged 18 years or older who used the Internet at home, most who did not accept a web site's data collection policy would nevertheless disclose their real name and e-mail address if they valued the web site (Turow, 2003).

More compelling than surveys are various experiments that gauged subjects' willingness to reveal personal information. Hui et al. (2006) conducted a field experiment to measure the likelihood that individuals would provide

personal information to Internet businesses. By estimating a discrete choice model using real online participation data, they found that people were willing to disclose more personal information in exchange for small monetary incentives. Similarly, in laboratory experiments, simple interface redesign could induce consumers to disclose more personal information (Hui, 2006), or opt-in to receiving future newsletters (Lai and Hui, 2004, 2005).

Wattal et al. (2004) procured data from field experiments conducted by an e-commerce vendor. The vendor contacted potential customers with different dimensions of customization—some received customized product information, while others received personalized greetings, e.g., "Dear Ms ABC." Consumers responded positively to customized product offerings, but negatively to personalized greetings.

Wathieu and Friedman (2005) suggest that privacy concerns are sensitive to indirect consequences of information transmission. In particular, they argue that personal information may not have intrinsic value, and the flow of personal information may not be the key privacy concern. Rather, it is the concern about information use that affects consumer behavior. Their argument was supported in an experiment that involved 647 subjects from a US business school research pool.

An experiment at Humboldt University provides further indirect evidence (Berendt et al., 2005). Two hundred and six volunteers interacted with an anthropomorphic 3-D shopping bot to select a compact camera or winter jacket. The bot engaged subjects in dialogue about product attributes and also posed 'soft' questions typical of selling in conventional stores. The experimental subjects willingly revealed personal identifying information to the bot, specifically, 35–40% provided their home address.

Earp and Baumer (2003) conducted an online survey with 415 respondents. Each respondent was randomly shown one of 30 web pages, from well- or lesser-known retail, medical/health, and financial sites. Respondents were most willing to reveal gender and age, and least willing to reveal their social security numbers. Moreover, they were significantly less willing to provide personally identifiable information (phone number, home address, e-mail address, social security number, and credit card number) to lesser known than well-known web sites.

The surveys and experiments clearly show that people value privacy, but to an extent less than some privacy advocates have claimed. In particular, many survey respondents indicated use of web sites as a sufficient motivation to provide personal information. The results suggest that consumer information can be directly solicited in exchange for simple monetary or procedural measures. Further, they also suggest that governments should evaluate practical implications for Internet businesses before introducing stringent privacy regulations.

A question related to individuals' value for privacy, in general, is how they value the use of their personal information. A set of conjoint analyses at Singapore and US universities show that people are willing to bear the

risks of improper access to or secondary use of their information in exchange for monetary incentives or increased convenience (Hann et al., 2003). In particular, the U.S. and Singapore subjects valued improper access to personal information at around US$11–20, whereas they valued secondary use at around US$8–27.[22] Hence, despite consumers' protests against price discrimination, sale of personal information to unauthorized third parties, spam, etc., it may indeed not be that difficult to convince them to agree to these information uses.

Hann et al. (2003) also identified three distinct segments in the consumer population—privacy guardians (the majority), information sellers, and convenience seekers. However, these segments were not significantly correlated with demographic characteristics. By contrast, using census data, Varian et al. (2004) identified household characteristics of telephone numbers registered with the US national "do not call" list. Those with annual incomes exceeding US$100,000 and college-level education were significantly more likely to register, while those with a member in the 13–19 age group were significantly less likely to register. It is intuitive that wealthier households would suffer more annoyance from telemarketing calls. Why households with teenagers suffer relatively less is more of a puzzle.

In the context of direct e-mail marketing, marketers do not bear the privacy costs imposed on consumers. Since the cost of spam is very low (e.g., Muris, 2003), do spammers broadcast their solicitations randomly? In a field experiment, Hann et al. (2006b) find that spam is not random but rather targeted. Specifically, the incidence of spam was higher among e-mail accounts created with particular service providers, accounts with particular declared interests, and accounts associated with persons more likely to make online purchases (Americans rather than Singaporeans, adults rather than teenagers).

Further, the spam arena provides evidence of the relative effectiveness of regulation vis-à-vis self-regulation. Web sites do indeed comply with their published privacy policies (Jamal et al., 2003). Hence, if self-regulation of privacy were economically efficient, it could work. Further, mandatory regulation tends to drive out self-regulation: web sites in the United Kingdom, which mandates privacy regulation, provide stronger privacy protection than those in the United States, which follows a self-regulatory approach (Jamal et al., 2005).

To conclude, the evidence so far indicates that consumers are not truly so sensitive about privacy. Economic solutions, such as the exchange of personal information for monetary incentives, convenience, or special resources, may suffice to regulate the market for personal information (Noam, 1995b; Laudon, 1996). The contentious debate about privacy regulation may have been misdirected—the question does not lie in whether

[22]See also Baumer et al. (2005) for the use of experimental economics to quantify the values that consumers place on privacy and security.

tighter control should be placed on information collection and use, but in setting the right "prices" for personal information.

9 Future directions

Clearly, a free market in personal information will not provide an economically efficient outcome. With regard to consequential externalities within and across markets, privacy over personal information may raise or lower welfare depending on the circumstances. This should not be surprising, as, generally, the direction of welfare gain in "second-best" situations is *a priori* ambiguous. Given that, it would be interesting to explore whether privacy regulation is relatively more likely to increase welfare in the context of non-productive as compared with productive information.

We see several other directions for future research. First, in all of the various models that apply the asymmetric information approach, it is assumed that the uninformed party knows of the existence of the parties with private personal information and knows their distribution of personal characteristics, but just does not know the characteristics of individual persons. For instance, in the setting of Acquisti and Varian (2005), only high types buy in the first period, so everyone else must be a low type. But what if the uninformed party does not even know the distribution of personal characteristics? Would the results be the same if the analysis begins from the uninformed party's *beliefs* about the distribution of the other party's personal characteristics?

Second, personal information, like information in general, is a public good (Stigler, 1980). Economists have given little attention to the public good aspects of privacy, specifically, the conditions for the optimal production and usage when the marginal cost of usage is zero. For instance, if disclosure of AIDS test results were mandatory, individuals might forgo testing, which would lead to unintended adverse consequences (Hermalin and Katz, 2006).

Third, as our discussion of WTP vis-à-vis WTA makes clear, there is substantial potential to apply behavioral economics for a better understanding of privacy. Personal information is such a sensitive thing that individual behavior is relatively more likely to depart from the rational model with respect to personal information than other things. Preliminary research has shown that consumers may often not have well-defined preferences on privacy—it is possible to influence their willingness to reveal or consent to use of their personal information by varying data solicitation procedures, even trivially (Hui, 2006; Lai and Hui, 2004, 2005).

Fourth, prior research and discussion has focused on privacy of personal information. Do the same analyses and conclusions apply to privacy of *corporate* information? Under what circumstances does protection of corporate information raise social welfare? This question is the counterpart to

a key issue in accounting research, viz., disclosure. The issue of corporate privacy also bears on two other concepts—trade secrets in intellectual property and corporate reputation.[23]

Fifth, we should mention economics-oriented research into the *technology* of privacy. Loder et al. (2006) apply the theory of mechanism design to devise an incentive-compatible technology to screen out spam. Serjantov and Clayton (2005) use a stylized model and a set of e-mail data to examine the implications of various spam-blocking strategies. More generally, an interesting direction for research is to apply economics to the technology of privacy, and specifically, issues of system and software security.

Finally, to ensure the currency of this review, we have created a complementary wiki at http://infoprivacy.pbwiki.com/. All scholars are invited to contribute information and links.

Acknowledgments

We thank Jean Camp, Robert Hahn, Karim Jamal, Luc Wathieu, and the editor, Terry Hendershott, for helpful comments.

References

Ackerman, M.S., L. Cranor, J. Reagle (1999). Privacy in e-commerce: examining user scenarios and privacy preferences, in *Proceedings of the ACM Conference in Electronic Commerce*, ACM Press, New York, pp. 1–8. Available at http://portal.acm.org/citation.cfm?id=336995&jmp=cit&coll=portal&dl=ACM&CFID=439217&CFTOKEN=36198287#CIT

Acquisti, A., H.R. Varian (2005). Conditioning prices on purchase history. *Marketing Science* 24(3), 367–381.

Akçura, M.T., K. Srinivasan (2005). Research note: customer intimacy and cross-selling strategy. *Management Science* 51(6), 1007–1012.

Akerlof, G.A. (1970). The market for 'lemons': quality uncertainty and the market mechanism. *Quarterly Journal of Economics* 84(3), 488–500.

Anderson, S.P., A. de Palma (2005). A theory of information overload. Unpublished manuscript, Department of Economics, University of Virginia.

August, T., T. Tunca (2004). Network software security and user incentives. Unpublished manuscript, Graduate School of Business, Stanford University.

Baumer, D.L., J.B. Earp, J.C. Poindexter (2005). Quantifying privacy choices with experimental economics. Unpublished manuscript, College of Management, North Carolina State University.

Becker, G.M., M.H. DeGroot, J. Marschak (1964). Measuring utility by a single response sequential method. *Behavioural Science* 9(July), 226–232.

Berendt, B., O. Günther, S. Spiekermann (2005). Privacy in e-commerce: stated preferences vs actual behavior. *Communications of the ACM* 48(4), 101–106.

Boadway, R., N. Marceau, M. Marchand (1996). Investment in education and the time inconsistency of redistributive tax policy. *Economica* 63(250), 171–189.

[23]For a preliminary discussion on corporate privacy and the related regulatory considerations, see Posner (1978, 1979).

Bouckaert, J., H. Degryse (2006). Opt in versus opt out: a free-entry analysis of privacy policies, in: *5th Workshop on the Economics of Information Security (WEIS 2006)*, Robinson College, University of Cambridge, England 26–28 June 2006.

Boyce, R.R., T.C. Brown, G.H. McClelland, G.L. Peterson, W.D. Schulze (1992). An experimental examination of intrinsic values as a source of the WTA–WTP disparity. *American Economic Review* 82(5), 1366–1373.

Bucklin, R.E., C. Sismeiro (2003). A model of web site browsing behavior estimated on Clickstream data. *Journal of Marketing Research* 40(3), 249–267.

Bulow, J., J. Geanakoplos, P. Klemperer (1985). Multimarket oligopoly: strategic substitutes and complements. *Journal of Political Economy* 93(3), 488–511.

Bulow, J., P. Klemperer (2006). Privacy and prices. Discussion paper, Nuffield College, Oxford University.

Calzolari, G., A. Pavan (2005). On the optimality of privacy in sequential contracting. *Journal of Economic Theory* 30(1), 168–204.

Camp, L.J., C. Osorio (2003). Privacy enhancing technologies for internet commerce, in: O. Petrovic, M. Ksela, M. Fallenböck, C. Kittl (eds.), Trust in the Network Economy, Springer, Berlin, pp. 317–332.

Chellappa, R.K., S. Shivendu (2003). A property rights approach to consumer concerns of privacy in online personalization: incentives and welfare implications. Available at http://ssrn.com/abstract=457003. Accessed August 15, 2005.

Chellappa, R.K., R. Sin (2005). Personalization versus privacy: an empirical examination of the online consumer's dilemma. *Information Technology and Management* 6(2–3), 181–202.

Chen, Y., G. Iyer (2002). Consumer addressability and customized pricing. *Marketing Science* 21(2), 197–208.

Chen, Y., C. Narasimhan, Z.J. Zhang (2001). Individual marketing with imperfect targetability. *Marketing Science* 20(1), 23–41.

Choudhury, V., A. Ghose, T. Mukhopadhyay, U. Rajan (2005). Personalized pricing and quality differentiation. *Management Science* 51(7), 1120–1130.

Culnan, M.J., J.R. Bies (2003). Consumer privacy: balancing economic and justice considerations. *Journal of Social Issues* 59(2), 323–342.

Direct Marketing Association. The DMA 2004 response rate report. New York, October 2004.

Dodds, S. (2003). Privacy and endogenous monitoring choice when private information is a public good. Department of Economics, Carleton University, December.

Earp, J., D. Baumer (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM* 46(4), 81–83.

Eddy, E.R., D.L. Stone, E.F. Stone-Romero (1999). The effects of information management policies on reactions to human resource information systems: an integration of privacy and procedural justice Perspectives. *Personnel Psychology* 52, 335–358.

Federal Trade Commission (2005a). *Internet service provider settles FTC privacy charges*. March 10. Available at http://www.ftc.gov/opa/2005/03/cartmanager.htm.Accessed April 8, 2005.

Federal Trade Commission (2005b). Statement of Federal Trade Commission Chairman Deborah Platt Majoras on the 100 millionth number on the national do not call registry. Available at http://www.ftc.gov/opa/2005/08/dncstatment.htm. Accessed September 14, 2005.

Fox, S., L. Rainie, J. Horrigan, A. Lenhart, T. Spooner, C. Carter (2000). *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*. Pew Internet & American Life Project, Washington DC. Available at http://www.pewinternet.org/reports/toc.asp?Report=19. Accessed March 31, 2005.

Fudenberg, D., J. Tirole (2000). Customer poaching and brand switching. *RAND Journal of Economics* 31(4), 634–657.

Fudenberg, D., J.M. Villas-Boas (2006). Behavior-based price discrimination and customer recognition. *Handbook in Information Systems*, Chapter 7.

Gantman, N., Y. Spiegel (2004). Adware, shareware, and consumer privacy. Working Paper No. 04-02, NET Institute, October. Available at http://ssrn.com/abstract=618741.

Ghose, A., P.Y. Chen (2003). Personalization vs. privacy: firm policies, business profits and social welfare. Working Paper, GSIA, Carnegie Mellon University.

Goodwin, C. (1992). A conceptualization of motives to seek privacy for nondeviant consumption. *Journal of Consumer Psychology* 1(3), 261–284.

Gould, J.P. (1980). Privacy and the economics of information. *Journal of Legal Studies* 9(4), 827–842.

Hahn, R.W. (2001). *An assessment of the costs of proposed online privacy legislation*. AEI-Brookings Joint Center for Regulatory Studies, Washington, DC.

Hahn, R.W. (2003). *Outlawing spam won't work. Policy matters 03-36*. AEI-Brookings Joint Center for Regulatory Studies, Washington, DC, October.

Hann, I.H., K.L. Hui, T.S. Lee, I.P.L. Png (2003). *The value of online information privacy: an empirical investigation*. AEI-Brookings Joint Center for Regulatory Studies, Related Publication 03-25, , October.

Hann, I.H., K.L. Hui, T.S. Lee, I.P.L. Png (2006a). Consumer privacy and marketing avoidance: a static model. Unpublished manuscript, Department of Information Systems, National University of Singapore.

Hann, I.H., K.L. Hui, Y.L. Lai, T.S. Lee, I.P.L. Png (2006b). Who gets spammed?. *Communications of the ACM* 49(10), 83–87.

Harris Interactive (2001). Consumer privacy attitudes and behaviors survey wave II. Available at http://www.bbbonline.org/UnderstandingPrivacy/library/harris2-execsum.pdf. Accessed August 15, 2005

Harris Interactive. (2003). Most people are ''privacy pragmatists'' who, while concerned about privacy, will sometimes trade it off for other benefits. Available at http://www.harrisinteractive.com/harris_poll/index.asp?PID = 365. Accessed August 15, 2005.

Hart, O.D., J. Tirole (1988). Contract renegotiation and Coasian dynamics. *Review of Economic Studies* 55, 509–540.

Hermalin, B., M. Katz (2006). Privacy, property rights & efficiency: the economics of privacy as secrecy. *Quantitative Marketing and Economics* 4(3), 209–239.

Hirshleifer, J. (1971). The Private and social value of information and the reward to inventive activity. *American Economic Review* 61(4), 561–574.

Hirshleifer, J. (1980). Privacy: its origin, function, and future. *Journal of Legal Studies* 9(4), 649–664.

Hui, K.L. (2006). Consumer disclosure: the effects of company information presentation and question sequence. Unpublished manuscript, Department of Information Systems, National University of Singapore.

Hui, K.L., H.H. Teo, T.S.Y. Lee (2006). The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, forthcoming.

Jamal, K., M. Maier, S. 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.

Jamal, K., M. Maier, S. Sunder (2005). Enforced standards versus evolution by general acceptance: a comparative study of e-commerce privacy disclosure and practice in the United States and the United Kingdom. *Journal of Accounting Research* 43(1), 73–96.

Kahn, C.M., J. McAndrews, W. Roberds (2000). A theory of transactions privacy. Working Paper 2000-22, Federal Reserve Bank of Atlanta.

Katz, M.L. (1984). Firm-specific differentiation and competition among multiproduct firms. *Journal of Business* 57(1 part 2), S149–S166.

Konrad, K.A. (2001). Privacy and time-consistent optimal labor income taxation. *Journal of Public Economics* 79, 503–519.

Koo, H.W., I.P.L. Png (1994). Private security: deterrent or diversion?. *International Review of Law and Economics* 14(March), 87–101.

Kraut, R.E., S. Shyam, J. Morris, R. Telang, D. Filer, M. Cronin (2002). Markets for attention: will postage for email help? *CSCW 02*, New Orleans, ACM, 206–215.

Lai, Y.L. and K.L. Hui (2004). Opting-in or opting-out on the internet: does it really matter? in: R. Agarwal, L. Kirsch, J.I. DeGross (eds.). *Proceedings of the International Conference on Information Systems*, Washington, DC, December.

Lai, Y.L., K.L. Hui (2005). Luring the prey: attracting online consumer participation through choice configurations in: J. Langenderfer, D.L. Cook, J.D. Williams (eds.). *Proceedings of the American Market Association (AMA) Marketing and Public Policy Conference*, Washington, DC, May.

Laudon, K.C. (1996). Markets and privacy. *Communications of the ACM* 39(9), 92–104.

Loder, T., M. Van Alstyne, R. Wash (2006). An economic response to unsolicited communication. *Advances in Economic Analysis & Policy* 6(1), Article 2.

Moe, W.W., P.S. Fader (2001). Uncovering patterns in cybershopping. *California Management Review* 43(4), 106–117.

Moe, W.W., P.S. Fader (2004). Dynamic conversion behavior at e-commerce sites. *Management Science* 50(3), 326–335.

Montgomery, A.L., S. Li, K. Srinivasan, J.C. Liechty (2004). Modeling online browsing and path analysis using clickstream data. *Marketing Science* 23(4), 579–595.

Mookherjee, D., I.P.L. Png (1989). Optimal auditing, insurance and redistribution. *Quarterly Journal of Economics* 104(2), 399–415.

Moorthy, K.S. (1984). Market segmentation, self-selection, and product line design. *Marketing Science* 3(4), 288–307.

Muris, T.J. (2003). The federal trade commission and the future development of U.S. consumer protection policy, in: *Aspen Summit: Cyberspace and the American Dream, The Progress and Freedom Foundation*, August 19. Available at http://www.ftc.gov/speeches/muris/030819aspen.htm

Mussa, M., S. Rosen (1978). Monopoly and product quality. *Journal of Economic Theory* 18(2), 301–317.

Noam, E. (1995a). Privacy in telecommunications, Part I. *New Telecommunications Quarterly* 3(2), 51–59.

Noam, E. (1995b). Privacy in telecommunications, Part III. *New Telecommunications Quarterly* 3(4), 51–60.

Odlyzko, A. (2003). Privacy, economics, and price discrimination on the internet, in: *Proceedings, 5th ACM International Conference on Electronic Commerce*. Available at http://portal.acm.org/citation.cfm?id=948051&coll=ACM&dl=ACM&CFID=15950150&CFTOKEN=71609284&ret=1#Fulltext

OECD (1980). *OECD guidelines on the protection of privacy and transborder flows of personal data*. 23 September 1980. Available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.htm. Accessed May 17, 2005.

Pau, L.F. (2005). Privacy management contracts and economics, using service level agreements (SLA). Working Paper, Rotterdam School of Management, RSM Erasmus University, P.O. Box 1738, Rotterdam 3000, Netherlands.

Petty, R.D. (2000). Marketing without consent: consumer choice and costs, privacy, and public policy. *Journal of Public Policy and Marketing* 19(1), 42–53.

Png, I. (1998). *Managerial Economics*. Blackwell Publishers, Malden, MA.

Posner, R.A. (1978). An economic theory of privacy. *Regulation* (May/June) 9(3), 19–26.

Posner, R.A. (1979). Privacy, secrecy, and reputation. *Buffalo Law Review* 28, 1–55.

Posner, R.A. (1981). The economics of privacy. *American Economic Review* 71(2), 405–409.

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology* 73(6), 741–752.

Schwartz, P.M. (2004). Property, privacy, and personal data. *Harvard Law Review* 117, 2056–2127.

Serjantov, A., R. Clayton (2005). Modeling incentives for email blocking strategies. *Workshop on the Economics of Information Security (WEIS05)*.

Sismeiro, C., R.E. Bucklin (2004). Modeling purchase behavior at an e-commerce web site: a task completion approach. *Journal of Marketing Research* 41(3), 306–323.

Smith, H.J. (2001). Information privacy and marketing: what the U.S. should (and shouldn't) learn from Europe. *California Management Review* 41(2), 8–33.

Spence, A.M. (1973). Job market signaling. *The Quarterly Journal of Economics* 87(3), 355–374.

Stigler, G.J. (1980). An introduction to privacy in economics and politics. *Journal of Legal Studies* 9(4), 623–644.

Stiglitz, J.E. (1975). The theory of screening, education and the distribution of income. *American Economic Review* 65(3), 283–300.

Stone, E.F., L.D. Stone (1990). Privacy in organizations: theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management* 8, 349–411.

Tang, Z., J. Hu, M.D. Smith (2005). Protecting online privacy: self-regulation, mandatory standards, or caveat emptor. Working Paper, Tepper School of Business, Carnegie Mellon University, April.

Taylor, C.R. (2004). Consumer privacy and the market for customer information. *RAND Journal of Economics* 35(4), 631–650.

Taylor, C.R. (2005). Privacy and information acquisition in competitive markets. Working Paper, Department of Economics, Duke University.

Thisse, J.F., X. Vives (1988). On the strategic choice of spatial price policy. *American Economic Review* 78(1), 122–137.

Tirole, J. (1988). *The Theory of Industrial Organization*. MIT Press, Cambridge, MA.

Tolchinsky, P.D., M.K. McCuddy, J. Adams, D.C. Ganster, R.W. Woodman, H.L. Fromkin (1981). Employee perceptions of invasion of privacy: a field simulation experiment. *Journal of Applied Psychology* 66(3), 308–313.

Turner, M.A. (2001). *The Impact of Data Restrictions On Consumer Distance Shopping*. Direct Marketing Association. Available at http://www.the-dma.org/isec/9.pdf. Accessed August 15, 2003.

Turow, J., (2003). Americans & online privacy: the system is broken. Annenberg Public Policy Center, University of Pennsylvania. Available at http://www.annenbergpublicpolicycenter.org/04_info_society/2003_online_privacy_version_09.pdf. Accessed March 31, 2005.

Van Zandt, T. (2004). Information overload in a network of targeted communication. *RAND Journal of Economics* 35(3), 542–560.

Varian, H.R. (1985). Price discrimination and social welfare. *American Economic Review* 75(4), 870–875.

Varian, H.R., F. Wallenberg, G. Woroch (2004). Who signed up for the do-not-call list? *Third Workshop on Economics and Information Security*, University of Minnesota, Minneapolis, May.

Ward, M.R. (2001). The economics of online retail markets, in: G. Madden, S. Savage (eds.), The International Handbook on Emerging Telecommunications Networks, Edward Elgar Publishers, Cheltenham, UK.

Warren, S., L. Brandeis (1890). The right to privacy. *Harvard Law Review* 4(1), 193–220.

Wathieu, L. (2002). Privacy, exposure and price discrimination. Harvard Business School Marketing Research Paper 02-03, October.

Wathieu, L. (2004). Marketing and the privacy concern. Unpublished manuscript, Harvard Business School, March.

Wathieu, L., A. Friedman (2005). An empirical approach to understanding privacy valuation. Unpublished manuscript, Harvard Business School.

Wattal, S., P.Y. Chen, R. Telang (2004). On personalization technology adoption and information sharing in digital markets. Working Paper, Carnegie Mellon University.

Westin, A.F. (1967). *Privacy and Freedom*. Atheneum, New York, NY.

Westin, A. (2001). Testimony before U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, Hearing on ''Opinion Surveys: What Consumers Have To Say About Information Privacy,'' May 8.

Woodman, R.W., D.C. Ganster, J. Adams, M.K. McCuddy, P.D. Tolchinsky, H. Fromkin (1982). A survey of employee perceptions of information privacy in organizations. *Academy of Management Journal* 25(3), 647–663.