An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization

RAMNATH K. CHELLAPPA AND SHIVENDU SHIVENDU

RAMNATH K. CHELLAPPA is an Associate Professor of Decision and Information Analysis at the Goizueta Business School, Emory University. He previously served on the faculty of Marshall School of Business, University of Southern California, from 1997 to 2005. He received his Ph.D. from the University of Texas at Austin. Dr. Chellappa's expertise is in the field of electronic markets, digital goods pricing, and economics of information security and privacy. His research on piracy has been widely published in leading journals and conferences. His work on information privacy in online transactions received the Best Paper Award at INFORMS-CIST 2003. Professor Chellappa works closely with the music industry on topics related to forecasting, piracy, supply-chain management, and iTunes/digital sales. He currently teaches in the MBA and Ph.D. programs at Emory and he recently designed and taught a course on IT and medicine in the Medical Management Program at the University of Southern California.

SHIVENDU SHIVENDU is a Research Associate and Visiting Lecturer at the Goizueta Business School, Emory University, and a Ph.D. candidate in the Department of Economics at the University of Southern California. He received an MBA from the Indian Institute of Management, Ahmadabad, and a B.Tech. from the Indian Institute of Technology, Kanpur. He belongs to the Indian Administrative Service (IAS), members of which work in the highest echelons of the government in India. His research interests are in the area of economics of information, intellectual property rights, e-governance, incentive theory, regulation of natural monopolies, and privatization in developing countries.

ABSTRACT: Advances in information-acquisition technologies and the increasing strategic importance of this information have created a market for consumers' personal and preference information. Behavioral research suggests that consumers engage in a privacy calculus where they trade off their privacy costs from sharing information against their value from personalization. Through a formal economic model of this personalization-for-privacy (p4p) trade-off, we examine welfare implications by characterizing consumption utilities as "no-free-disposal" functions. We investigate the optimality of four regulatory regimes (through allowance/disallowance of usage-enforcing technologies, and private contracts) by analyzing the strategic interaction between a monopolist who offers personalization services "free of charge" and two consumer types—privacy and convenience seekers. While many privacy watchdog groups have called for technology restrictions and more regulation, our research broadly suggests that society is better off with assignment of property rights over their information to consumers and full allowance of technological control and contractual

Journal of Management Information Systems / Winter 2007–8, Vol. 24, No. 3, pp. 193–225.

0742–1222 / 2008 $9.50 + 0.00.
DOI 10.2753/MIS0742-1222240307

abilities for the monopolist. However, when private contracts are proscribed, the regulator should also prevent the deployment of usage-enforcing technologies, particularly when the market is predominantly composed of privacy seekers. Interestingly, unlike traditional price-instrument markets for goods with free disposal, a regulator should not only encourage this market's knowledge of consumers' p4p preferences but also the various uses and benefits of preference information to the vendor.

KEY WORDS AND PHRASES: economic modeling, incentives, Nash bargaining, personalization, privacy, property rights, social welfare.

> The FTC [Federal Trade Commission] can reassure consumers that privacy promises will be honored. We are an agency with knowledge about both consumer protection and the way markets address consumer privacy concerns. We will increase our enforcement of laws protecting consumer privacy.
>
> —Timothy J. Muris, Chairman of the Federal Trade Commission

THE QUESTIONS "DOES PERSONALIZATION JEOPARDIZE OUR PRIVACY?" and "If so, what should the law do about it?" have been recently raised in the legal community as a result of significant advances in information acquisition and personalization technologies [48]. Commonly, online personalization is offered at two places: (1) information goods that are personalized to individual tastes, such as management of investment portfolios through personalized portals and custom bundles of music and software, and (2) services that accompany the selection and purchase of virtually all goods, from books to electronics, which are also personalized by many online vendors [6]. In both cases, in order to personalize a service or product to one's tastes, the consumer needs to share his or her personal and preference information with the vendor.

An important aspect of online personalization is that these services are generally offered free of charge. However, consumers may not use all offered services even if they value personalization, as they are likely to be concerned about the privacy of the information that they share in order to use these services [49]. Such a privacy concern is indeed valid because the business rationale behind free services is often based on the exploitation of consumers' preference information, such as for pricing and targeted advertising.

Motivation

With technological advances, there has been a call for regulating information collection and usage by online firms. Many privacy watchdog groups, such as the Center for Digital Democracy (CDD; www.democraticmedia.org), U.S. Public Interest Research Group (U.S. PIRG; www.uspirg.org), and Electronic Privacy Information Center (EPIC; www.epic.org), have taken the view that privacy-related information

acquisition should be treated with the same alacrity by a regulator as would be price/quantity in many other public utilities markets. In the United States, the regulatory body the Federal Trade Commission (FTC) is tasked with protecting the interests of an individual in commercial transactions (both online and offline) including those that involve privacy concerns. However, CDD and U.S. PIRG contend that current privacy disclosure policies are totally inadequate, "Unfortunately, over the last several years the FTC has largely ignored the critical developments of the electronic marketplace that have placed the privacy of every American at risk. The FTC should long ago have sounded a very public alarm—and called for action—concerning the data collection practices stemming from such fields as Web analytics, online advertising networks, behavioral targeting, and rich 'virtual reality' media, all of which threaten the privacy of the U.S. public" [9]. EPIC also suggests that privacy should be more regulated: "Emerging technologies represent serious threats to privacy and are not addressed by self-regulation or law" [20]. The popular press suggests that "with the rapid growth of online commerce and recreation, lawmakers and consumers alike are becoming increasingly concerned about the collection and disclosure of personal information over the Internet. Despite the enormity of press coverage, the United States still has no unified regulatory scheme to protect online privacy" [42, p. 2]. Furthermore, most public polls on privacy also ask for more regulation; not only do 57–87 percent of respondents of a privacy poll feel that the government should pass more regulations for privacy but many (38–63 percent) also feel that current laws do not protect consumers adequately [43]. The question of interest therefore is the nature of regulation that will enhance social welfare in the online context.

Generally, research in economics has interpreted privacy as information asymmetry—that is, consumers' private knowledge of their preferences and price points prevents vendors from engaging in first-degree price discrimination. Indeed, a recent paper in economics acknowledges this gap: "while most consumers probably have an inherent preference for privacy, the analysis presented here focuses on . . . dynamic pricing" [44, p. 632]. Such formalization is relevant to studying insurance premiums, mortgage rates, or other goods and services where information asymmetry between sellers and buyers affects outcomes [10]. However, there is relatively little formal analysis of online privacy as discussed in this paper; that is, the concern for privacy that is subjective, intangible, and unique to an individual—one that has been exacerbated by online commerce. The impact of this type of privacy concern is not with regard to immediate price discrimination but a general need to be free from "excessive intrusion," as well as control over how the individual's information may be "used or shared." The spirit of this concern is best captured by the definition of privacy provided by the Committee on National Statistics [16], a governmental body that has a history of collecting and sharing individual-level information: "Informational privacy encompasses an individual's freedom from excessive intrusion in the quest of information and an individual's ability to choose the extent and circumstances under which his or her beliefs, behaviors, opinions and attitudes will be shared with or withheld from others" [16, p. 22]. With this definition in mind, we seek to identify optimal regulatory approaches in markets for information.

Interestingly, our research questions are consistent with those from one of the early reports commissioned by the U.S. Department of Commerce titled *Privacy and Self-Regulation in the Information Age*. One of contributors to that report asks, "Given that privacy is important to so many people, and given that information technology keeps raising new questions, what approach should be adopted to deal with privacy problems? In the past, if remedies were considered, the primary strategy was to resort to regulation. The call for the state to control and protect privacy is a natural response especially in the field of electronic communications, given their history around the world as either a state-controlled telephone or broadcast monopoly or tightly regulated sector" [29]. This report further examines a number of regulatory issues and ends with the question, "The reflexive approaches to privacy problems have been regulation, or denial. Are there other options?"

Generally, in other markets, such as telecommunications or utilities, one role of a regulatory body such as the Federal Communications Commission (FCC) is to curb excessive vendor power, and this is often accomplished by prescribing price caps, prohibiting price collusion, and monitoring other restrictive trade practices. Extending this regulatory role to markets for information might suggest that vendors should be proscribed (or at least limited) from information collection or usage, for fear of privacy violations. However, the FTC has been somewhat conflicted about more versus less regulation. At one end, while the FTC has sought more regulatory authority [35], its own commissioners have been troubled by this aspect. Two of the five members of the FTC dissented with the findings of the first report. Commissioner Orson Swindle wrote a long damning dissent in which he stated that the "embarrassingly flawed" report calls for "extensive government regulation" through "breathtakingly broad laws" [35]. So an important question is, how should a regulatory body choose a regime that protects consumers' privacy concerns—while not limiting the growth of online commerce?

Overview

Our paper suggests that markets for consumer information are fundamentally different from traditional price-quantity-instrumented buyer–seller markets. The information-privacy context is perhaps more akin to a trading regime or bartering system. One key aspect of online personalization is that it is offered for free, so from users' point of view, information is exchanged for personalization services and, from a vendor's perspective, services are offered to acquire information. In a sense, both agents are endowed with some inherent market power in that a vendor may limit the number of services offered and a consumer may choose to consume less than the number of services available (hence provide less than the maximum amount of information possible), though available for free. Intrinsically, personalization is *not* feasible without sharing personal information, and *free* allowance of services is not feasible without some exploitation of this information by the vendor.

Research on the legal and ethical aspects of privacy has argued that privacy is not a fundamental human, moral, or absolute right; rather, it is a prudential right [39]. In fact, in the U.S. judicial context, privacy has been largely treated as a "highly subjec-

tive and contingent commodity, a matter of tradeoffs and balanced interests" [5, p. 14]. Behavioral research also suggests that consumers are more likely to accept loss of privacy if it accompanies some benefit [23]. In this regard, an important contribution of our research is the economic formalization of this nonmonetary exchange so as to investigate social welfare-maximizing approaches for a regulator.

Our model assigns consumers a *property right* to their information where they are willing to trade it for certain benefits based on some "privacy calculus" [13]. The alternatives available to the regulator are modeled along two dimensions: (1) *Allowance of technological enforcement:* (a) allow the use of a technology that enforces a consumer's agreed-upon service level and (b) disallow the use of enforcement technologies. (2) *Provision for private contracts:* (a) allow vendors to buy information that is beyond what a consumer will share to satisfy his or her personalization needs (private contracts) and (b) disallow vendors from buying information. In the absence of a formal structure and analysis of the regulatory problem, intuition might lead one to believe that enforcement technologies by their design might be bad for the society or vendors should be prohibited from engaging in private contracts to buy information. Our formal modeling allows us compare these options and arrive at results, some of which are counter to intuition.

Model

The focus of our research is to identify optimal regulator strategies in the market for information. Generally, the need for regulator intervention is greater in monopolistic markets where the monopolist's impact on consumer welfare can be quite severe. We consider a market for information under a monopoly, where there is an online vendor who sells some good z and offers a set of personalization services along with the good.

The Market for Information and Privacy

Recent research points toward the need to examine markets for customer information in the context of privacy [44], where it has been suggested that "there is an active market for personal consumer information served by such web-based marketing firms as Double Click and I-Behavior" [44, p. 632]. Others [37, 46] note that many online firms collect and sell both personally identifiable and anonymous individual information suggestive of a market for personal and preference information. The proliferation of online portals and the increasing number of personalized services (in exchange for information) offered by portal majors such as Google, Yahoo, and MSN is a testament to the growth of this market. In addition, personalization of services that accompany a product browsing/purchase experience is also very prevalent and is an important aspect of online selling [6], as, for example, an online vendor such as Amazon.com that employs various data mining techniques to provide personalized product/gift/shipping and other recommendations to the consumer.

This market of consumer information has emerged in the online context due to three important factors: (1) *Personalization technologies:* data mining techniques such as rule-based and collaborative filtering [36, 52] that can use personal and preference information (acquired voluntarily or through monitoring browsing behavior) and tailor future online services to an individual's needs. For example, new document-clustering techniques have emerged to manage Web pages into categories that facilitate document management and subsequent access and browsing [50]. (2) *Convenience to consumers:* the convenience value (and hence the reduction in opportunity costs) created by having myriad services tailored to one's own tastes, particularly free of charge. (3) *Vendor's access to information:* the value that vendors place on knowing consumers' preferences.

Personalization Technology

While personalization depends on how much information is shared (voluntarily or through monitoring) with the service provider, personalization technologies determine how many such services can be offered. For example, providing one's home address to Google allows it to "autofill" this information when choosing shipping or credit card options with some Froogle vendors. In addition, to a user who subscribes to Google's personalized Web page, this information is also used to provide recommendations for movie listing/timings in the home area, maps and traffic information, as well as common information such as weather and television listings. Amazon.com's superior personalization technologies also allow for personalized recommendations, discounts, coupons, and shipping/gift options based on browsing behavior. But not all online vendors are capable of offering the same number of personalized services even if they may be acquiring the same amount of information. For a given amount of consumer information the level of personalization technology determines how many personalized services can be created. This information-services mapping is given by $g^{-1}(i) = s$, where i is customer's preference information, s is the personalization services, and $g^{-1}(.)$ is the current state of personalization technology.

We assume that the marginal rate of personalized services that can be provided decreases with increasingly personal information as the ability to tailor services becomes increasingly difficult. This implies that $g^{-1}(.)$ is concave or $g(.)$ is a convex function. Because no personalization can be provided in the absence of customer information, we have $g(0) = 0$, and if I represents the entire information set that can be used to describe consumers and their preferences, then we have $g^{-1}(I) = S$, where S is the maximum possible service set for a given state of personalization technology. Any *affine* transformation function will suit this abstraction.

Consumer's Personalization-for-Privacy Trade-Off

Personalization is infeasible to achieve without loss of privacy [49]. Research on privacy informs us that consumers are willing to disclose their personal information in exchange for some economic or social benefits [8, 23]. An individual's decision to

share information is said to be based on a "privacy calculus" that is the individual's assessment of benefits and costs from sharing his or her information [12].

The primary benefit to a consumer from using personalization services is captured by a marginal value for personalization parameter p such that the benefit to consumer is increasing and linear in the number of services consumed. Prior research on services marketing has argued that consumers value individualized treatments. This research suggests that the perceived quality of service is dependent upon how a consumer perceives his or her individual needs to be met [27]. Personalized services can also reduce information overload and hence increase user satisfaction [25]. The convenience value that personalization provides can also be understood as the opportunity cost incurred by an individual in the absence of personalization. This is often observed in luxury goods and services markets, where the allayment of opportunity cost is extracted through a price premium. Business executives who have a high opportunity cost of time often prefer to stay in high-end hotels that charge a premium but personalize rooms and services to their specific tastes and requirements [26]. The importance of this convenience may vary from one individual to another. Recent empirical research finds that these variations in consumers' value for personalization strongly influence their intention to use online personalization [8].

The willingness to share information is known to be related to an individual's perception of risks of disclosure [14], and thus individuals vary in their concerns for privacy [8]. In prior research in economics [44], privacy is captured by an individual's valuation for a product being kept as private information, and the corresponding cost is the extra price that the vendor will charge upon knowing the true valuation (thus the consumer does not want to share this information). In our work, we introduce an individual consumer's privacy cost coefficient r such that the cost of using s personalized services by sharing i information is given by ri^2. Note that this abstraction of privacy cost coefficient is consistent with our definition of privacy as some intangible cost suffered by each individual. Independent of what the vendor may do with this information, this coefficient captures the consumer's belief regarding his or her comfort in sharing personal information. The privacy cost is assumed to be convex as information is ordered and increasingly personal information needs to be shared by the consumer in order to use more personalized services. Hence, the consumer's net benefit from using personalization can be written as $v_c(s) = ps - rg^2(s)$. Note that $v_c(s)$ is an inverted U-shaped (nonmonotonic and strictly concave) function in s, suggesting that using more services is not necessarily better for a consumer. This utility is characteristic of goods with no-free-disposal. If a consumer derives a certain value $V(z)$ from consuming the good z and if $P(z)$ is the price that the consumer pays for the good, then the net utility to an individual in consuming the good z and the personalized services s is given by $U(z, s) = V(z) - P(z) + v_c(s)$.

Vendor's Costs and Benefits of Offering Online Personalization for Free

Online vendors do not directly charge a price for personalization services, but they derive other benefits from investing in personalization. The most obvious and direct

value of consumer information is the revenue from sharing or selling preference information to supply-chain partners and advertisers. For example, many portals, newspapers, and other Web sites are attractive to advertisers not only because of the number visitors to the site but also because of their ability to create reasonably accurate customer profiles leading to targeted advertising efforts. Recent research has elaborated on the role and importance of Web-based personalization in acquiring customer information for other important purposes as well [30, 51].

Personalization allows a vendor to not only acquire transactional information from purchases but it also helps him or her in acquiring information about browsing and other actions of the consumer that may not have translated into a fiscal transaction. This information can help differentiate a vendor from his or her competitors and allows him or her to understand demand, manage inventory, and create an efficient supply chain. Production paradigms such as just-in-time (JIT) owe their success to managing information. On the marketing end, customer information is crucial for price discrimination and segmentation. It has been argued that marketing strategies of successful firms depend on access to and effective use of detailed customer information [1, 3, 12, 17, 32, 34].

All online vendors do not value customer information at the same level. Those vendors who rely on maintaining smaller inventories and an efficient supply chain would place a greater emphasis on knowing their customers better as compared to vendors who can manage large product inventories and mainly target a homogeneous group of customers. For example, it has been suggested that online vendors with a real-time supply chain and those dealing with digital products have greater value for customer information due to the "on-demand" production and delivery requirements in such environments [2]. To capture this heterogeneity, we introduce a marginal value for information parameter α such that a vendor's benefit from acquiring information i, by offering personalization services s, is given by αi or, equivalently, $\alpha g(s)$.

The marginal cost of providing an online service is negligible; however, there are capital or one-time costs incurred by the vendor. Broadly there are three types of *capital* costs involved in providing personalization services—infrastructure, trust building, and information protection or liability costs. The infrastructure costs mainly arise from investments in personalization tools such as collaborative filtering systems, and rule-based engines that are built into customer relationship management (CRM) systems [21]. The ability to collect information depends upon consumer trust in retailers [19], and this trust is intrinsically linked to the reputation of a firm [15, 38, 47]. In the online world, reputation of a firm can be enhanced through trust-building activities such as alliances with trusted third parties, implementation of security mechanisms, reassurances through disclosure notices, and compliance with FTC rules [35]. Vendors also need to protect the information they acquire and store. They invest both in technological protection mechanisms [24] and in having a legal infrastructure. The magnitude of these investments is domain dependent since the U.S. Congress [35] stipulates context-specific requirements and guidelines, such as the Children's Online Privacy Protection Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA) [4, 18, 40]. As the nature of information acquired is increasingly personal

with increasing number of services, the capital costs are assumed to be convex while the *marginal costs* of serving an additional consumer remain *zero.*

We introduce a cost coefficient β such that the net capital costs are convex in the total number of services offered, given by βs^2. We can now write the profit (v_v) from offering personalization services s as $v_v(s) = \alpha g(s) - \beta s^2$. $v_v(s)$ is a nonmonotonic strictly concave (inverted U-shaped) function in s, such that there is an interior optimum given by $s_v^* \in (0, S)$ that is the solution to $\max_s \alpha g(s) - \beta s^2$, where $g''(s) < (2\beta/\alpha)$, $\forall s$. The intuition behind this is that while vendors are still finding innovative ways to use consumer information, the information acquisition technologies are evolving at a much more rapid pace. This would imply that the feasible set of personalization services is generally greater than the vendor's ideal number of services. We can now write the vendor's net profit from selling a good z, and offering personalization services s as $\pi(z, s) = R(z) - C(z) + v_v(s)$, where $R(z)$ is the revenue from and $C(z)$ is the cost of product z.

The Regulator's Problem

In the United States, any commercial transaction that involves the collection and use of consumer information falls under the legal purview of the FTC. Privacy issues also receive considerable attention from other governmental and nongovernmental entities, including the media. The opinions of these groups vary across the protection spectrum; while some hold consumer privacy sacrosanct and argue that consumer information should not be collected in any event, it is now generally accepted that consumer information can be collected and used as long as the data gathering entity conforms to the fair information practices principle recommended by the FTC. While legislative bodies and popular press routinely discuss the threats to consumer privacy, what is missing, however, is an academic debate on the formulation of ideal legal frameworks that take into account the technological, behavioral, and economic rationale in the collection and use of consumer information.

For example, should the FTC take the view that the threat to consumer privacy is so severe that society is better off by restricting vendors in their information acquisition strategies? Or should the FTC take the approach that consumer information is really a property that the consumer owns and the vendor values, and should therefore allow the vendor and consumer to exchange this property through mutual agreements? There are two dimensions along which the regulator can directly influence vendor/consumer behavior and thus the market outcome: (1) by allowing/disallowing certain usage-enforcing technologies and (2) by allowing/disallowing "buying" of information (or selling of services).

As discussed earlier, consumers prefer an ideal level of personalization services depending upon their personalization for privacy (p4p) ratio. However, it is possible for vendors to require consumers to use certain enforcing technologies such as browser-helper objects (BHO) that can force consumers to accept monitoring of information that may be above their preferred level. Note that consumers may still sign up to use this suboptimal level of services as they may still be enjoying positive utility. Many

Table 1. Regulatory Choices

Allowance of	Private contractual agreements	
Technology for usage enforcement	Regime 1 (R1) Vendor is *not allowed* to "buy" information *and* he or she is *not allowed* to use technologies that enforce usage.	Regime 4 (R4) Vendor is *allowed* to "buy" information *but* he or she is *not allowed* to use technologies that enforce usage.
	Regime 2 (R2) *Vendor* is *not allowed* to "buy" information *but* he or she is *allowed* to use technologies that enforce usage.	Regime 3 (R3) Vendor is *allowed* to "buy" information *and* he or she is *allowed* to use technologies that enforce usage.

legitimate vendors employ personalization toolbars with BHOs, but it is the rampant misuse of such technologies that has led to spyware concerns. Thus, there has been a clamor from one section of privacy advocates for a complete ban or disallowance of these technologies. Further, some vendors have also begun to offer incentives (in the form of coupons/discounts) for the usage of information-acquiring technologies such as toolbars, which literally amounts to "buying" customer information. Intuitively, it might appear that a summary ban of these vendor strategies might be best from the society's point of view, particularly in light of concerns associated with consumers' privacy protection and vendors' monopoly power in this market.

However, it is not clear if such an outright disallowance will be welfare maximizing for two reasons: (1) the unique no-free-disposal nature of the utility function (the nonmonotonic concave shape) might endow the consumer with some control, and (2) prior legal research has argued that contracts between buyers and sellers may be the most appropriate tools for protecting information privacy [48]. Hence, we formally examine welfare implications when a vendor is confronted with each of the regulatory regimes outlined in Table 1. A popular perspective might suggest that regime 1 is ideal for the consumer (society) and regime 3 is perhaps the harshest.

To investigate the true nature of each of the regulatory regimes, in the following section, we study a monopolist's optimal market strategy and the resulting consumer surplus and social welfare. Further, in this context, we analyze if there are any taxation policies that could be employed by the regulator to benefit society.

Regulatory Regimes and Monopolist Strategies

We consider a vendor who cannot extract any separate price premiums for personalization—that is, he or she does not charge the consumer for using personalization services. This is consistent with the strategies of online vendors such as Amazon.com or Barnes & Noble (www.barnesandnoble.com) that do not explicitly charge for providing

Table 2. Objective Functions and Strategy Space

	Strategy space	Objective function	Constraints
Consumer	$i \in [0, I]$	$\max_s ps - rg^2(s)$	$ps - rg^2(s) \geq 0$ $s \geq 0$
Vendor	$s \in [0, S]$	$\max_s \alpha g(s) - \beta s^2$	$\alpha g(s) - \beta s^2 \geq 0$ $s \geq 0$
Regulator	Regulatory regime $\in$ {R1, R2, R3, R4}	$\max_s\{ps - rg^2(s) + \alpha g(s) - \beta s^2\}$	$ps - rg^2(s) \geq 0$ $\alpha g(s) - \beta s^2 \geq 0$ $s \geq 0$

personalized recommendation or other services. While this consumer surplus cannot be extracted as prices, vendors maintain this surplus to the consumer as it translates to loyalty and increased switching costs. Thus, in our model, $P(z)$ and service level s are two independent decision variables for the vendor. As a monopolist, the vendor will set a price $P(z) = V(z)$ such that $U(z, 0) = 0$. Therefore, in order for us to examine the service level that will be offered by the vendor, we need to only consider the portion of the vendor's profit from personalization services $v_v(s) = \alpha g(s) - \beta s^2$ and the portion of the consumer's utility that is derived from personalization—that is, $v_c(s) = ps - rg^2(s)$. Before we analyze vendor strategies, we first elaborate on the nature of the consumer's usage of personalization services as outlined in Table 2.

Lemma 1: A consumer's maximum ($s_c^0|_{v_C(s_C^0)=0}$) *and utility-maximizing* ($s_c^*|_{arg\ max_s\{ps-rg^2(s)\}}$) *number of services are increasing in the consumer's p4p ratio (p/r).*

Proof: See the Appendix.

The p4p ratio is a critical parameter for analysis of consumer behavior in this market. It not only determines the consumer's indifference point but also determines the consumer's optimal behavior if the consumer has full freedom to choose his or her service level. A large value of the p4p ratio is representative of consumers who derive high benefits from personalization services or possess low concern for privacy, whereas a lower value of this parameter is indicative of the privacy-sensitive types. Based on the p4p ratios, we define a market to consist of two consumer types; a *convenience seeker* whose p4p ratio is high enough such that he or she will prefer more services than the market offering and a *privacy seeker* with a low p4p ratio such that his or her ideal, preferred number of services is lower than the market offering (Definition 1).

Definition 1: Convenience seekers ($\overline{p4p}$) *are those whose p4p ratio (p/r) is such that their utility-maximizing number of services* $s_c^* \geq s_v^*$ *and the privacy seekers* ($\underline{p4p}$) *are those whose p4p ratio is such that their utility-maximizing number of services* $s_c^* < s_v^*$, *where* $s_v^* = arg\ max_s\{\alpha g(s) - \beta s^2\}$.

Figure 1 shows the relative preferred service level for the two consumer types with respect to the vendor's optimal service level. From a vendor's perspective, when

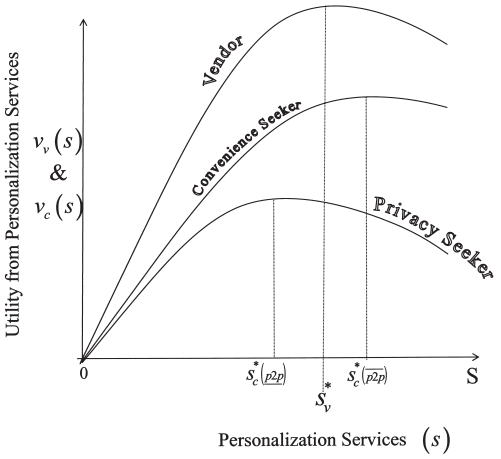

Figure 1. Profit Function of the Vendor and Utility Functions of the Two Consumer Types

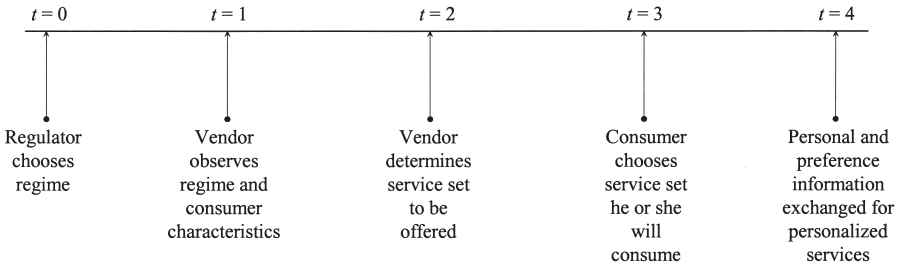

Figure 2. Sequence of Events

consumer types vary significantly in their preference for personalization services, the vendor should seek separate strategies for each consumer type. Such an approach is consistent with prior economics literature, where a monopolist in an experience goods market divides his or her consumers into optimistic and pessimistic types depending upon whether they overestimate or underestimate his or her product's quality, and pursues very different strategies for each of these consumer types [41]. Others have also used this approach of exploring separate strategies such as when consumers overestimate and underestimate the fit of digital goods to their tastes [7]. The timing of strategic interaction between the monopolist and the consumer is given in Figure 2. Now we analyze the monopoly strategies under each regulatory regime.

Regulatory Regime 1

Regulatory regime 1 describes a setting where the regulator restricts the monopolist from both employing a usage-enforcing technology and from engaging in private contracts. This environment is descriptive of simple Web-based personalization (with no

toolbars or BHOs) where the consumer fully self-selects from the set of services offered by the vendor. In our personalization context, the consumer does not pay a dollar value for personalization but rather pays in the form his or her information. For a given set of services, if the consumer provides information about his or her preferences, then he or she gets services that are tailored to his or her taste. When no technological usage enforcement is in place, the consumer will simply use his or her utility-maximizing level of services. From the shape of the utility function, we can see that this service level may be equal to or lower than the market offering depending upon whether the consumer's utility is still increasing or decreasing at that point.

Regulatory Regime 2

Now consider the situation where the regulator allows the use of cookies, BHOs, and other technologies that can be embedded inside of Web pages and toolbars. In this situation, a vendor can create a toolbar with a certain fixed number of services such that a consumer who installs the toolbar is necessarily monitored for those pieces of information (and hence provided corresponding personalized services). For example, Google allows consumers to choose the number of services that will be personalized on its toolbar, but users of its Gmail service cannot opt out of receiving personalized advertisements based on a system that actually scours through a user's e-mail. Similarly, consider the case of the free RealAudio service; a consumer who values a personalized radio service can voluntarily indicate his or her preferences for various music genres, but he or she can also be forced to provide other personal information (often an asterisk [*] next to fields indicates that filling them in is compulsory), such as an e-mail address—without which the service may be unavailable. Yahoo e-mail becomes unavailable if a consumer turns the "cookies" feature off (as this is the mechanism through which the vendor tracks usage).

Lemma 2: Under regime 1, a monopolist will offer s_c^* to the privacy seeker ($\underline{p4p}$) and offer s_v^* to the convenience seeker ($\overline{p4p}$), whereas under regulatory regime 2, the monopolist will offer $\min\{s_c^0, s_v^*\}$ to the privacy seeker ($\underline{p4p}$) and offer s_v^* to the convenience seeker ($\overline{p4p}$).

Proof: See the Appendix.

s_v^* is the utility-maximizing number of services for the vendor—that is, the vendor's preferred set of services—and because the convenience seeker's utility is increasing at s_v^*, he or she will use all of the services offered by the monopolist irrespective of the regime. However, the behavior of the privacy seeker is closely tied to the regulatory regimes. By definition, the privacy seeker's utility-maximizing set of services or his or her ideal service level is less than that of the vendor. The nonmonotonic and strictly concave nature of the consumer utility implies that the marginal benefit from consuming personalization services is outweighed by the marginal loss from providing private information at any service level above s_c^*. Under regime 2, when the vendor can enforce usage, he or she only needs to consider whether or not the consumer will

participate. If $v_c(s_v^*) \geq 0$, then the vendor will offer s_v^*, and since the vendor's profit curve is always increasing at any service level less than s_v^*, he or she will prefer to offer the maximum number of services that the privacy seeker will use—that is, s_c^0. However, under regime 1 in the absence of any enforcement technologies, the monopolist is unable to exercise his or her market power in offering personalization services as the privacy seeker will choose his or her preferred service level—that is, his or her s_c^*. As any services above this level will imply a wasteful investment, the vendor will simply find it optimal to provide s_c^*.

Proposition 1: The regulator may be indifferent between regimes 1 and 2 (allowance and disallowance of enforcement technologies) under either of the following two conditions:

(a) The market is primarily defined by convenience seekers—counter to intuition, the allowance/disallowance of such a technology has no bearing on the consumer, producer, and social welfare when the market is defined by convenience seekers.

(b) The market is primarily defined by privacy seekers and the monopolist's investment in enforcement technologies is greater than $v_v(\min\{s_c^0, s_v^*\}) - v_v(s_c^*)$. *The vendor gains monopoly power with enforcement technologies only with privacy seekers (the consumer surplus of this type becomes zero as in any monopoly).*

If both conditions are not met, the regulator should strictly prescribe regime 1.

Proof: See the Appendix.

The intuition behind P1 is that a combination of distribution of types and the no-free-disposal nature of the utility function can prevent the monopolist from exercising his or her power and thus obviating the need for regulation. However, the need for regulatory mechanics becomes evident with the decreasing costs of sophisticated technologies that can be used to enforce certain levels of information monitoring and usage. So, the only situation over time where the regulator need not step in is where the consumers' need for personalization services increases along with technological sophistication of enforcing technologies. While this is clearly a burden to be borne by vendors of personalization technologies, an alternate possibility is that regulators invest in consumer education such that the overall level of privacy concern decreases with increasing understanding of personalization technologies.

It is also critical for us to understand the privacy seeker's behavior as it may partly explain the failure of some business models on the Internet that were based solely on their ability to acquire and sell customer information. Many portals and e-tailers operate on the notion that even if a product may be sold at cost price, profits could still be realized through selling and sharing consumer preference information. These business models operate on the expectation that intense price competition will attract large numbers of consumers and information on them and their preferences can be mined so as to be attractive for product placements and advertisements. Commonly, the failure of some of these business models has been attributed to exaggerated valuation

on customer information. However, it may indeed be that the firms were faced with privacy seekers who only used their optimal level of services and therefore provided information below the online vendor's expectations.

The cost of enforcement can be understood in another way as well. It could also be interpreted as the burden that the vendor is willing to place on the consumer without the fear of losing him or her. For example, Microsoft Passport will disable a consumer's account after a certain period of inactivity, thus forcing the user to reregister, but such an action may be of great inconvenience to the user due to lost e-mail and reconfiguration of stock portfolio and other personalized services. This raises the possibility that the user may altogether abandon using Passport services. Thus, even if the provision for enforcement exists and the investment costs are also not high, the monopolist needs to consider the burden on the consumers in adopting such technologies.

Regulatory Regime 3

When a monopolist has high information needs, he or she may not restrict him- or herself to acquiring information through consumers' need for personalization alone. The monopolist may in fact choose to provide other incentives (in addition to the convenience from personalization), such as coupons, discounts, and even small monetary rewards, to motivate the consumer to perhaps use more services than optimal in a pure personalization–privacy exchange. Many online vendors, including Amazon.com, have introduced incentives in the form of discount coupons based on consumers' clicking through its Gold Box services and sharing certain information. From a privacy advocate point of view, such strategies may amount to "buying" information through some private contract and hence flag privacy concerns. Thus, from a regulator's point of view, one needs to evaluate the implication of allowance of such private contracts offered along with personalization services. Clearly, a monopolist will need to engage in such contracts only when he or she has to incentivize the consumer to use beyond s_c^* and, as discussed earlier, the presence/absence of enforcing technologies become relevant due to the inverted-U nature of the utility function. Hence, we first consider regime 3 where the regulator allows for private contracts as well as the use of enforcing technologies.

Under the allowance of information "buying," let the vendor and the consumer engage in a private contract through a transfer good (τ). We develop these contracts between the provider and the consumer through a bargaining mechanism. In economics literature [31], bargaining is employed in situations in which (1) the strategic players (agents) have the possibility of negotiating a mutually beneficial agreement, (2) there is a conflict of interest about which agreement to conclude, and (3) no agreement may be imposed on players without their explicit approval. In our context, when there are no enforcement capabilities, the vendor is forced to offer s_c^* to the privacy seekers. At this point, one agent's (vendor's) surplus is increasing in the number of personalization services, while the other's (privacy seeker's) is decreasing, and hence the second and third conditions for bargaining as discussed above clearly exist. There is a conflict of interest around the number of personalization services, and due to lack of enforcement

capabilities, the privacy seeker will not use any services above s_c^* even if he or she derives a positive utility. Therefore, in order to create an agreement point as required by the first condition, we introduce the transfer good into both the vendor and the consumer's utility, with the assumption that when the consumer agrees to receive a transfer payment, he or she also agrees to be monitored. Thus, the vendor is guaranteed that the consumer will use all of the agreed-upon services irrespective of whether it is more or less than the consumer's optimum. Note that the transfer good that the vendor is now willing to provide will depend on the agreed-upon service level. We can now formally rewrite the vendor and consumer's utility from personalization as

$$\begin{aligned} v_v(s) &= \alpha g(s) - \beta s^2 - \tau(s) \\ v_c(s) &= ps - rg^2(s) + \tau(s). \end{aligned} \tag{1}$$

Lemma 3: In order to determine the optimal incentive ($\tau(s)$), the vendor and privacy seeker will bargain over $\beta_\pi(s_B) = max_s\{(v_c(s) + v_v(s)) - (v_c(s_c^*) + v_v(s_c^*))\}$, where the solution ($s_B$) to the maximization problem is the agreed-upon personalization service level under regime 3.

Proof: See the Appendix.

In regime 3, the monopolist's problem and the consumer's problem are not independent of each of other and hence we cannot simply maximize their respective utilities. Further, the problem is also not one of simply maximizing the combined utilities as we also need a mechanism that provides the incentives for both parties to enter into contracts. Therefore, we adopt an axiomatic bargaining framework to identify the solution set as first described by Nash [28]. The basic setting states that there are players who bargain with each other and either reach an *agreement* in a set A, or fail to reach an agreement, in which case the *disagreement event* D occurs. The set of all utility pairs that can be the outcome of bargaining is the union of the set Θ of all pairs $(u_1(a), u_2(a))$ for $a \in A$ and the point $d = (u_1(D), u_2(D))$, where $u_1(.), u_2(.)$ are the utilities of the players engaged in bargaining. The pair $\langle \Theta, d \rangle$ is the primitive of the bargaining problem. If there exists a bargaining solution to our problem, then our solution should belong to a set Θ that satisfies the axioms of invariance to equivalent utility representations (INV), symmetry (SYM), independence of irrelevant alternatives (IIA), and pareto efficiency (PAR) [31].

Therefore, we construct our set Θ, and formally describe the disagreement point d to get the utility pairs $\langle \Theta, d \rangle$. The utility pairs are constructed from the set of possible agreements (set A) and the disagreement event (D). In the case of privacy seekers, the disagreement point D in context is s_c^*, the point where the privacy seeker feels satisfied while the vendor stills feels he or she can do better. This process can be described as one where the privacy seeker agrees to use some $s > s_c^*$ in return for some amount of the transfer good τ. And if no agreement is reached, then both parties will revert to the point where the conflict of interest first appeared—that is, s_c^*—and the vendor will provide no incentive or transfer good at this point. Hence, D can be formally represented as $D = \{s_c^*, 0\}$ (Figure 2). Now we identify the feasible set A for the agents. The feasible set represents all possible agreement points starting from the

disagreement point $\{s_c^*, 0\}$. In our context, the vendor will offer any $s > s_c^*$ and will provide some τ_c as long as his or her utility from doing so is at least as much as at the disagreement point. Similarly, the consumers will use the set of services and accept the transfer good as long their utility is greater than or equal to what they enjoy at the disagreement point. Hence, our feasible set $\{s, \tau\}$ for the privacy seekers and the vendor should satisfy

$$\begin{aligned} v_c(s) + \tau(s) &\geq v_c(s_c^*) \\ v_v(s) - \tau(s) &\geq v_v(s_c^*). \end{aligned} \tag{2}$$

The feasible region for this incentive lies above the frontier given by $v_c(s_c^*)$, which is the utility the consumers get at the disagreement point. The increasing convex shape of the iso-utility curve for the consumer is because, after s_c^*, the utility from the exchange surplus is concave and decreasing. Hence, the rate at which $\tau(s)$ is increasing with s corresponds to the rate at which $v_c(s)$ is decreasing in s. Hence, the feasible region for the consumers represents a compensation that is more than or equal to the loss in utility due to using services higher than their optimal. Similarly, the vendor's feasible region of offering this incentive $\tau(s)$ lies below the frontier given by $v_v(s_c^*)$. The shape of the vendor's iso-profit curve is concave, as he or she can provide increasing $\tau(s)$ as his or her own profit is increasing until s_v^*. After this point, the vendor's profit begins to decrease (recall the nonmonotonic concave nature of the vendor's profit function in s) in services so the amount of transfer good he or she can offer also decreases. The vendor cannot offer any transfer good after some service level $\exists s : v_v(s) < v_v(s_c^*)$. Note that a rational vendor will not choose to offer any service greater than s_v^*, as the utility of both agents are decreasing beyond this point. Therefore, the intersection region A in Figure 2 is the feasible set of agreement points for our bargaining problem. The feasible set of agreement points can then be written as

$$A = \{(s, \tau(s)) : v_c(s) + \tau(s) \geq v_c(s_c^*),\ v_v(s) - \tau(s) \geq v_v(s_c^*),\ s \geq s_c^*,\ \tau(s) \geq 0\}. \tag{3}$$

As discussed in the beginning of this subsection, we now construct the utility pairs $\langle \Theta, d \rangle$. The point $d = (v_c(s_c^*) + 0, v_v(s_c^*) - 0)$ is the utility to the two agents at the disagreement point. Within the region A, the set of agreement points corresponding to $s = s_B$ represents the values of transfer good $\tau(s)$ where the combined exchange surplus is maximized. Mapping the feasible set to the utility plane of the consumer and vendor, we get the solution set Θ. The frontier of the solution set represents the line corresponding to service level s_B and all feasible values of the transfer good $\tau(s)$. As we observe from Figure 2, our solution set Θ is compact and convex.

Lemma 4: In regulatory regime 3, the monopolist will provide the privacy seeker an incentive given by $\tau(s_B) = ((v_c(s_B) + v_v(s_B)) - (v_c(s_c^*) + v_v(s_c^*))/2$ *for which the privacy seeker will agree to use the service level* $s_B = s_w^* < s_v^*$.

Corollary 1: Even when the vendor faces convenience seekers, it is optimal for him or her to engage in private contracts and he or she will offer some $s_B = s_w^* \geq s_v^*$, *and charge a fee given by* τ *in Lemma 4.*

Proof: See the Appendix.

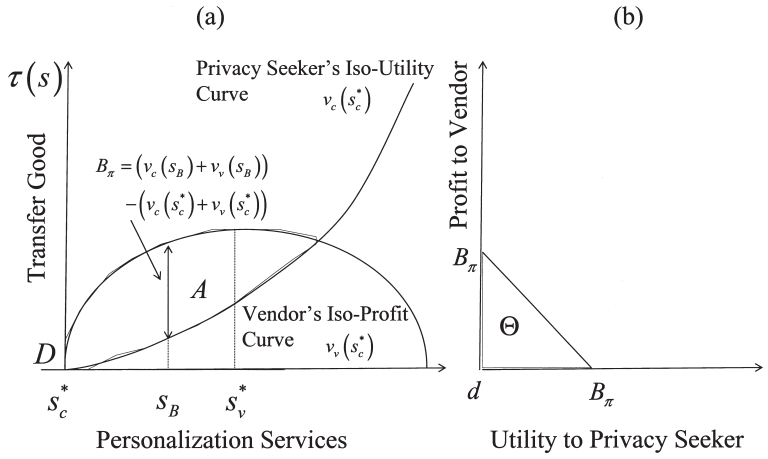

Figure 3. Bargaining Solution Set

The simple intuition behind Lemma 4 is that under regime 3, the vendor extracts a greater profit from personalization, and by giving back some of the profit to the consumer, the vendor makes the consumer better off as well. The bargaining framework helps in deriving the optimal service level that would serve as the agreement point and the amount of incentive that the vendor has to provide to the privacy seeker. By developing the problem along the lines of an axiomatic bargaining setup, we were able to reduce it to the equivalent of dividing a fixed pie, or better known as dividing the dollar problem [31]. Without loss of generalizability, and in order to provide an analytically tractable value for the incentives, we assume that both of our agents have the same preferences over the exchange surplus. Note that this assumption merely implies that both agents have the same attitude toward risk.

The problem can be divided into two parts: (1) to seek the largest pie and (2) the decision on how to split it. In order for the bargaining process to work, the consumer has to agree to a private contract in addition to his or her use of personalization services as this is the only way the vendor can ensure that the consumer provides the promised information. Because the privacy seeker can get his or her surplus-maximizing level of personalization services in the absence of enforcement capabilities, any contract he or she agrees to has to provide him or her a higher utility. The bargaining solution tells us that the pie is maximized at s_w^*, representative of the social welfare maximization point (Figure 3). Because the vendor's profit has now gone up from $v_v(s_c^*)$ to $v_v(s_w^*)$, he or she provides part of this excess to the privacy seeker such that the new utility is greater than $v_c(s_c^*)$. Therefore, not only are the two involved parties better off but because the agreed-upon service level is s_w^*, the welfare is also maximized (Figure 4).

While Amazon.com provides a broad range of personalization services, more recently it also introduced new ways through which the consumer is incentivized to provide more information than he or she would normally share in the course of using his or her optimal level of personalization services. One type of incentive that Amazon.com pro-

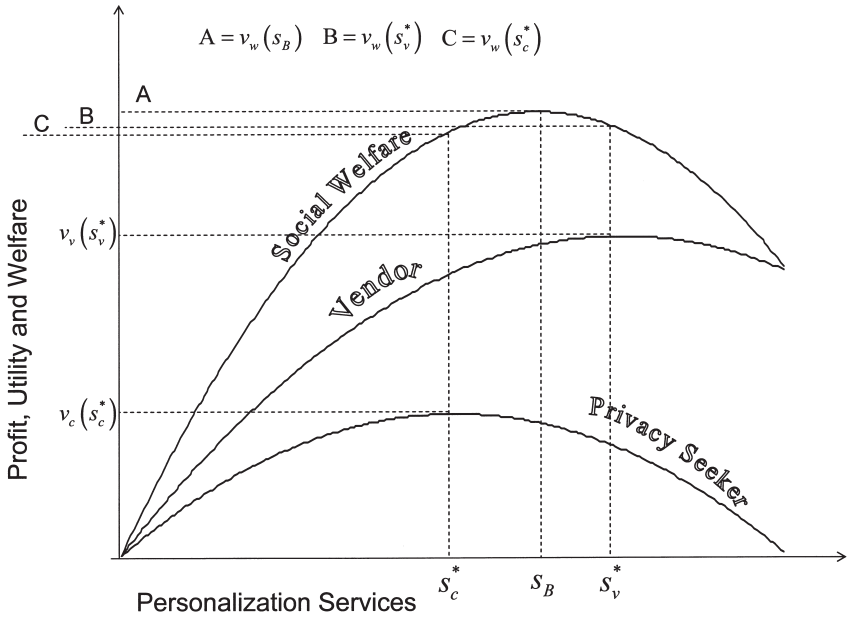

Figure 4. Producer and Consumer Surplus and Social Welfare

vides is through the Gold Box program wherein it discounts products from its current inventory attracting the consumers to browse through this list. Some of the offerings in this list are not individual items but consumers are asked about product categories in which they would most likely be interested. Thus, even if the consumer eventually does not buy a product, he or she has provided some information on his or her preferences as he or she hunts for a sale. Further, the store also incentivizes consumers to part with their friends' and family members' e-mail addresses by promising to send coupons of related products. Clearly, this is a piece of information that a consumer is unlikely to provide if he or she only used the optimal level of personalization services. More recently, Amazon.com has even been offering $0.05 to consumers to induce them to answer simple questions about their product preferences.

Proposition 2: Counter to intuition, when a regulator allows private contracts in the market for information, the consumer, producer, and social welfare are maximized only when usage enforcement is allowed. Alternatively, when the regulator allows private contracts in the absence of usage enforcement or vice versa, at least one party (vendor/consumer) is necessarily worse off.

Proof: See the Appendix.

Our results suggest that even when regulators do not allow vendors to directly buy consumer information (in order to protect privacy), the firms can pursue a property rights approach in the well-defined context of personalization and to the benefit of the consumers as well as the society. Our approach converges to Coase's [11] observation that if property rights are initially assigned and valuations are known, then bargaining

will lead to a socially efficient outcome. An important aspect of our results is that the consumer gains a utility that is even greater than his or her maximum utility from only using his or her optimal personalization services. Thus, incentive for the consumer to participate in bargaining is naturally built in, while also maximizing the welfare to the society. The incentive for the vendor to participate in such contracts is also naturally present if he or she is unable to exercise his or her monopoly behavior.

During the allowance of enforcement technologies, the regulator can alternatively consider a form of taxation that can be beneficial to the society. While the consumers do not pay a "price" for the use of services, they pay in the form of information and the regulator can possibly tax the vendor's collection of this information. Such a tax would be equivalent to the Pigovian tax [33] that is typically imposed in the context of pollution where there are negative externalities and the polluter pays a tax in proportion to the units of good he or she produces. The Pigouvian tax leads to the internalization of externalities in the producer's profit function. In our context, the regulator can theoretically impose a tax on the vendor that takes effect from the point ($\forall_s > s_c^*$) where the use of services gives a negative marginal utility to the consumer. The optimal tax will be designed by the regulator such that the vendor's profit-maximizing level of service (where profit function now includes the tax to be paid) will be the same as the welfare-maximization level of service (s_w^*), and tax imposed on the vendor will be given by $-v_c'(s_w^*)$. There are two points to be noted regarding the taxation: First, the welfare is maximized but unlike in the bargaining context, the excess profit is paid to the government. Second, the Pigovian tax has generally been criticized as being unrealistic; as for the optimal solution, it is required that the regulator know the characteristics of the vendor and the consumers (i.e., α, β, p, r). It is perhaps more realistic to presume that vendors and consumers know each other's characteristics (as required in the bargaining approach) rather than the regulator's knowledge of the same.

Regulatory Regime 4

Regulatory regime 4 describes the situation where the regulator allows private contracts but does not allow the monopolist to incorporate any sort of enforcement technology that can externally allow him or her to ensure the usage of a particular level of service. It is apparent that under such a regime, the monopolist will not engage a privacy seeker in private contracts. In the absence of an external technology, the privacy seeker might initially agree to use $s_w^* \geq s_c^*$ and collect his or her $\tau(.)$ but might continue to use his or her s_c^* level of services or perhaps even misrepresent information between $s_c^* \leftrightarrow s_w^*$. Thus the monopolist will expect the privacy seeker to use his or her s_c^*. However, in the case of convenience seekers, because $s_c^* > s_w^*$ (i.e., these types want more services than what is offered), there is no need for external enforcement and, indeed, there is a guarantee of usage because the consumer pays the vendor for the provision of services greater than s_v^*. We summarize the results of the different regimes in Table 3 and proceed to provide their numerical illustration along with welfare implications next.

Table 3. Results Under Different Regulatory Regimes

	No private contracts	Private contracts
No usage enforcement	Regime 1 Vendor will offer s_v^* Consumers will choose: • Privacy seeker s_c^* • Convenience seeker s_v^*	Regime 4 Vendor will offer s_w^* Consumers will choose: • Privacy seeker s_c^* • Convenience seeker $(s_w^*, -\tau(s_B))$
Usage enforcement	Regime 2 Vendor will offer s_v^* Consumers will choose: • Privacy seeker $\min\{s_c^0, s_v^*\}$ • Convenience seeker s_v^*	Regime 3 Vendor will offer s_w^* Consumers will choose: • Privacy seeker $(s_w^*, \tau(s_B))$ • Convenience seeker $(s_w^*, -\tau(s_B))$

Numerical Illustration

For our analysis, we assume a simple personalization technology function $g(s) = s$—that is, at least one service can be offered for a unit of information—and consider a monopolist whose profit-maximizing number of services is six—that is, the ratio of his or her value for information to the cost of providing services is 12. All consumers with a utility-maximizing set of services below six are privacy seekers where their p4p ratio is $p/r \in [0, 12)$ and those with a utility-maximizing set of services above six are convenience seekers where their p4p ratio is $p/r \geq 12$. Figure 5 shows the optimal service levels and corresponding utilities and profits for the consumer and monopolist, respectively. It also illustrates optimal incentive (fee) that the vendor will offer (charge) to privacy seekers (convenience seekers) under regulatory regimes 3 and 4.

Figure 6 shows the welfare curve under regimes 1, 2, and 3 (regime 4 has the same welfare as regime 1 for privacy seekers and regime 3 for convenience seekers) for varying p4p ratios. Consistent with the theoretical arguments on bargaining presented above, we can see that welfare under regime 3 at least weakly dominates welfare from any other regime. However, when we compare regimes 1 and 2 where no private contracts exist but the regulator's choice is between allowance and disallowance of technology, we see that the relative valuation of the vendor's cost coefficient (β) and the coefficient of the consumer's concern for privacy cost (r) comes into play. When these two cost coefficients are the same, the welfare is the same in both cases; however, when $\beta > r$, then regime 2 is worse off than regime 1 and vice versa. This illustration supports the economic intuition that society is better off in an exchange, when the agent with lower costs chooses the production or service level. In regime 1, consumers determine the market offering, while in regime 2, the vendor regains monopoly power and determines the market service level.

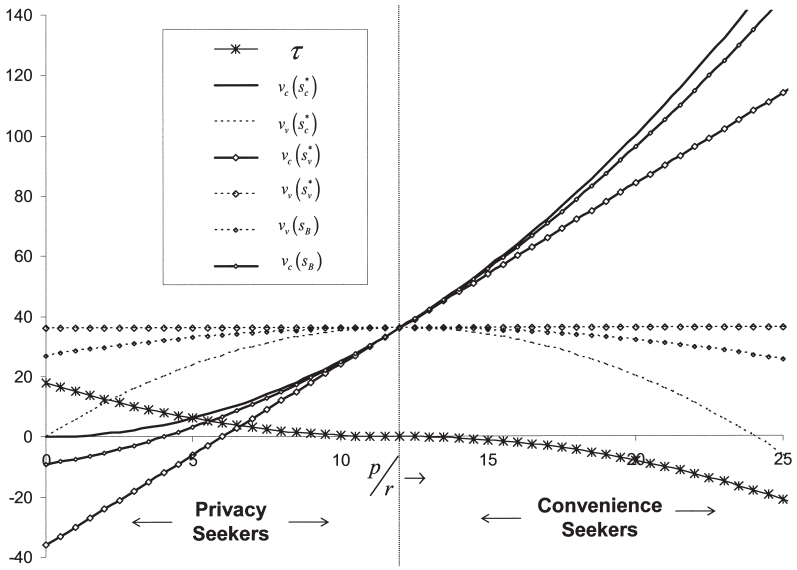

Figure 5. Utility from Personalization for Different Service Offerings

Effect of Information Asymmetry on Regulatory Choices

Until now, we assumed that both the vendor and consumer parameters were common knowledge. In the property rights approach to privacy as in regimes 3 and 4, both agents were aware of each other's valuations. However, if there is no standard market value for a property and if the owner's valuations are private, then when two parties bargain over the property, it is clearly in the interest of the owner to claim that the property is more valuable to him or her than it really is. Similarly, if consumers' property value for their privacy is unknown to the vendor, the vendor may not engage in private contracts as consumers are likely to lie. Thus, even if the regulator allows for private contracts, the socially desirable outcome discussed under regime 3 may not emerge.

> *Proposition 3: Unlike traditional price-instrument markets for goods with free disposal, a regulator should encourage the market's knowledge of consumers' p4p preferences. Interestingly, it is the privacy seekers who are worse off when the p4p ratio is private information.*
>
> *Proof: See the Appendix.*

Typically, the consumer is better off if his or her preference information is private, thus allowing a monopolist to only engage in second- or third-degree price discrimination. First-degree price discrimination would have amounted to zero consumer surplus. This intuition might suggest that privacy-seeking types are better able to protect themselves by hiding their true privacy concerns. On the contrary, our results suggest that the regulator should encourage revelation of privacy preferences. The basis for the private contract with the privacy seekers is the possibility that the vendor

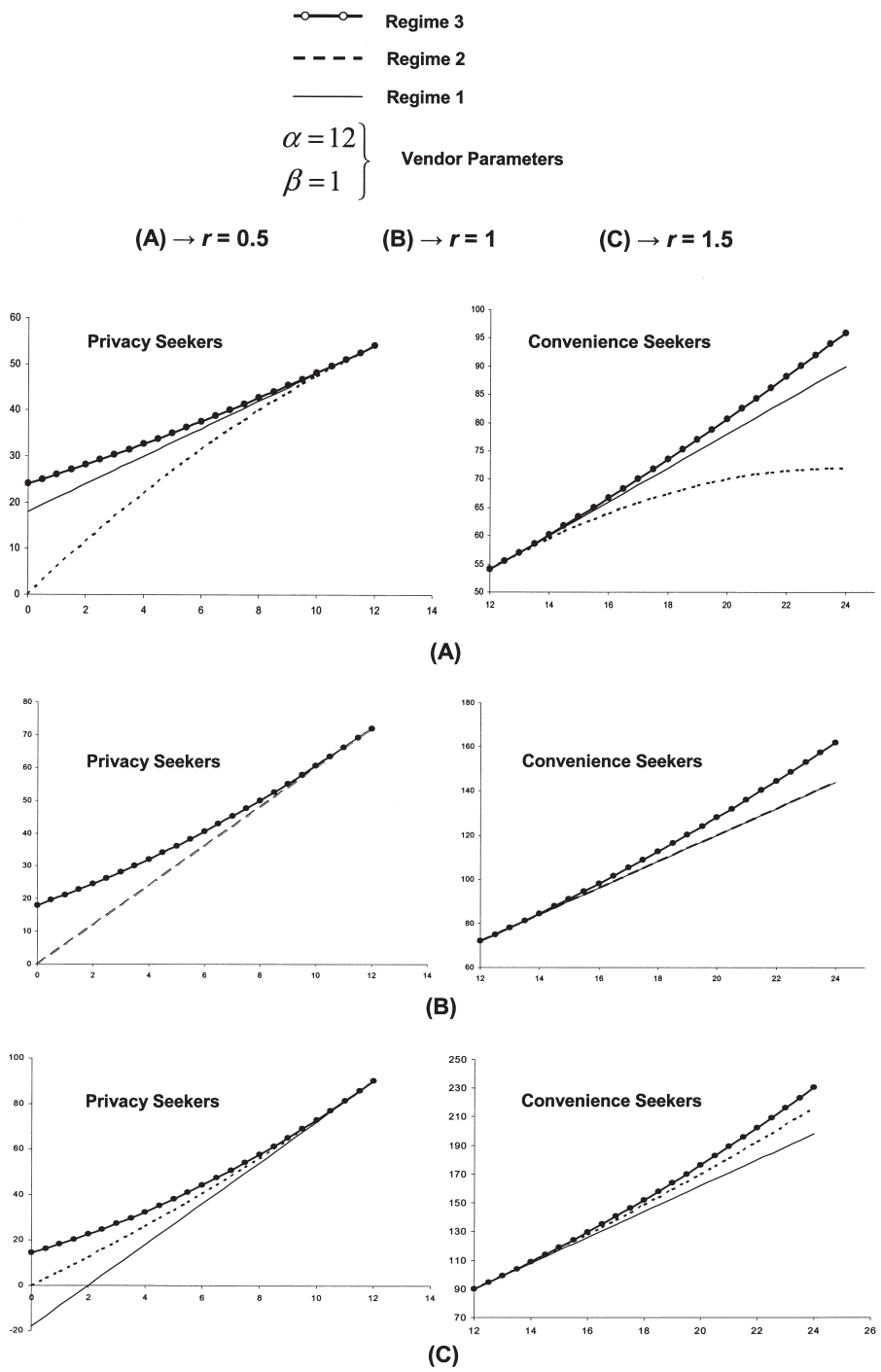

Figure 6. Welfare Effect Under Different Regulatory Frameworks

can incentivize the privacy seeker to use more services than he or she would ideally like to use. However, the agreed-upon set of services s_B is arrived at by the *vendor's assessment* of the privacy seeker's loss. If the p4p ratio is private information, then the privacy seeker will claim a lower ratio than his or her true value. From our numerical illustration in Figure 7, we can see the amount of incentives is increasing with decreasing p4p values. Similarly, the service level under regime 3 is always higher than the preferred level for the privacy seeker. Because the marginal utility from personalization and that from the transfer good is the same, the consumer will declare a p4p ($\tilde{p}/r$) such that the bargained service level from the new p4p ratio is the same as the consumer's true surplus-maximizing level—that is, $\widetilde{s_B} = s_c^*$, and thus derives a net utility of $v_c(s_c^*) + \tau(\widetilde{s_B})$. Because the privacy seeker would have anyway consumed s_c^* without any incentives, the vendor is now clearly worse off. Thus it is not optimal for the vendor to engage in a private contract when he or she does not know the privacy seeker's valuation. Our findings parallel that of Coase's theorem [11], which also stresses that the bargaining may not lead to efficient outcome when valuations are private even if the property rights are well defined.

Along the lines of P3 and similar to the behavior of privacy seekers, one would expect the convenience seekers also to lie and possibly declare a higher p4p ratio such that the vendor would offer more services than before. However, unlike the asymmetry in a typical principal–agent setup, in our context, the information asymmetry does not bestow any advantage to the agent. The intuition behind this proposition is that by asking the vendor to provide services that are higher than his or her profit-maximizing level, the convenience seeker promises to not only compensate for the vendor's loss in profit but also share the remaining surplus with the vendor. If the convenience seeker declares a p4p ratio higher than his or her true value, then he or she would indeed get more services than the full-information bargaining solution, but he or she would also have to pay a higher fee to the vendor. Similarly, if the convenience seeker declares a p4p value that is lower than his or her true value, then even if the fee to be paid is less, the resulting bargained service level would also be further away from his or her ideal point. At the full information service level under regime 3, the marginal gain to the consumer from more services (than s_v^*) equals the marginal loss to the vendor from offering services greater than his or her profit-maximizing level. For a declared p4p ratio higher than the true value, the marginal gain to the consumer is less than the marginal loss to the vendor and hence the consumer cannot gain anything after compensating the vendor's loss. For a declared p4p ratio lower than the true value, the marginal gain to the consumer is higher than the marginal loss to the vendor and therefore the consumer can compensate the vendor for any loss and still have an extra surplus to share. This gain to the consumer continues until the point described by the full information solution, where it equals the marginal loss to the vendor.

The implication of the above analyses is that even when the p4p ratio is not common knowledge, the regulator must allow for the vendor and consumers to engage in a private contract. While the vendor and the market condition will determine whether or not such a contract will be pursued, the welfare to society with the provision of a private contract is always greater than or equal to the social welfare that relies only

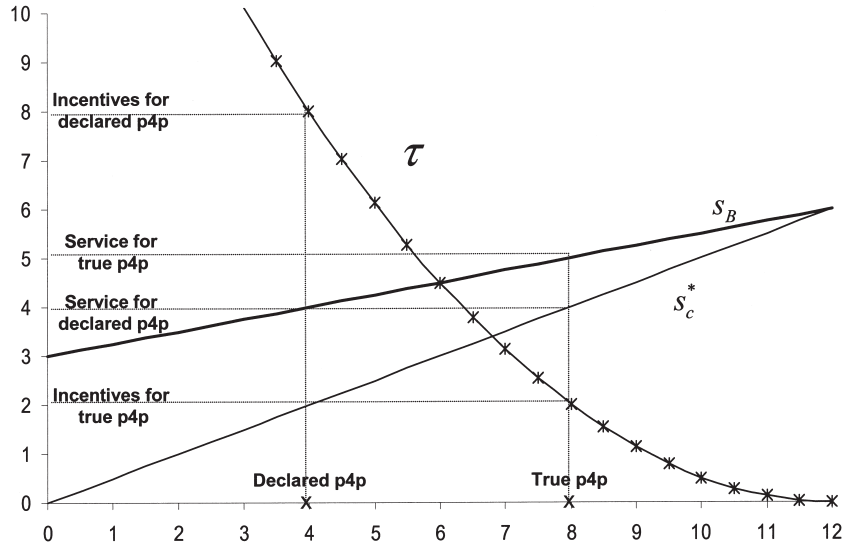

Figure 7. Incentives and Service Levels When a Privacy Seeker Lies About His p4p

on the vendor's enforcement abilities. Indeed, we can observe that the results of information asymmetry will be similar to that of regime 4 where the vendor designs private contracts for convenience seekers while privacy seekers use their respective surplus-maximizing service level.

Discussions, Limitations, and Future Research

Our research evaluates four regime choices that a regulator faces in the market for information. These regimes describe the (dis)allowance of technologies that may be considered intrusive as well as the (dis)allowance of "buying" information. We model these choices by examining a monopolist's service offering for a market defined by two consumer types—privacy and convenience seekers. By investigating the strategic interaction between consumers and the monopolist and deriving the optimal service offerings, we are able to compare the profits, consumer surplus, and social welfare under each regime.

Our formalization of the personalization–privacy trade-off through the nonmonotonic concave utilities underlines the no-free-disposal nature of the service. The "free-of-charge" aspect of this service combined with its "more-is-not-necessarily-better" character endows consumers with certain unique abilities that challenge the conventional wisdom of monopoly markets. While a commonsense approach might suggest the need for strong regulation toward the prevention of information acquisition, through formal modeling, we show that some recommendations in this market may be counter to intuition. Considering the cases where private contracts are not feasible, and comparing regimes 1 and 2, we see that under regime 2, when the monopolist is able to enforce services usage, he or she gains back his monopoly power and forces some types to have zero surplus. Thus, from a consumer's point of view, a regulator should disallow the use of enforcement technologies if no private contracts are offered.

On the other hand, we see that when private contracts are feasible such as in regimes 3 and 4, it is the privacy seeker who is worse off (although no worse than in regime 1) when enforcement technologies are not allowed. This interesting situation emerges due to the fact that vendors will not seek to engage the privacy seekers with private contracts unless they can be sure of a tangible manner through which the agreement can be enforced. Thus our results suggest that the regulator should allow enforcement technologies only conditional on private contracts. In summary, the focus of a regulator should be in educating the consumers on their property rights over information and ensure that contracts are honored on the part of the vendor.

Our approach finds support in early reports on privacy where some researchers have advocated a property rights approach to information. It has been asked of the information age as to "how can we live in a society where individuals can have as much information privacy as they want, and yet where the economic benefits of using personal information in commerce are optimized?" [22]. This report suggested that market failure in privacy-related markets has occurred because of "poor social choice in the allocation of property rights" [22]. In the absence of any formal modeling exercise that examines or lends credibility to this theory, our research provides the necessary framework to examine the social welfare effect of allocation of property rights in the context of online privacy and technological advancements.

Managerial Insights

Many online firms are investing in technologies related to the acquisition and mining of consumers' preference and personal information. Recently, Yahoo acquired Overture Services, which is well-known for its "contextual advertising" (see www.overture.com). The natural synergy between the two is due to the fact that Yahoo acquires customer information and Overture can mine this customer information to construct user profiles and place targeted advertisements. Yahoo offers many different sets of services that a consumer can personalize in my.yahoo.com, but most consumers use only a subset of these services and hence provide information only for those services. If Yahoo's business model is built around a certain amount of information, it could require its users to consume that level; for example, it could require that all users should at least provide information for their weather, stock portfolio, and horoscope. Such a strategy on the part of Yahoo can be viable only if either all of its consumers find it optimal to provide information for these three services or if Yahoo had the ability to ensure that consumers will indeed use these services. While Yahoo can use account expiration and other techniques to force its consumers to use a certain level of services, the abundance of competitors challenges the viability of this strategy.

Our results suggest a vendor should find innovative ways through which he or she can provide consumers with incentives that are related to their use of personalization services. Firms such as Amazon.com are exemplars in this strategy and they provide various forms of incentives to the consumers to use services that are normally not within their optimal level. The most common form used by many vendors is to provide coupons that are sent through e-mail and consumers navigate through a series of

clicks to redeem them. But other techniques, such as a "Gold Box" scheme, are also used that require the user to browse through a store in prescribed order to avail of discounts. Firms also entice customers to provide their friends/family e-mail addresses during shipping on the promise of providing price discounts to their friends on similar items. Amazon.com now has a new scheme where an instant reward of 1.57 percent (called $\pi/2$% by Amazon) of purchases is provided after adequate usage of its A9.com (which acquires search and browsing information) services. Similar to our discussion under regimes 3 and 4, Amazon.com states, "How can we afford this?—Sponsored links revenue—from the small text-based ads on A9.com and Amazon.com search results pages—will help offset costs we incur through the Instant Reward promotion. With our automatic π/2% Instant Reward, we are effectively sharing with you some of the money we collect from sponsored links, i.e. sharing the pi" (www.amazon.com/gp/sx/sharethepi.html).

Our analyses also suggest that vendors should invest in mechanisms to learn about consumer parameters as it is key to the success of personalization strategies. While there is relatively little academic research on measuring personalization and privacy relationships, recent empirical research provides some guidance on measuring these individual specific parameters [8].

Furthermore, the success of the socially optimal regime 3 is dependent upon the truthful execution of the private contract; if the consumers or the vendor violate the terms of their contract, then the society will be worse off. From an implementation perspective, the consumer's choices and bargaining with the vendor can be facilitated by suitably modifying privacy protocols such as the platform for privacy preferences (P3P) framework. The potential for such bargaining frameworks is very high, as the possible range of personalization and potential use of consumer information is still in its infancy. This is particularly true with the emerging fields of genetic and biometric technology, where there is not only the potential for personalized drugs but also the possibility of serious privacy violations [45].

Limitations and Future Research

As the first model of personalization in the presence of privacy concerns, we develop our analysis with a vendor and representative consumer types. For future research, it would be interesting to explore vendor strategies assuming a distribution of consumer types. Further, we explore a monopolistic context; a duopolistic analysis may shed more light on the competitive aspects in this market and we may be able to better analyze the strategy of a portal such as Yahoo vis-à-vis the service offerings of a competitor such as MSN.

References

1. Alba, J.; Lynch, J.; Weitz, B.; Janiszewski, C.; Lutz, R.; Sawyer, A.; and Wood, S. Interactive home shopping: Consumer, retailer, and manufacturer incentives to participate in electronic marketplaces. *Journal of Marketing, 61,* 3 (1997), 38–53.

2. Barua, A., and Chellappa, R.K. Quasi-naturally occurring experiments with electronic

markets and digital products. In C. Holsapple, V. Jacob, and H.R. Rao (eds.), *Business Modeling: Multidisciplinary Approaches—Economics, Operational, and Information Systems Perspectives.* Boston: Kluwer Academic, 2002, pp. 293–307.

3. Bessen, J. Riding the marketing information wave. *Harvard Business Review, 71,* 5 (1993), 150–160.

4. Bloom, P.N.; Milne, G.R.; and Adler, R. Avoiding misuse of new information technologies: Legal and societal considerations. *Journal of Marketing, 58,* 1 (1994), 98–110.

5. Brin, D. *The Transparent Society—Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, MA: Perseus Books, 1998.

6. Chellappa, R.K., and Kumar, K.R. Examining the role of "free" product-augmenting online services in pricing and customer retention strategies. *Journal of Management Information Systems, 22,* 1 (Summer 2005), 355–377.

7. Chellappa, R.K., and Shivendu, S. Managing piracy: Pricing and sampling strategies for digital experience goods in vertically segmented markets. *Information Systems Research, 16,* 4 (2005), 400–417.

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

9. Chester, J. Consumer groups call for FTC investigation of online advertising and consumer tracking and targeting practices. Center for Digital Democracy Press Release, Washington, DC, November 1, 2006.

10. Clemons, E.K., and Thatcher, M.E. Evaluating alternative information regimes in the private health insurance industry: Managing the social cost of private information. *Journal of Management Information Systems, 14,* 2 (Fall 1997), 9–32.

11. Coase, R. The problem of social cost. *Journal of Law and Economics, 1* (October 1960), 1–44.

12. Culnan, M.J., and Armstrong, P.K. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10,* 1 (1999), 104–115.

13. Culnan, M.J., and Bies, R.J. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59,* 2 (2003), 104–115.

14. Derlega, V.; Metts, S.; Petronio, S.; and Margulis, S. *Self-Disclosure.* Newbury Park, CA: Sage, 1993.

15. Doney, P.M., and Cannon, J.P. An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing, 61,* 2 (April 1997), 35–51.

16. Duncan, G.T.; Jabine, T.B.; and De Wolf, V.A. (eds.). *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics.* Washington, DC: National Academy Press, 1993.

17. Glazer, S. Marketing in an information-intensive environment: Strategic implications of knowledge as an asset. *Journal of Marketing, 55,* 4 (1991), 1–19.

18. HIPPA privacy rule takes effect. *Healthcare Financial Management, 55,* 6 (2001), 9.

19. Hoffman, D.L.; Novak, T.P.; and Peralta, M. Building consumer trust online. *Communications of the ACM, 42,* 4 (1999), 80–85.

20. Hoofnagle, C.J. Privacy self regulation: A decade of disappointment. Electronic Privacy Information Center, Washington, DC, March 4, 2005 (available at www.epic.org/reports/decadedisappoint.html).

21. Kwak, M. Web sites learn to make smarter suggestions. *MIT Sloan Management Review, 42,* 4 (2001), 17.

22. Laudon, K.C. Extensions to the theory of markets and privacy: Mechanics of pricing information. In W.M. Daley and L. Irving (eds.), *Privacy and Self-Regulation in the Information Age.* Washington, DC: U.S. Department of Commerce, June 1997 (available at www.ntia.doc.gov/reports/privacy/selfreg1.htm#1D).

23. Laufer, R.S., and Wolfe, M. Privacy as a concept and a social issue: A multidimensional developmental theory. *Social Issues, 33,* 3 (1977), 22–24.

24. Lemos, R. Analysts: Egghead's inquiry cost millions. ZDNet News, January 9, 2001 (available at http://news.zdnet.com/2100-9595_22-527001.html).

25. Liang, T.-P.; Lai, H.-J.; and Ku, Y.-C. Personalized content recommendation and user satisfaction: Theoretical synthesis and empirical findings. *Journal of Management Information Systems, 23,* 3 (Winter 2006–7), 45–70.

26. Mattila, A. Consumers' value judgment. *Cornell Hotel & Restaurant Administration Quarterly, 40,* 1 (1999), 40–46.

27. Mittal, B., and Lassar, W.M. The role of personalization in service encounters. *Journal of Retailing, 72,* 1 (1996), 95–109.

28. Nash, J.F. The bargaining problem. *Econometrica, 18,* 2 (1950), 155–162.

29. Noam, E.M. Privacy and self-regulation: Markets for electronic privacy. In W.M. Daley and L. Irving (eds.), *Privacy and Self-Regulation in the Information Age.* Washington, DC: U.S. Department of Commerce, June 1997 (available at www.ntia.doc.gov/reports/privacy/selfreg1.htm#1B).

30. Peppers, D., and Rogers, M. *The One to One Future (One to One).* New York: Currency, 1996.

31. Osborne, M.J., and Rubinstein, A. *Bargaining and Markets.* New York: Academic Press, 1990.

32. Peppers, D.; Rogers, M.; and Dorf, B. Is your company ready for one-to-one marketing? *Harvard Business Review, 77,* 1 (1999), 3–12.

33. Pigou, A.C. *The Economics of Welfare.* London: Macmillan, 1932.

34. Pine, B.J., II; Peppers, D.; and Rogers, M. Do you want to keep your customers forever? *Harvard Business Review, 73,* 2 (1995), 103–114.

35. Privacy online: Fair information practices in the electronic marketplace. Report to Congress, Division of Financial Practices, Bureau of Consumer Protection, Federal Trade Commission, Washington, DC, 2000 (available at www.ftc.gov/reports/privacy2000/privacy2000.pdf).

36. Raghu, T.S.; Kannan, P.K.; Rao, H.R.; and Whinston, A.B. Dynamic profiling of consumers for customized offerings over the Internet: A model and analysis. *Decision Support Systems, 32,* 2 (2001), 117–134.

37. Rendleman, J. Customer data means money. *InformationWeek* (August 20, 2001) (available at www.informationweek.com/news/showArticle.jhtml?articleID=6506304).

38. Rogers, J.L. Mail advertising and consumer behavior. *Psychology and Marketing, 13,* 2 (Winter 1996), 211–233.

39. Rosenberg, A. Privacy as a matter of taste and right. In E.F. Paul, F.D. Miller, and J. Paul (eds.), *The Right to Privacy.* Cambridge: Cambridge University Press, 2000, 68–90.

40. Scott, J.S. Privacy, confidential, and security: Protecting "personally identifiable information." *Healthcare Financial Management, 53,* 3 (1999), 26–27.

41. Shapiro, S.P. The social control of impersonal trust. *American Journal of Sociology, 93,* 3 (November 1987), 623–658.

42. Sharton, B., and Wilcoxson, J. Privacy: The next frontier in online regulation? *Boston Bar Journal* (March–April 2001), 1–6.

43. Sheehan, K.B. How public opinion polls define and circumscribe online privacy. *First Monday, 9,* 7 (2004) (available at http://firstmonday.org/issues/issue9_7/sheehan/index.html).

44. Taylor, C.R. Consumer privacy and the market for customer information. *RAND Journal of Economics, 35,* 4 (2004), 631–651.

45. Thatcher, M.E., and Clemons, E.K. Managing the costs of informational privacy: Pure bundling as a strategy in the individual health insurance market. *Journal of Management Information Systems, 17,* 2 (Fall 2000), 29–58.

46. Thibodeau, P. FTC workshop looks at key data privacy issues. *Computerworld* (March 13, 2001) (available at www.itworld.com/Man/2688/CW031301ftc/).

47. Vidmar, N., and Flaherty, D.H. Concern for personal privacy in an electronic age. *Journal of Communication, 35,* 2 (Spring 1985), 91–103.

48. Volokh, E. Freedom of speech and information privacy: The troubling implications of a right to stop people from speaking about you. *Stanford Law Review, 52,* 5 (2000), 1049–1124.

49. Volokh, E. Personalization and privacy. *Communications of the ACM, 43,* 8 (2000), 84–88.

50. Wei, C.-P.; Chiang, R.H.L.; and Wu, C.-C. Accommodating individual preferences in the categorization of documents: A personalized clustering approach. *Journal of Management Information Systems, 23,* 2 (Fall 2006), 173–201.

51. Wind, J., and Rangaswamy, A. Customerization: The second revolution in mass customization. eBusiness Research Center Working Paper no. 06-1999, Penn State University, University Park, 2001.

52. Winer, R.S. A framework for customer relationship management. *California Management Review, 43,* 4 (2001), 89–105.

Appendix

Proof of Lemma 1

We have $v_v(s) = \alpha g(s) - \beta s^2$ and $v_c(s) = ps - rg^2(s)$. s_c^* is the solution to the equation $v_c' = 0$—that is, $g(s_c^*)g'(s_c^*) = p/2r$. Because g is strictly convex and increasing, g and g′ are both increasing in s and hence s_c^* is increasing in p/r. $v_c(s_c^0) = ps_c^0 - rg^2(s_c^0) = 0 \Rightarrow (p/r)s_c^0 = g^2(s_c^0)$. Differentiating both sides with respect to (w.r.t.) p/r, we get

$$\frac{\delta s_c^0}{\delta \frac{p}{r}} = \frac{s_c^0}{2g\left(s_c^0\right)g'\left(s_c^0\right) - \frac{p}{r}}.$$

Because $s_c^0 > s_c^*$ and $2g(s_c^*)g'(s_c^*) = p/r$, $2g(s_c^0)g'(s_c^0) > p/r$. Hence $\delta s_c^0/\delta(p/r) > 0$.

Proof of Lemma 2

By definition, for the privacy seeker, $s_c^* < s_v^*$, and for the convenience seeker, $s_c^* \geq s_v^*$. In the presence of enforcement capabilities, only consumers' participation constraint needs to be satisfied, whereas in the absence of enforcement abilities, the consumers can use any service level equal to or below that offered by the vendor. In the presence of enforcement, for the privacy seeker, if $v_c(s_v^*) \geq 0$, then the vendor will offer s_v^*; however, if $v_c(s_v^*) < 0$, then the vendor will offer the service level closest to his or her surplus-maximizing level, such that the privacy seeker's participation constraint is met—that is, the privacy seeker gets zero utility. Because the vendor's profit is increasing at service levels less than s_v^*, he or she will offer s_c^0, where $v_c(s_c^0) = 0$. For the convenience seeker, $v_c(s_v^*) > 0$ and $v_c'(s_v^*) > 0$, hence the vendor will offer s_v^*.

Also, in the absence of enforcement, the vendor will offer s_v^* to the convenience seeker as he or she will find it optimal to use this service level irrespective of external enforcement. However, the privacy seeker will use $s_c^* < \min\{s_c^0, s_v^*\}$, if the vendor offers $\min\{s_c^0, s_v^*\}$. Hence the vendor will offer only s_c^*.

Proof of Proposition 1

By definition, $s_c^* \geq s_v^*$ for convenience seekers. Because $(\delta v_v(s_c^*))/\delta s < 0$ for any $s > s_v^*$, the vendor will only choose s_v^* irrespective of the ability to enforce. However, the effect of enforcement (when s_v^* is chosen) and nonenforcement (when s_c^* is chosen) on the welfare of the society becomes ambiguous when the market has some privacy seekers—that is, $v_w(s_c^*)$ is not always greater than $v_w(s_v^*)$ or vice versa. Let us assume that for a given set of vendor parameters (α, β) and a given privacy coefficient (r),

there is some consumer type for whom $v_w(s_c^*) = v_w(s_v^*)$. We need to prove that for these given parameters, there are other consumer types for whom the equality does not hold. For a fixed value of r and changing values of p, the direction of the right-hand side—that is, $\delta v_w(s_v^*)/\delta p = s_v^*$—is constant and positive. However, the direction of the left-hand side is ambiguous.

$$\frac{\delta v_w\left(s_c^*\right)}{\delta p} = s_c^* + p\frac{\delta s_c^*}{\delta p} - 2rg'\left(s_c^*\right)g\left(s_c^*\right)\frac{\delta s_c^*}{\delta p} + \alpha g'\left(s_c^*\right)\frac{\delta s_c^*}{\delta p} - 2\beta s_c^*\frac{\delta s_c^*}{\delta p}$$

and because $2rg'(s_c^*)g(s_c^*) = p$, we have

$$\frac{\delta v_w\left(s_c^*\right)}{\delta p} = s_c^* + \frac{\delta s_c^*}{\delta p}\left(\alpha g'\left(s_c^*\right) - 2\beta s_c^*\right).$$

$(\delta v_w(s_c^*))/\delta p$ is positive if

$$\alpha g'\left(s_c^*\right) - 2\beta s_c^* \geq 0 \Rightarrow \frac{\alpha}{2\beta} \geq \frac{s_c^*}{g'\left(s_c^*\right)}$$

and $\delta v_w(s_c^*)/\delta p$ is negative if

$$s_c^* < \frac{\delta s_c^*}{\delta p}\left(\alpha g'\left(s_c^*\right) - 2\beta s_c^*\right).$$

Hence we have (a) of the proposition.

If through some mechanism the vendor can force the consumer to use the consumer's break-even level or the vendor's optimal service level, then the vendor will willingly invest in such a mechanism—that is, the vendor will prefer $v_v(\min\{s_c^0, s_v^*\})$, whereas the consumer will prefer s_c^*, where the vendor will get only $v_v(s_c^*)$. However, the cost of doing so has to be less than any gain the vendor makes in forcing the privacy seeker to move to this new service level. Hence we have P1(b).

Proof of Lemma 3

The reason that the vendor will engage in bargaining is that he or she can do better than his or her current profit at $v_v(s_c^*)$. The consumer will agree to such a bargaining only when he or she is not worse off than at $v_c(s_c^*)$, and possibly does better. Hence, the vendor's problem is to offer a service level such that his or her excess profit $(v_v(s) - v_v(s_c^*)$ from the new service level (s_B) is maximized after compensating the consumer's loss $(v_c(s_c^*) - v_c(s))$. As the loss to the consumer is also dependent on the new service level, the vendor has to include this loss in his or her maximization problem; hence we have Lemma 3.

Proof of Lemma 4 and Corollary 1

We develop an axiomatic bargaining problem where both the vendor and the privacy seeker have the same preferences over v_i, $i = \{v, c\}$ as the utility from personalization to the consumer and the profit from personalization for the vendor are transferable and have one-to-one equivalence. Hence $\langle \Theta, d \rangle$ is a symmetric bargaining problem. For such problems, the Nash solution is obtained directly from SYM and PAR conditions [31]. The unique symmetric efficient utility, profit pair will be obtained at the point where the vendor and the consumer divide the pie $B_\pi(s_B)$ in equal parts. Because all of $B_\pi(s_B)$ is initially made available to the vendor, he or she will offer a total incentive of

$$\tau(s_B) = \frac{v_c(s_B) + v_v(s_B) - v_c(s_c^*) - v_v(s_c^*)}{2}$$

to the privacy seekers.

s_B is determined by the solution to the problem posed in Lemma 3. Differentiating B_π with respect to s, we get

$$\frac{\delta B_\pi}{\delta s} = \frac{\delta v_c}{\delta s} + \frac{\delta v_v}{\delta s},$$

as $v_c(s_c^*)$ and $v_v(s_c^*)$ are constant. This is nothing other than the first order of the welfare-maximization problem of $v_w(.) = v_v(.) + v_c(.)$. Hence the service level from bargaining is equal to the welfare-maximizing service level $s_B = s_w^*$.

The convenience seeker's case is the converse of the privacy seeker's in that the convenience seeker prefers more services than the vendor's optimal level. In the bargaining setup, the convenience seeker will not only compensate the vendor for the cost of offering services in excess of the vendor's optimal level but the convenience seeker will also pay an additional charge that is proportional to the gain in his or her utility. If we apply the bargaining framework to this regime as well, we would get τ as the optimal price that the vendor will be willing to accept. Hence we have Corollary 1.

Proof of Proposition 2

In the absence of enforcement, the vendor's profit is $v_v(s_c^*)$; with enforcement and private contracts (regime 3), net profit from personalization is

$$v_v(s_B) - \tau(s_B) \Rightarrow v_v(s_B) - \frac{v_c(s_B) + v_v(s_B) - v_c(s_c^*) - v_v(s_c^*)}{2}$$
$$\Rightarrow \frac{v_v(s_B) + v_v(s_c^*) + v_c(s_c^*) - v_c(s_B)}{2}.$$

We know that $v_c(s_c^*) - v_c(s_B) > 0$ and $v_v(s_B) > v_v(s_c^*)$, so $v_v(s_B) + v_v(s_c^*) > 2v_v(s_c^*)$. This implies $v_v(s_B) - \tau(s_B) > v_v(s_c^*)$, and hence the *producer welfare* is always higher during regime 3. Under regime 1, the privacy seeker would have received $v_c(s_c^*)$, and in regime 3, he or she receives $v_c(s_B) + \tau(s_B)$. Because $\tau(s_B) > v_c(s_c^*) - v_c(s_B)$ (the privacy

seeker being compensated for his or her loss), we have $v_c(s_B) + \tau(s_B) > v_c(s_c^*)$. Hence the *privacy seeker* is also always better off during regime 3. Thus, we see the agreed-upon service level $s_B = s_w^*$ from Lemma 4, hence $v_w(s_B) > v_w(s_c^*)$ (regime 3 > regime 1) and $v_w(s_B) > v_w(s_v^*)$ (regime 3 > regime 2). If only private contracts are allowed and enforcement is not (regime 4), we know that the privacy seeker will only get $v_c(s_c^*)$ and the vendor will only get $v_v(s_c^*)$—so both the privacy seeker and the vendor are worse off with regard to their exchange. The contracts between the convenience seeker and the vendor will be the same between regimes 3 and 4.

Proof of Proposition 3

Let the p4p ratio (p/r) be given by some $\theta \in [\underline{\theta}, \bar{\theta}]$, with a cumulative distribution $F(\theta)$ and a density function $f(\theta) > 0$ on $[\underline{\theta}, \bar{\theta}]$. Let the vendor's parameters α and β be common knowledge and he or she knows only the distribution of the consumer's p4p ratio. In the event of engaging in private contracts, the vendor would pay a net transfer of

$$\tau(\theta) = \frac{\left(v_v\left(s_B(\theta)\right) - v_v\left(s_c^*(\theta)\right)\right) + \left(v_c\left(s_c^*(\theta)\right) - v_c\left(s_B(\theta)\right)\right)}{2}$$

to the consumer. Now, if the consumer announces his or her p4p ratio to be some $\hat{\theta} = \theta - \Delta\theta$, then the transfer received will be

$$\tau(\hat{\theta}) = \frac{\left(v_v\left(s_B(\hat{\theta})\right) - v_v\left(s_c^*(\hat{\theta})\right)\right) + \left(v_c\left(s_c^*(\hat{\theta})\right) - v_c\left(s_B(\hat{\theta})\right)\right)}{2}.$$

For the privacy seekers, at the bargaining solution point s_B, $\partial v_v(s_B(\theta))/\partial s < 0$ and $\partial\tau(\theta)/\partial s < 0$. If a consumer of θ announces $\hat{\theta}$, then the new bargaining solution is $\hat{s}_B < s_B$. Because the value v_c is increasing up to s_c^*, the consumer will lower his or her p4p ratio so that $\hat{s}_B = s_c^*$. While the transfer good τ continues to increase with smaller values of $\hat{\theta}$, lying below $\hat{s}_B = s_c^*$, v_c begins to decrease and, hence, from this point onward, any decision to declare a lower $\hat{\theta}$ will depend on the trade-off between the loss in consumer surplus and gain in the transfer good. Therefore, the privacy seeker will always lie at least up to a p4p ratio $\hat{\theta}$ such that the bargained service level $\hat{s}_B = s_c^*$.

From the vendor's point of view, the consumer will never contract a service level greater than s_c^*. Even without bargaining, this is the service level that the consumer would have chosen, and the vendor would not have had to pay any transfer good as well. Hence, if lying can take place, the vendor will never engage in private contracts with the privacy seeker. However, because the convenience seeker is paying a fee for services that are provided above the vendor's profit-maximizing level, and as the fee $\tau(s_B)|s_B > s_v^*$ is increasing in s and as s_B is increasing in the p4p ratio, the consumer will never be better off by declaring a p4p ratio higher than his or her true value. Similarly, if the consumer declares a lower p4p ratio, then the fee the consumer would need to pay is less but he or she will also get a service level that is farther from his or her optimal level.