The Customer Economics of Internet Privacy

Roland T. Rust, P. K. Kannan and Na Peng

Journal of the Academy of Marketing Science 2002; 30; 455
DOI: 10.1177/009207002236917

The Customer Economics of Internet Privacy

Roland T. Rust
P. K. Kannan
Na Peng
University of Maryland

The World Wide Web has significantly reduced the costs of obtaining information about individuals, resulting in a widespread perception by consumers that their privacy is being eroded. The conventional wisdom among the technological cognoscenti seems to be that privacy will continue to erode, until it essentially disappears. The authors use a simple economic model to explore this conventional wisdom, under the assumption that there is no government intervention and privacy is left to free-market forces. They find support for the assertion that, under those conditions, the amount of privacy will decline over time and that privacy will be increasingly expensive to maintain. The authors conclude that a market for privacy will emerge, enabling customers to purchase a certain degree of privacy, no matter how easy it becomes for companies to obtain information, but the overall amount of privacy and privacy-based customer utility will continue to erode.

> The advance of civilization is nothing but an exercise in the limiting of privacy.
>
> —Isaac Asimov
>
> Civilization is the progress toward a society of privacy.
>
> —Ayn Rand

Science fiction writer Isaac Asimov and political novelist Ayn Rand take opposite sides with respect to the eventual outcome with respect to privacy. It is clearly the case, as Asimov might argue, that technology is getting better and better at obtaining and processing personal information and that this trend has been greatly accelerated by the advent of the Internet. However, Rand implies that the economics of a competitive marketplace will protect the individual and maintain his or her privacy. Who is right? Our approach is to take the main features of both of their arguments (the advance of technology and the existence of a competitive marketplace) and to project the result, given no government intervention, using a simple economic model. We conclude that if privacy is left to market forces, the future will be a mix of the Asimov and Rand points of view. That is, privacy will continue to decline, but it will not go away because the emerging privacy industry will persist indefinitely, although it is likely to shrink over time as the maintenance of privacy becomes more expensive.

INTERNET PRIVACY—AN EMERGING ISSUE

While customer privacy has always been a significant issue in marketing, it has assumed a greater significance in recent years with the advent of Internet-based commercial transactions. To take advantage of the key benefits of online transactions such as convenience, customers need to trade off by providing valuable information about themselves—be it name, address, credit card number—all in pursuit of seamless and effortless online transactions (Feldman 2000). In fact, it may be quite impossible for customers to transact business on the Internet without revealing information about themselves that they may be unwilling to share. Also, the higher the levels of service customers demand, the more information they may have to provide to get the required service. Consequently,

Journal of the Academy of Marketing Science.
Volume 30, No. 4, pages 455-464.
DOI: 10.1177/009207002236917

Internet-based transactions are creating large databases of information about customers, their demographics, and their purchase habits. In many cases, the customer himself or herself enters this information into the databases, thus rendering the costs of obtaining such information much lower than in traditional transactional situations.

In addition to the customer information that is voluntarily provided by customers themselves, businesses can also collect information on customer online behavior using cookies and click-stream analysis, which do not require the conscious participation of the consumer. The advances in technology and rapidly falling costs of computing technology, which render such data collection easy and cheap, also make it relatively easy and cheap to store, retrieve, and mine the information to develop customer profiles, behavior profiles, and insights for targeting and discriminating customers. Efficient and cost-effective data-mining techniques and data-warehousing technology allow marketers to analyze the growing information pool to understand and target their customers better (Markoff 1999; Richards 1997). Finally, the network environment within which customer information is collected and coded also makes it easy to distribute and/or sell the information efficiently, thus aiding the process of combining bits and pieces of seemingly disparate customer information to develop full, integrated profiles of consumers and their behavior (Rombel 2001). Thus, owing to its very structure and characteristics, the Internet environment is providing the impetus to create more and better customer information and at significantly lower costs as compared to those characterizing physical transactions.

The Erosion of Privacy on the Internet

For the purposes of this article, we define *privacy* as the degree to which personal information is not known by others. Many forces accelerated by the Internet would seem to erode privacy based on this definition.

For example, while the costs of obtaining and processing information about consumers are decreasing with the advances in technology, the value of consumer information for businesses has been increasing. This trend is the natural outcome of the evolution of business strategies from a mass-market approach to segmentation, niche marketing, and personalization approaches (Mason 1986; Richards 1997). In the fiercely competitive markets, demands for greater economic efficiency and improved customer loyalty have given rise to greater demands for more detailed information about customers that can help in segmenting and targeting customers. As a result, online businesses are economically motivated to gather and use greater amounts of customer information. Due to its multidimensional character, the Internet holds great promise of becoming a powerful marketing tool through intelligent use of customer information (Richards 1997). This greater need for customer information, however legitimate, is naturally leading to pressures on customer privacy and its gradual erosion.

The online privacy problem is further exacerbated by the very structure of computer systems and the Internet. The initial design of personal computer systems was never intended to be privacy-friendly or to be used in social contexts, and thus the system is particularly leaky from a privacy viewpoint (Lester 2001). In addition, compared with some other media, the Internet is woven into people's lives in a more intimate way as it connects people with places and people with people. Gradually, the applications of new technologies have eroded the distinction between public and private space and compromised the very idea of private space "by establishing long-lived interconnections among formerly separate spaces" (Bellotti 1997). Consequently, consumers can no longer depend on the intuitive sense of place and presence that governs their observable behavior to ensure that they are not watched or recorded, thus lowering the privacy barrier.

Even when customers voluntarily provide information to a marketer on the Internet, their privacy is often compromised. Sometimes the information a visitor provides to one Web site might bleed into another without the customer realizing it. This compromises customers' information privacy on two dimensions: environmental control and control over secondary use of information (Hoffman, Novak, and Peralta 1999). On the dimension of environment control, the leaky systems and networks allow hackers to obtain customer information illegitimately. The structure of the Internet also compromises customers' ability to influence how marketers use customers' personal information subsequent to its collection. Although the secondary use of personal information violates the principle of autonomy (Foxman and Kilcoyne 1993) and is considered an invasion of consumers' privacy (Cespedes and Smith 1993), commercial Web sites are still selling or renting consumers' names, addresses, telephone numbers, and purchase histories to interested marketers. Therefore, although the Internet provides convenience for its users, it also fosters the abuse of its features and erodes customers' privacy.

The Future of Privacy—Conventional Wisdom

It is clear from the preceding discussion that the marketing practices on the Internet that give customers little control over their information, combined with the leaky structure of the network environment, have led to significant Internet privacy concerns. As a U.S. Senate (2000) report states, "Companies are able, because of recent technological advances, to collect a vast amount of information about online consumers, often without that consumer's knowledge or consent" (p. 2). In fact, no other medium has been a “catalyst of such a wide range of criticisms regarding privacy invasion” (Richards 1997). Although many Web sites have adopted privacy policies under pressure from consumer groups, many others still continue selling consumer information to marketers (Clark 2000). In 1999, Enonymous.com, a Web privacy rating company, found that in more than 30,000 Web sites, only 3.5 percent of Web sites never shared personal information with third parties, and 73 percent or 22,000 sites had no privacy policy at all (enonymous.com 2000). Given the increasing demand for valuable customer information, many consider the privacy battle already lost. This has led to such comments as the following from Scott McNealy, the chief executive officer of Sun Microsystems: “You have zero privacy anyway. Get over it” (Lester 2001). Given the increasing value of information, the tremendous technological advances that make it easy to collect customer information, and the decreasing the cost of obtaining such information, one school of thought holds that privacy will continue to erode at an exponential rate until it virtually disappears. It is believed that the ability of individuals to protect their information privacy is almost nonexistent, leading Harper (1998) to argue that there is only one choice to protect Internet privacy—turning off the computer.

Opinion is divided as to how this trend of decreasing privacy could be stopped before privacy invasion practices become an established pattern and get ingrained in the Internet economy. Some believe that the only way to reverse the trend is for the government to legislate and monitor privacy practices of businesses. Others who are more skeptical of government intervention hold the view that industry self-regulation, under pressure from consumer advocacy groups and market forces, is a viable solution for protecting customer privacy. Their argument is that if consumers punish businesses engaged in dubious privacy practices, then businesses will have an incentive to self-regulate. While the debate on the pros and cons of government legislation versus industry self-regulation continues, there is an emerging view that privacy will become so valuable for customers that there will be an emerging market for it, with companies providing the privacy protection that customers demand. This market, the proponents of the view argue, will work to maintain the privacy equilibrium in the Internet economy. The very technological advances that erode privacy can also be used to protect privacy that customers demand.

In this article, we propose a simple model to provide insights into the above issues. What is the future for Internet privacy? Will privacy continue to erode as many expect? Can a market for privacy maintain a steady level of privacy in the Internet economy? What kinds of privacy mechanisms can ensure a steady market? In the next section, we propose our model. In the third section, we discuss, in light of our model results, the various business models that could emerge in an industry for Internet privacy. We discuss areas of future research and conclude in the fourth section.

AN ECONOMIC MODEL OF INTERNET PRIVACY

If we are specific about our assumptions, then a simple model may serve to explore their implications. We make some seemingly noncontroversial assumptions about the psychology and economics of privacy, how privacy is affected by information gathering, and how the cost of information gathering is affected by technology, and we show how these assumptions lead inexorably to the rapid growth and eventual slow decline of a privacy industry.

Assumptions

We explore our model from the standpoint of industry (viewed as a representative company) and a typical customer. This may be thought of as a monopolist model with one customer. The simplifications (one customer, one company) greatly facilitate the mathematical development, with minimal loss of the central operating mechanisms. Despite its simplicity, the model is sufficiently complex to illuminate the most important insights. Such simplifications are frequently employed in economic modeling.

Our economic model is driven by a small set of plausible assumptions that are translated later into the model formulation. First, we assume that technology (which we view broadly as capability for efficiency) is continuously advancing. In fact, most measures of the increase of technology suggest that the rate of advance is quickening. Except for a few isolated and temporary occurrences (e.g., the destruction of advanced civilizations by primitive tribes), the march of technology has been a constant throughout human history. Thus, our first assumption is as follows:

Assumption 1: Technology is advancing over time.

A result of advancing technology (especially in the past 150 years) is that technologies for gathering and analyzing personal information also move forward. This reduces the cost of obtaining and processing personal information. Thus,

Assumption 2: As technology advances, the cost of obtaining and processing personal information declines.

From the psychology literature, we know that each individual has a desired optimal level of stimulation (Menon and Kahn 1995; Raju 1980) and a desired personal space

(Hall 1966). We also know that each individual has a desired level of privacy (Larson and Bell 1988). Too little privacy is uncomfortable, but too much privacy is also uncomfortable because of loneliness (Hosman 1991). From these findings, we assume the following:

> *Assumption 3:* From the customer's point of view, there is an ideal level of privacy. Too little privacy is undesirable, but too much privacy is also undesirable because of loneliness.

Methods of protecting privacy exist (Cavoukian and Tapscott 1996), and the provision of privacy services represents a basis for making money from customers (Lester 2001). On the basis of this, we have the following:

> *Assumption 4:* The company may offer privacy for sale, for a fixed price, per unit of privacy.

Information is the enemy of privacy. That is, privacy is invaded by information obtained, and a unit of privacy may be thought of as a given amount of information revealed. Hence, privacy provided means information that is not obtained. From this, we have the following:

> *Assumption 5:* Each unit of privacy sold is a unit of information that the company does not have.

Some information is not cost-effective for the company to obtain. That information has no sale value because the customer's privacy with respect to that information is not under threat. Only the information that might be collected and used is of value to the customer. Hence,

> *Assumption 6:* The information considered for sale is that information for which the value of a unit of information (to the company) exceeds the cost of obtaining and processing it.

An Alternative Interpretation

It is interesting to note that the above assumptions, as well as the model that results from them, also are consistent with an alternative interpretation. In Assumption 5, instead of the firm offering privacy for sale, it might instead pay the customer for information. The result is formally identical. That is, in either case, the customer faces the decision of whether to have more money or more privacy, with the company having more information or more money as a result. In fact, there may be a combination of the two interpretations at work, with no ill effect on the model and its conclusions, which are identical under either or both interpretations.

Model Formulation

Based on Assumption 3, we write the customer's utility function as follows:

$$U(X) = aX - bX^2 - PX = (a - P)X - bX^2, \qquad (1)$$

where X is the number of units of privacy purchased, a is a "desire for privacy" parameter, b is a "loneliness" parameter, and P is the price charged per unit of privacy. The terms $aX - bX^2$ represent an inverted U function of privacy, which implements Assumption 3, which says that there will be an ideal level of privacy. The PX term represents the amount of money paid to the company to preserve privacy. The customer wishes to maximize $U(X)$ with respect to X.

Assumptions 4, 5, and 6 form the basis for the company's profit function, which is written as

$$\Pi(P) = cX + PX - vX = (P - (v - c))X, \qquad (2)$$

where c is the cost per unit of information obtained, and v is the value of each unit of information to the company. This equation may not be obvious at first glance, so some explanation is called for. The cX term says that each unit of privacy makes one unit of information collection unnecessary, which saves c in information collection costs. On the basis of Assumption 6, we know that the company would have collected the information otherwise. The PX term is income from providing privacy. The vX term says that each unit of privacy deprives the company of one unit of information, reflecting Assumption 5.

Equilibrium Solution

The equilibrium solution is straightforward, so we do not show the derivational details here. The solution is the following:

$$P = (a + (v - c))/2, \qquad (3)$$

$$X = (a - (v - c))/4b, \qquad (4)$$

$$\Pi = [(a - (v - c)^2]/8b, \qquad (5)$$

$$U = [(a - (v - c)^2]/16b. \qquad (6)$$

Defining the market for privacy, M, as the amount spent to protect privacy, we have

$$M = PX = [a^2 - (v - c)^2]/8b. \qquad (7)$$

Comparative Statics

Examining the equations above, we can explore the comparative statics of the equilibrium. That is, given changes in the parameters that describe the market, how will the equilibrium solution change? We will not show the equations because they are simple calculations of the partial derivative with respect to the input parameter.

As desire for privacy (a) increases, we see increases in the price of privacy (P), amount of privacy (X), and the market for privacy (M). This is not surprising because it is the desire for privacy that makes the privacy market both possible and lucrative.

The loneliness parameter (b) works in mostly the opposite manner. While an increase in loneliness has no impact on price, it does result in a decrease in the amount of privacy and the market for privacy. This is not surprising because more loneliness means that privacy is less attractive.

As the cost of information (c) decreases, we find that the price of privacy increases, the amount of privacy decreases, and the market for privacy shrinks. These changes also are intuitive. If information is less expensive to obtain and process, then it is more valuable, and customers will be forced to pay more to cover the opportunity cost from obtaining and processing the information. The higher the price of privacy, the less privacy is demanded. As it turns out, the decrease in demand overwhelms the increase in price, resulting in a shrinking market for privacy.

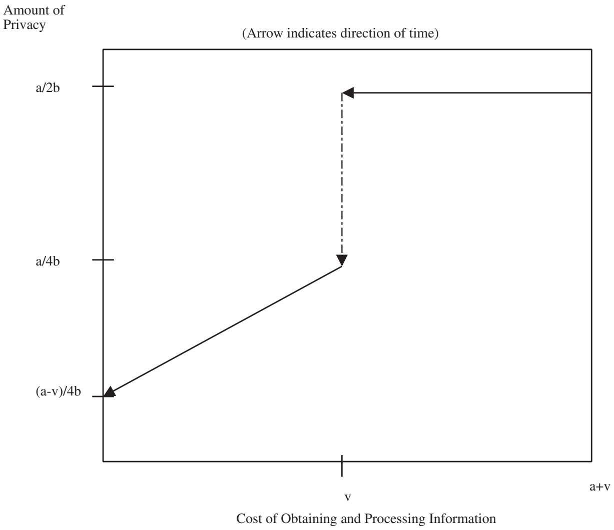
As the value of information (v) increases, we find that the price of privacy increases (because companies have to receive more to forfeit their valuable information), and the increased price causes the amount of privacy to decrease. Again the market for privacy shrinks because when information is valuable enough, companies would rather be in the information business than the privacy business.

The Path of Time

On the basis of Assumptions 1 and 2, we can see that the path of time is the direction of decreasing costs of obtaining and processing information. So in other words, by tracking how the market for privacy changes as costs of information decrease, we are actually tracking how the privacy market will change over time. Figures 1 through 4 show how the privacy market will change over time, given the assumptions of our model. Using the cost of obtaining and processing information as our x-axis, the path of time is right to left. We have drawn arrows on each figure to show the direction of time.

Figure 1 shows the amount of privacy. The amount of privacy is $a/2b$ until the cost of obtaining and processing information reaches v. Then there is a discontinuous jump down in the amount of privacy, to $a/4b$. At that point, the market in privacy kicks in and moderates the decline. Privacy continues to decline but at a slower rate. Even if the cost of obtaining and processing information goes to zero, the amount of privacy does not go to zero but instead bottoms out at $(a - v)/4b$, reflecting the fact that the privacy market will not disappear.

FIGURE 1
How the Amount of Privacy Will Change Over Time



Actually, the market for privacy is an aggregation of many markets, each with somewhat different cost structures, meaning we are likely to be at varying parts of this curve in different parts of the economy. Nevertheless, the overall pattern of a precipitous decrease in privacy, followed by a moderating decline after a privacy market emerges, is likely to hold in the aggregate.

Figure 2 shows the price of privacy as a function of the cost of obtaining and processing information. Until cost reaches v, privacy is free because it costs companies too much to collect information. At that point, the privacy market emerges, with a price of $a/2$ that progressively increases over time, increasing linearly with the reduction in information costs. The price eventually approaches $(a + v)/2$ as the cost of obtaining and processing information approaches zero.

Figure 3 shows the profits from the privacy market as the cost of obtaining and processing information decreases. Again, until cost reaches v, there is no market for privacy. At that point, profits from the privacy market shoot up to $a^2/8b$, only to decrease again (and at an increasing rate) until profits approach $(a - v)^2/8b$ as costs approach zero. This indicates that there will still be a viable privacy market, even if costs of obtaining and processing information go to zero.

FIGURE 2
How the Price of Privacy Will Change Over Time

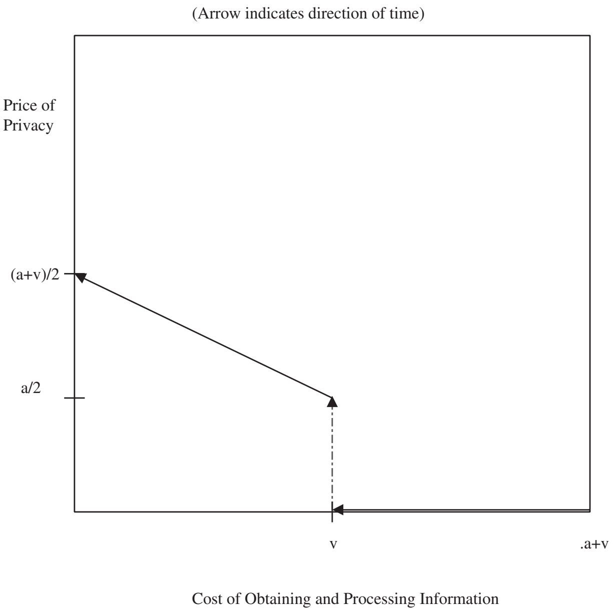


FIGURE 3
How Privacy Market Profits Will Change Over Time

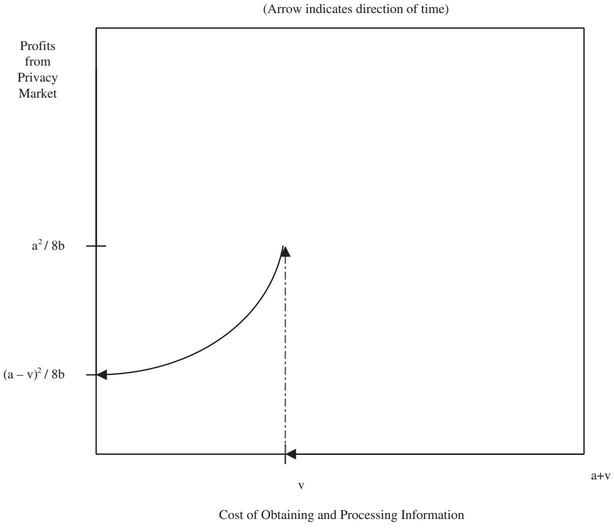


FIGURE 4
How Customer Privacy Utility Will Change Over Time

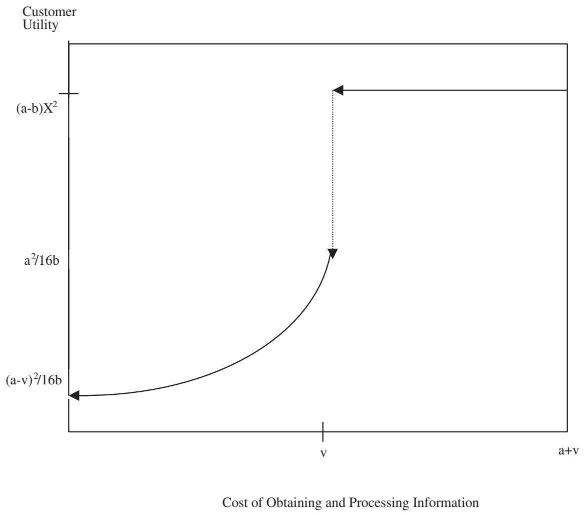


Figure 4 shows customer utility as a function of the cost of obtaining and processing information. Privacy-based utility has two elements, as we can see from Equation 1. There is utility from privacy and disutility from having to pay for it. Putting the two together, we can see that utility is maximized when companies have not yet begun eroding privacy. When information becomes cheap enough to obtain, utility drops due to the decreased privacy and then continues to drop, but at a decreasing rate, as customers begin to repurchase their lost privacy.

BUILDING AN INDUSTRY IN INTERNET PRIVACY

Our model indicates that as the cost of obtaining and processing information decreases, the emergence of a privacy market is inevitable, but that market is not enough to reverse the decline of privacy. A privacy market is already emerging to provide online privacy to interested consumers amid the various organizational mechanisms that are evolving to arrest the decline of online privacy. At the consumer level, many consumer advocacy groups (e.g., Privacy Foundation and Center for Democracy and Technology) educate consumers regarding their privacy rights and lobby the government and various regulatory agencies regarding appropriate regulations to safeguard consumer privacy. At the online marketers' side, associations (e.g., Center for Social and Legal Research, and Online Privacy Alliance) are being formed that focus on industry self-regulation or policing the practices with regard to consumers' privacy. In addition, many organizations are creating distinct job positions such as chief privacy officer (CPO) to oversee privacy protection practices within their organization, partly in reaction to high-profile privacy blowups over companies collecting and using data (e.g., DoubleClick's fiasco over consumer data collection and Amazon's pricing experiment over the Web), partly due to the realization that privacy protection is key to developing consumer trust and revenue, and partly to ward off legislation from the government. Finally, many third-party organizations have emerged to create the privacy market by acting as intermediaries between consumers and marketers. The three types of intermediaries operating in today's privacy market include the "anonymizers," the "infomediaries," and the "authenticators."

The anonymizers are third-party infrastructure providers that provide consumers the capability to surf the Web and send e-mail anonymously. Good examples of such organizations include Zero-Knowledge and Privada Inc., which provide anonymous browsing systems (Petersen 2001). They essentially provide cloaking services to consumers through untraceable pseudonymous identities at a monthly service charge of $50 to $60. Given that ISPs generally charge a $20 monthly service fee, consumers essentially pay $30 to $40 per month for the privacy-anonymity feature. The appeal of the anonymizers may not be universal, as not all consumers may want such total privacy. According to Westin (1967), the consumer population can be segmented into three groups based on their attitudes toward privacy: on one extreme, we have the *privacy fundamentalists* (those who are deeply concerned about privacy rights and breaches of privacy); at the other extreme, there are the *privacy unconcerned* (those who do not care about privacy and freely provide information); and those in the middle are called the *privacy pragmatists* (those who are willing to share information based on what they get in return). While the anonymizers may appeal to the privacy fundamentalists (Lester 2001), they may not appeal to privacy pragmatists, who may not value the complete "loneliness" (b) the anonymizers provide. However, it is clear from our model that as the costs of obtaining and processing information decrease and their valuation increases, anonymizers will be under increasing pressure to raise their prices to safeguard anonymity. This will lead to shrinking market shares in the equilibrium and a focus on consumer segments with very high valuation for privacy.

Other infrastructure providers provide some control to consumers as to how much privacy they want as they surf the Web. For example, Microsoft plans to add a privacy technology called Platform for Privacy Preferences (P3P) in its upcoming version of its browser (Internet Explorer 6.0) (Bowman 2001). With P3P, consumers surfing the Web can configure their browsers to dictate whether they will relay personal information to specific sites (accept or reject cookies) based on those sites' privacy policies. This feature allows consumers to control the level of privacy protection they desire instead of complete anonymity and thus may appeal to the privacy pragmatists.

Since the Internet Explorer comes free, it may seem that consumers are getting privacy services for free, but this will not be the case. First, there is cost involved at the consumers' end in deciding how much privacy is desired and in learning and setting the appropriate controls on the browser. Second, given the increasing valuation of information, work may already have begun by marketers to devise ways to obtain consumer information despite the P3P technology (Bowman 2001). This will obviously lead to decline in privacy and additional costs to protect it. Thus, in the context of our model, Microsoft's P3P is only a temporary solution to arrest the decline in privacy.

Microsoft's P3P could well fall into the category of an "infomediary" business model. Infomediary organizations, such as Lumeria and Persona, allow consumers to store their personal information in their own so-called "profiles." These profiles could contain demographic information, psychographic information, preference data, and current shopping interests, depending on what each consumer wishes to provide. Marketers interested in targeting these consumers join the network provided by these organizations. Advertisements are targeted to individual consumers based on the "opt-in" principle—consumers choose to "opt in" to advertisements/marketers that they wish to see. Marketers get to target their messages to specific demographic profiles, while consumers get messages from only those marketers or category of marketers they have given permission to. This creates a win-win situation for both consumers and marketers. The revenue from advertisements goes directly to the consumers, with the infomediaries taking a small margin (Lester 2001). In the context of our model, infomediaries provide privacy protection by restricting the passage of private information to only those whom the consumers have given permission to. This system does lower consumers' privacy (privacy still decreases as consumers provide information to some marketers, if not all), but consumers receive payment in return. Thus, in the ideal situation, their overall utility remains nondecreasing. In addition, their "loneliness" (lack of interaction with or communication from preferred marketers) is reduced, thereby contributing their overall utility. There is no out-of-pocket cost to consumers for participating within the network, but to the extent that the "customization" provided by the infomediary is inadequate, there are externalities present. For example, the network may not include the specific marketers from whom consumers would like receiving communication. In this case, the disutility in receiving communication from second-best marketers may exceed the payment the consumers receive in return.

While the "infomediary" model may appeal to privacy pragmatists, the overall success of the model depends on the coverage of the network (in terms of the type of marketers consumers wish to receive communication from), the degree of customization the consumers receive, and the revenue consumers receive in return for their information. If the infomediary market is too fragmented, then the above conditions may not be realized, and thus the market may not exist in equilibrium. On the other hand, if the market consists of a few players, each with significant market coverage, then it augurs well for the privacy market. While the increased valuation of consumer information may lead to marketers breaching privacy even within an "infomediary" system, some of these organizations could use monitoring mechanisms to ensure appropriate compliance by marketers (Kannan, Chang, and Whinston 1998).

The third type of intermediary, authenticators, consists of organizations that audit the privacy practices of online marketers on the basis of established privacy norms. Examples of such organizations include TrustE, which provides the TrustE seal of approval to Web sites that meet their privacy standards, and traditional audit organizations such as PricewaterhouseCoopers, which audits companies such as Microsoft, Expedia, and DoubleClick on how well they live up their stated privacy policies. These audit services can cost several million dollars, which is borne entirely by the organizations that request them; in addition, the service provider audits privacy policies, practices, and potential breaches to privacy by the organization and its employees. To the extent that consumers look for the seal of approvals from these authenticators and choose to do business with only reputed organizations that respect their privacy, their privacy is protected. Privacy pragmatists and privacy unconcerned may choose the above solution as a viable approach to safeguard privacy, while it may not appeal to privacy fundamentalists, who may want a more proactive approach. In the context of our model, consumers may not directly pay out of their pockets for such services, but they may pay indirectly through the premium they pay for goods and services they purchase from these reputed organizations. From the consumers' perspective, the extra premium they pay for such privacy protection could be much less than the reduction in their privacy risk costs, thus leading to an increase in overall utility. Since the premium may appeal to only those consumers with higher valuations for privacy, the authenticators cannot completely halt the decrease of consumer privacy, as other consumers may still choose to do business with organizations with less stellar privacy practices.

The net impact of the above three types of intermediaries would be to create a viable privacy market. Each model may appeal to different segments of consumers, and while privacy on the whole would decrease over time, these models can ensure that a market for privacy exists even under limiting conditions. In addition, nonmarket forces such as legislation (or fear of government legislation among marketers, leading to self-regulation and the need for authenticators) would ensure that privacy does not totally disappear.

AREAS FOR FUTURE RESEARCH

In developing our model, we have made several assumptions, one of which is that the cost of obtaining and processing personal information decreases over time. However, this is based on the premise that technological developments would make it easier to collect and analyze personal information. However, there is a school of thought that contends that technological developments would make it very easy for consumers on the Web to ensure anonymity. Already there are tools and technologies that allow consumers surfing the Web to assume untraceable pseudonyms, set up private chat rooms, cloak their surfing and behavioral patterns on the Web, and ensure confidentiality of all interactions (Loeb 2000). If the costs of designing and using such technology drop significantly over time, then it is conceivable that more consumers would adopt such technology and tools, and their appeal may move beyond the privacy fundamentalists to the privacy pragmatists. In such a case, it is conceivable that the costs of obtaining and processing personal information could increase over time rather than decrease. It may be an interesting exercise to examine how the privacy market would evolve under conditions of increasing cost and increasing valuation. However, evidence suggests that technological developments are more active in the area of personal information collection and analysis than privacy protection, so the net impact could be decreasing costs nevertheless.

Our discussion in the previous section has presented different mechanisms that are emerging to build a privacy industry. However, it is not clear how effective they are in safeguarding consumers' privacy while still creating an online environment in which consumers could conduct social and business interactions online. For example, it would be very interesting to examine whether intermediaries such as anonymizers can create a climate in which consumers can freely transact online. Are their risk perceptions any lower? Do consumers using such systems regard businesses as their "enemy"? Can such systems allow trust to be established between businesses and consumers? Does the environment inhibit their online behavior, and if so, what are the implications for e-commerce? Extant research has shown that the privacy risk *perception*, rather than the objective safeguards that are instituted, plays an important role in online consumer behavior (Hoffman et al. 1999). It would be very useful to examine how the different mechanisms—anonymizing, informediation, and authentication—affect consumers' perception of privacy risks and their online behavior. Such research may also provide insights into the efficacy of these different mechanisms and how the market for privacy might evolve over time.

CONCLUSIONS

In this article, we have presented a simple economic model to explore how individual privacy will fare over time, assuming no government intervention. We find support for the conventional assertion that the amount of privacy will decline over time and that privacy will be increasingly expensive for consumers to maintain. Our model suggests that a market for privacy will emerge that will enable customers to purchase a certain degree of privacy, no matter how easy it becomes for companies to obtain information, but the overall amount of privacy and privacy-based customer utility will continue to erode. On the basis of the emerging trends in the privacy industry, we have also provided details of possible market mechanisms through which a market for privacy could be maintained. The exact nature of this market may well rest on how effectively these mechanisms perform over time in protecting consumer online privacy. While the research questions highlighted in the previous section may shed some light on this issue, the nature of the market may also depend on the specific technological developments that are ongoing currently, such as wireless technology, bioengineering, and security technologies (Zerega 2001). It would be interesting to watch how they play an important role in shaping the market.

ACKNOWLEDGMENTS

This work was supported by the Center for E-Service at the Robert H. Smith School of Business, University of Maryland.

REFERENCES

Bellotti, Victoria. 1997. “Design for Privacy in Multimedia Computing and Communications Environments.” In *Technology and Privacy: The New Landscape*. Eds. Philip Agre and Marc Rotenberg. Cambridge, MA: MIT Press.

Bowman, Lisa. 2001. “Is Microsoft’s Privacy Plan an Improvement?” *CNET news.com*, March 22. Available: http://news.com.com/2100-1023-886552.htm

Cavoukian, Ann and Don Tapscott. 1996. *Who Knows: Safeguarding Your Privacy in a Networked World*. New York: McGraw-Hill.

Cespedes, Frank V. and H. Jeff Smith. 1993. “Database Marketing: New Rules for Policy and Practice.” *Sloan Management Review* 34 (4): 7-22.

Clark, Don. 2000. “E-Commerce (A Special Report): The Lessons We’ve Learned—Privacy: You Have No Secrets—It’s the Dark Side of E-Commerce: You Leave a Trail of Personal Information Wherever You Go.” *The Wall Street Journal*, October 23, p. R32.

enonymous.com. 2000. *Internet Privacy: A Summary of Privacy Ratings Research by enonymous.com*. Retrieved from http://www.privacyratings.org/research.htm

Feldman, Amy. 2000. “Protecting Your Financial Privacy.” *Money* 29 (6): 161-164.

Foxman, Ellen R. and Paula Kilcoyne. 1993. “Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues.” *Journal of Public Policy & Marketing* 12 (1): 106-119.

Hall, E. T. 1966. *The Hidden Dimension*. Garden City, NJ: Doubleday.

Harper, Christopher. 1998. *And That’s the Way It Will Be: News and Information in a Digital World*. New York: New York University Press.

Hoffman, Donna L., Thomas P. Novak, and Marcos A. Peralta. 1999. “Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web.” *The Information Society* 15 (2): 129-139.

Hosman, Lawrence A. 1991. “The Relationships Among the Need for Privacy, Loneliness, Conversational Sensitivity, and Interpersonal Communication Motives.” *Communication Reports* 4 (2): 73-80.

Kannan, P. K., Ai-Mei Chang, and Andrew B. Whinston. 1998. “Marketing Information on the I-Way.” *Communications of the ACM* 41 (3): 35-43.

Larson, J. H. and N. J. Bell. 1988. “Need for Privacy and Its Effect Upon Interpersonal Attraction and Interaction.” *Journal of Social and Clinical Psychology* 6:1-10.

Lester, Toby. 2001. “The Reinvention of Privacy.” *The Atlantic Monthly*, March, 27-39.

Loeb, Vernon. 2000. “Web Security, Privacy Are Goals of CIA Effort.” *The Washington Post*, February 16, p. A21.

Markoff, John. 1999. “The Privacy Debate: Little Brother and the Buying and Selling of Consumer Data.” *Upside* 11 (4): 94-106.

Mason, Richard O. 1986. “Four Ethical Issues of the Information Age.” *MIS Quarterly* 10 (1): 5-12.

Menon, Satya and Barbara E. Kahn. 1995. “The Impact of Context on Variety Seeking in Product Choices.” *Journal of Consumer Research* 22 (December): 285-295.

Petersen, Andrea. 2001. “E-Commerce (A Special Report): Industry by Industry—Privacy—Private Matters: It Seems That Trust Equals Revenue, Even Online.” *The Wall Street Journal*, February 12, p. R24.

Raju, P. S. 1980. “Optimum Stimulation Level: Its Relationship to Personality, Demographics, and Exploratory Behavior.” *Journal of Consumer Research* 7 (3): 272-282.

Richards, Jef I. 1997. “Legal Potholes on the Information Superhighway.” *Journal of Public Policy & Marketing* 16 (2): 319-326.

Rombel, Adam. 2001. “Privacy and Security in a Wired World.” *Global Finance* 15 (1): 26-31.

U.S. Senate. 2000. “Know the Rules, Use the Tools: Privacy in the Digital Age: A Resource for Internet Users.” U.S. Senate Judiciary Committee Report.

Westin, Alan. 1967. *Privacy and Freedom*. New York: Atheneum.

Zerega, Blaise. 2001. “Ten Trends for What’s Ahead.” *Red Herring*, December 17. Available from www.redherring.com/insider/2001/1217/419.html

ABOUT THE AUTHORS

Roland T. Rust (Ph.D., University of North Carolina at Chapel Hill) holds the David Bruce Smith Chair in Marketing at the Robert H. Smith School of Business at the University of Maryland, where he directs the Center for e-Service. His lifetime achievement honors include the American Marketing Association’s (AMA’s) Gilbert A. Churchill Award for contributions to marketing research, the Outstanding Contributions to Research in Advertising Award from the American Academy of Advertising, Fellow of the American Statistical Association, the AMA Career Contributions to the Services Discipline Award, and the Henry Latané Distinguished Doctoral Alumnus Award from the University of North Carolina at Chapel Hill. He has won best article awards for articles in *Marketing Science*, *Journal of Marketing Research*, *Journal of Marketing*, *Journal of Advertising*, and *Journal of Retailing*, as well as the Marketing Science Institute (MSI) Best Paper Award. His seven books include *e-Service*, *Driving Customer Equity*, *Service Marketing*, and *Return on Quality*. His work has received extensive media coverage, including a *Business Week* cover story and an appearance on *ABC World News Tonight With Peter Jennings*. He is the founder and chair of the AMA Frontiers in Services Conference and serves as founding editor of the *Journal of Service Research*. Professor Rust also is an area editor at *Marketing Science* and serves on the editorial review boards of the *Journal of Marketing Research*, *Journal of Marketing*, and the *Journal of Interactive Marketing*.

P. K. Kannan (Ph.D., Purdue University) is Safeway Fellow and Associate Professor of Marketing at the Robert H. Smith School of Business at the University of Maryland, where he is the associate director of the Center for E-Service. His research focuses on e-commerce, centering on marketing information services on the Internet, pricing information products, and marketing and product development in virtual communities. He is working with the IBM Institute for Advanced Commerce on e-couponing and also with National Academy Press on pricing information products. He is an associate editor of *Decision Support Systems and Electronic Commerce* and serves on the editorial board of the *Journal of Service Research* and the *International Journal of Electronic Commerce*. He is currently editing a special issue on marketing in the e-channel for the *International Journal of Electronic Commerce*. He is the chair for the American Marketing Association Special Interest Group on Marketing Research. He has corporate experience with Tata Engineering and Ingersoll-Rand and has consulted for companies such as Frito-Lay, Pepsi Co, Giant Food, SAIC, Fannie Mae, Proxicom, and IBM.

Na Peng is a doctoral student at the University of Maryland.