

Information Privacy in the Marketplace: Implications for the Commercial Uses of Anonymity on the Web

Donna L. Hoffman, Thomas P. Novak, and Marcos A. Peralta

Project 2000, Owen Graduate School of Management, Vanderbilt University, Nashville, Tennessee, USA

While there is no question that the commercial development of the World Wide Web is still in its infancy and growing rapidly, this development faces a serious barrier to ultimate commercialization. In this article we develop the argument that the primary barrier to the successful commercial development of the Web is the current lack of consumer trust in this new commercial medium. This lack of trust is engendered primarily by the industry's documented failure to respond satisfactorily to mounting consumer concerns over information privacy in electronic, networked environments. We examine how such concerns are affecting the growth and development of consumer-oriented commercial activity on the World Wide Web and investigate the implications of these concerns for potential industry response. In the short run, the commercial development of the Web depends on giving consumers the opportunity to be anonymous when engaging in information exchanges and online transactions. Ultimately, however, commercial Web providers must come to realize that the Internet dramatically shifts the balance of power between a business and its customers, and therefore, radical new business strategies will be required for long-term success. Because the Web offers unprecedented opportunities for interacting with customers, strategies that take advantage of the medium's unique features are likely to reap important rewards in customer satisfaction, loyalty, and retention. Therefore, in the long run, the most effective way for commercial Web providers to develop profitable exchange relationships with online customers is to gain consumer trust by allowing the balance of power to shift toward more cooperative interactions between firms and their customers.

Keywords commercialization of the Internet, computer-mediated environments, consumer privacy, online anonymity, online retailing

Received 17 December 1997; accepted 17 November 1998.

Address correspondence to Donna Hoffman, Owen Graduate School of Management, Vanderbilt University, Nashville, TN 37203, USA. E-mail: donna.hoffman@vanderbilt.edu Web site: <http://www2000.ogsm.vanderbilt.edu/>

The Information Society, 15:129-139, 1999

Copyright © 1999 Taylor & Francis

0197-2243/99 \$12.00 + .00

Currently, revenues from consumer online shopping, estimated at \$5.775 billion for 1998, are meager, despite optimistic industry forecasts that such revenues are expected to grow dramatically to \$37.5 billion over the next 5 years (Jupiter Communications, 1998). Barriers such as few online consumers interested in the few available online offerings and the absence of profitable business models are believed to play important roles in the relative dearth of commercial activity among businesses and consumers on the Internet.

While there is no question that the commercial development of the World Wide Web is still in its infancy and growing rapidly, this development faces a serious barrier to ultimate commercialization. We argue that the primary barrier to the successful commercial development of the Web is the current lack of consumer trust in this new commercial medium. We believe that this lack of trust is engendered primarily by the industry's documented failure to respond satisfactorily to mounting consumer concerns over information privacy in electronic, networked environments. In this article we examine how such concerns are affecting the growth and development of consumer-oriented commercial activity on the World Wide Web and investigate the implications of these concerns for one potential industry response: the commercial uses of online anonymity.

The successful commercial development of the Web depends upon a variety of interdependent structural factors. Often cited is the fact that there are still relatively few consumers online in general and relatively few offerings available for online purchase, especially compared to purchases made in the physical world of sophisticated retail environments and direct mail shopping. Indeed, although in 1997 over 45 million individuals 16 and over had used the Web in the United States at least once, only 4.5 million or 10% had ever purchased a product or service on the Web (Hoffman & Novak, 1997b). In addition, almost

123 million people, or nearly 62% of the United States population in 1997, had no access to the Internet and had never used it, and another 32 million Americans had access but had yet to use the Internet even once (Hoffman & Novak, 1998).

Still, the number of consumers on the Internet is growing impressively and increasingly mirrors the demographics of the population as a whole. Numerous market research studies additionally suggest that the very small but growing number of cyberconsumers who do shop online consistently report high rates of satisfaction with the shopping experience. Not surprisingly, convenience is seen as the key benefit that online shopping provides. From a marketing perspective, the problem can be seen as how to stimulate "trial," as the rate of conversion is nearly 100%.

Although it is not possible yet to do all of one's shopping online, there has been a rapid expansion in the diversity and number of products available for consumption on the Web. Since 1995, many commercial Web sites have evolved from static "brochure-ware" to innovative and exciting interactive environments where consumers may find an increasingly broad range of offerings from physical goods like books, cars, and groceries to information offerings and services including investments, travel, and entertainment.

As the technologies for secure payment mechanisms continue to mature, the last several years have also witnessed the explosive development of a variety of mechanisms designed to provide for the secure exchange of information. Encryption technology, digital signatures, certificates and authentication, secure protocols, secure credit card and debit payment systems, and digital currency all compete to protect business transactions. However, no single mechanism or combination of systems has yet to emerge as a security standard, and numerous surveys have shown (see, for example, Pitkow & Kehoe, 1997; Boston Consulting Group, 1997) that security concerns loom large among online users and remain a critical contributing factor inhibiting consumer behavior.

Additionally, despite the fact that the Web offers a number of important benefits to both consumers and firms (Garcia, 1997; Hoffman et al., 1995; Wigand, 1997), most online firms are still searching for the best strategies and business models for conducting electronic commerce. If the Web were to ultimately fail as a commercial medium, it would not only imply a loss of these benefits, but could also threaten the development and evolution of computer-mediated environments in general.

Yet despite these very real barriers to continued development, we believe that the commercial portion of the Web faces a far more serious threat from the perceived lack of information privacy accorded to cyberconsumers during the online navigation process. Unlike transactions

that take place in the physical world, we argue that these perceptions of computer-mediated interactions are influencing consumer willingness to engage in relationship exchanges with online businesses, and negatively impacting the further development of commercial efforts. Even worse, preliminary research suggests that this impact is likely to grow as less technically sophisticated consumers come online and are less able to sort out valid threats to privacy from media hype and misinformation.

We investigate these issues in this discussion article. First, we examine consumer concerns regarding information privacy on the Web and provide empirical support for our argument regarding the consumer lack of trust in online commercial environments. A relationship exchange framework provides the theoretical context for our analysis and permits examination and comparison of the role of trust in both the physical and virtual worlds, and an assessment of how the lack of trust is negatively impacting the further development of online commercial activity by consumers. Next, we examine alternatives that may contribute to the short-term development of the "marketplace" (Rayport & Sviokla, 1994). Finally, we examine what is necessary in the long run for the emergence of mutually beneficial online exchange relationships among firms and consumers interacting in online commercial environments.

CONSUMER CONCERNS REGARDING INFORMATION PRIVACY

Consumer privacy in online environments is an important policy issue, and the debate concerning how to proceed involves users, government authorities, and business communities. As noted, we focus our attention on information privacy issues on the Web rather than on anonymity, because we regard anonymity as one effective strategy that consumers can use to achieve desired levels of privacy (Goodwin, 1991; Marshall, 1974). On the Web, anonymity is valuable and regarded as desirable for many online shoppers as one of the most powerful methods of protecting information privacy.

In this section, we summarize the research documenting consumer concerns over information privacy. Hoffman et al. (1998) investigated key consumer perceptions of privacy based on consumer responses to the Nielsen Media Research/CommerceNet Internet Demographics Study (Nielsen Media Research, 1997) and the GVU 7th WWW User Survey (Pitkow & Kehoe, 1997). They found that consumer expectations of privacy depend on the medium. In traditional media, they noted that attitudes range from "tolerance to resigned disgust," but that in electronic media, consumers' need for control and protection is intense.

Based on their empirical analyses, they further argued that consumers do not view their personal data in the context of an economic exchange of information, as many

commercial Web providers believe. That is, consumers are decidedly uninterested in selling their personal data to Web sites, either for monetary incentives or access privileges. Rather, Web consumers report wanting another type of exchange (Culnan & Milberg, 1998): one that characterizes an "explicit social contract executed in the context of a cooperative relationship built on trust" (Hoffman et al., 1998).

Current commercial Web provider behavior (Landesberg et al., 1998; Miller, 1995) suggests that many cybermarketers lack faith in consumers or treat them poorly (Bloom et al., 1994; Caruso, 1998; Culnan & Armstrong, 1999; Green, 1998). Consumers know this (*Business Week*, 1998) and respond accordingly, either by withholding their personal data and/or by providing false data (Boston Consulting Group, 1997; Hoffman et al., 1999; Pitkow & Kehoe, 1997). Despite this, empirical research suggests that consumers do realize that personal data are important to Web marketers, and report being interested in providing such information, both when it is appropriate and provided that certain enabling conditions, including full disclosure and informed consent, are present (Culnan & Armstrong, 1999; Hoffman et al., 1999).

On the basis of this growing body of empirical research, we propose a set of issues for further discussion:

1. Consumers are concerned about their information privacy when shopping on the Web.
2. Because consumers cannot make anonymous discrete transactions when shopping online, they instead seek to engage in relationship exchanges.
3. Relationship exchanges on the Web involve both an economic and a social contract.
4. When consumers choose not to engage in relationship exchanges it is because they do not trust commercial Web providers to honor their social obligations of respecting consumer information privacy.
5. Consumers make cost-benefit trade-offs when considering whether to engage in a relationship exchange. However, such trade-offs are not evaluated purely on an economic basis. Instead, consumers decide to engage in commercial transactions on the Web primarily on the basis of noneconomic factors.

Consumers Are Concerned About Their Information Privacy When Shopping on the Web

Information privacy is the ability of an individual to control the access that others have to personal information (Culnan & Armstrong, 1999; Foxman & Kilcoyne, 1993; Westin, 1967). online shoppers are concerned about their information privacy because they do not have the ability to control the access others have to personal information. According to Goodwin (1991), consumers' information

privacy concerns two dimensions: *environmental control* and *secondary use of information control*.

Environmental control is the consumer's ability to control the actions of other people in the environment during a market transaction or commercially oriented exchange. Environmental control directly affects the security of online shopping. For example, in the physical world, a consumer may be concerned about giving out credit-card information over the telephone to an unknown mail-order company. On the Web, some consumers may fear typing in their credit card information to any commercial Web provider. Similarly, a commercial Web provider may fear the efforts of a hacker out to steal a cache of credit-card numbers.

Secondary use of information control is the consumer's ability to control the dissemination of information related to or provided during such transactions or behaviors to those who were not present. We consider secondary use of information to be the use of personal information for other purposes, subsequent to the transaction where the information was originally collected (Culnan & Milberg, 1998). On the Web, this dimension is manifested by consumers' concern that Web providers are selling their personal information to third parties without their knowledge or permission.

Both issues are of great concern to consumers in online environments such as the Web, as well as in traditional retail environments in the physical world. Although we do not address it in this article, an important research question is the relative weight consumers place on these two dimensions and whether such weightings vary by both product category and/or whether the item was purchased in traditional versus online retail environments.

Environmental control cannot currently be assumed for online transactions over the Web because, at this writing, the Internet still lacks mature mechanisms for the secure transmission of information. Secure transaction technologies that grant both consumers and commercial Web providers control over the environment for online transactions may provide the most attractive long-run solutions. Yet, even though there may eventually be readily available and reliable technology that is understood by consumers, consumers may still not feel confident to engage in online transactions. Interestingly, even though consumers report that security concerns (environmental control) are a major deterrent to shopping online today, consumers are also discouraged from engaging in information and commercial exchanges by their fears of commercial Web providers' likely secondary use of their personal information (Hoffman et al., 1999).

Contrary to environmental control, which is a shared concern between commercial Web providers and consumers, secondary use of information is a source of conflict between commercial Web providers and consumers. Even

though this is also true for transactions in the physical world, the issue takes on a greater urgency in computer-mediated commercial environments, owing to the unique characteristics of the Internet medium (Hoffman & Novak, 1996; Hoffman et al., 1995).

First, the Internet facilitates the widespread collection, dissemination, and commercial use of personal information because it is a distributed, networked environment requiring fewer sources and data formats than in the physical world (Cavoukian & Tapscott, 1996). Data mining and data warehousing opportunities are greater than ever before by exploiting the capabilities of the Internet, high-speed networks, and terabyte data storage (see, for example, Cespedes & Smith, 1993; Hearst, 1997). Traditionally, consumer information is stored in a much wider variety of databases and data formats and is much more difficult to combine, analyze, and access.

Second, online shopping potentially allows commercial Web providers to collect much more detailed consumer behavior information than is possible from most physical world shopping trips. Commercial Web providers can not only collect the same information available in most “real-world” transactions—identity data, credit history, employment data, and public record information—but also additional information such as electronic mail address, specific history of goods and services searched for and requested, some other Internet sites visited by the consumer, and contents of the consumer’s data storage device (Choi et al., 1997).

Finally, with the notable exception of so-called single-source data (for example, consumer scanner panels), most secondary uses of information captured from transactions in the physical world have been limited to aggregate group-level data.¹ This typically involves inferring broad characteristics and behaviors about groups of consumers (such as geography and demographics) and drawing generalizations across those groups. Secondary use of information captured online from computer-mediated transactions can much more easily take advantage of individual-specific information.² For example, data specifically linked to a single identifiable person can be used to customize an offer to that potential customer to maximize the likelihood of consumer acceptance of the offer. Importantly, this activity can be done without the consumer’s awareness, let alone permission.

Because Consumers Cannot Make Anonymous Discrete Transactions When Shopping online, They Instead Seek to Engage in Relationship Exchanges

Transactions (or exchanges) can be seen as dispersed over a continuum from discrete to relational. Relationship exchanges differ from discrete transactions along several key

dimensions (Culnan & Milberg, 1998; Dwyer et al., 1987; Houston & Gassenheimer, 1987; MacNeil, 1980; Peppers & Rogers, 1997).

Relationship exchanges transpire over time, and every transaction must be viewed in terms of its history and its expected future. Relationship exchanges are based on implicit and explicit assumptions, trust and planning. Furthermore, relationship exchange participants can be expected to derive complex, personal, noneconomic satisfactions, and engage in social exchange.

Discrete transactions specifically exclude these relational elements. Very limited communications and narrow content characterize discrete transactions. The identity of all parties to a transaction must be ignored or relational aspects to the exchange transactions come into play. An unbranded gasoline (e.g., no brand relationship), out of town (e.g., unlikely that identities of buyer or seller will be known to each other) at an independent station (e.g., no prior relationship with the seller’s firm), paid for with cash (e.g., no clues to buyer identity) approximates a discrete transaction (Dwyer et al., 1987). A one-time purchase of a pack of gum with cash at a convenience store while on vacation is another example of a discrete transaction.

The notion of instantaneous exchanges between completely anonymous partners who will never interact in the future is of course an abstract model that does not exist in the real world (Dwyer et al., 1987), so most transactions conducted in the physical world are in truth within the boundaries of relationship exchanges. This is even more true for current online transactions. In the virtual world, consumers do not have the opportunity to be anonymous by buying “unbranded gasoline out-of-town at an independent station paid for with cash.” Instead, online consumers are required to engage in relationship exchanges.

Relationship Exchanges on the Web Involve Both an Economic and a Social Contract

A transaction (exchange³) over the Web implies not only a simple quid pro quo (a monetary exchange for goods) between two entities, but also exchanges that are often indirect (Culnan & Milberg, 1998). These may involve intangible and symbolic aspects, and more than two parties may participate. Thus, Web transactions involve both (1) an economic contract characterized by monetary exchange for goods and services, and explicit legal forms and (2) a social contract characterized by nonmonetary exchanges and implicit (nonlegal) forms.

Consumer behavior in economic contracts is directed to maximize personal economic utility; in social contracts with unpredictable outcomes, consumers do not tend to conduct a financial cost–benefit analysis (Blau, 1964). In this view, social exchange refers to voluntary actions of individuals motivated by the returns they are expected to

receive and typically do in fact receive from others. In this sense, social exchange tends to engender feelings of personal obligation, gratitude, and trust, while economic exchange does not.

Another difference is that economic contracts tend to be regulated by law, while social contracts are very difficult to regulate. The basic and most crucial distinction between economic and social contracts is that social exchange entails *unspecified* obligations (Blau, 1964). Since there is no way to ensure an appropriate return for an unspecified obligation, social exchange requires *trusting* others to discharge their obligations. Social contract obligations cannot be enforced through legal sanctions like economic contracts (Blau, 1964).

It seems obvious that relationship exchanges over the Web involve both an economic and a social contract. The economic contract with the seller is characterized by an exchange of goods or services for money. Because the seller may capture personal information from the consumer without the consumer's notice or consent, this information exchange is not included in the quid pro quo and is thus comprised within a social contract.

In the current commercial Web environment, this social contract dictates how commercial Web providers handle consumer information. A consumer engaging in an online transaction implicitly trusts the seller not to compromise his or her information privacy. Yet in current practice, the exact nature of this future return is rarely stipulated in advance, and not regulated by law.

When Consumers Choose Not to Engage in Relationship Exchanges, It Is Because They Do Not Trust Commercial Web Providers to Honor Their Social Obligations of Respecting Consumer Information Privacy

Current practice reviewed earlier has led many consumers to expect that commercial Web providers cannot be relied upon to respect consumer information privacy. Trust⁴ and relationship commitment⁵ are central to successful relationship exchanges (Morgan & Hunt, 1994). We believe that many consumers avoid relationship exchanges on the Web primarily because they do not trust commercial Web providers. We believe this lack of trust arises from consumers' belief that commercial Web providers do not share their values about information privacy in online commercial environments, and that commercial Web providers are likely to engage in opportunistic behaviors. This may likely lead to a lessened commitment to the relationship, which in turn generates higher decision-making uncertainty, less cooperation, and higher propensity to leave.

In the physical world, low consumer relationship commitment, regardless of the seller's position, will result in

discrete exchanges and/or no exchanges at all (Dwyer et al., 1987; Milne & Gordon, 1993). In the virtual world, there are currently no opportunities for discrete exchanges, so low relationship commitment can be expected to result in no exchange. Computer-mediated environments threaten consumer information privacy in such novel ways that consumers tend to adopt extreme positions between low and high relationship commitment. Only when commercial providers adopt behaviors consistent with high relationship commitment (for example, by posting privacy policies) will consumers follow with trust and an increased propensity to engage in online transactions (Culnan & Armstrong, 1999).

Consumers Make Cost-Benefit Trade-Offs When Considering Whether to Engage in a Relationship Exchange

However, such trade-offs are not evaluated purely on an economic basis. Instead, consumers decide to engage in commercial transactions on the Web primarily on the basis of noneconomic factors.

We believe that recent empirical studies discussed earlier support the idea that online consumers do not use economic criteria solely as the basis of judging the trade-off between the gain from the transaction and information privacy. Instead of economic utility-based decisions, we argue that consumers structure their decisions in the context of a relationship development process, in which they balance a number of critical relationship marketing variables (Donaldson & Dunfee, 1994; Dwyer et al., 1987), with the objective of engaging in mutually favorable commercial relationships (Culnan & Milberg, 1998).

THE COMMERCIAL DEVELOPMENT OF THE WEB IN THE SHORT RUN

In the short run, online consumers will not develop trust in commercial Web providers because there is a conflict of interest without a clear solution. As we describe, one way of resolving this conflict and encouraging consumers to engage in online transactions, especially in the short run, is by giving consumers the option of traceable anonymity and/or pseudonymity. *Traceable anonymity* is a communication that gives the recipient no clues about the sender's identity but leaves this information in the hands of a third party. *Traceable pseudonymity* is communication with a nom de plume attached, which can be traced back to the author (by someone), although not necessarily by the recipient (Froomkin, 1996a).

At the same time, commercial Web providers will accept those transactions only if they have the minimum information to ensure authentication, certification, confirmation, nonrepudiation, and payment. These functions can

be ensured through the use of pseudonymity and a third party acting as a mediator.

Conflict of Interest Between Commercial Web Providers and Consumers

During the purchasing process, marketers have established that consumers pass through the following stages: (1) search; (2) purchase (negotiation, decision, payment); (3) fulfillment and delivery; and (4) postpurchase relationship. In each of these stages, consumers and commercial Web providers are confronted with dissimilar and conflictive interests (Driscoll et al., 1997; Froomkin, 1996b). We outline these issues in Table 1.

These conflicts of interest are not easily solved in the short run. In the first place, the U.S. federal government currently supports industry self-regulation for Internet privacy, perhaps concerned that regulation is likely to do more harm than good (Froomkin, 1996b). Further complicating the matter, the European Union Privacy Directive (Andrews, 1998) may very likely wreak havoc with electronic commerce efforts in the United States, as it serves at the same time to raise consumer awareness of privacy protection policies and procedures in other countries. Second, consumers want to preserve their information privacy, and there is no evidence to date that they desire financial incentives in exchange for giving it up. Finally, as we have seen, most commercial Web providers' current marketing practices have met with considerable and mounting objections in the virtual world.

One feasible short-run solution is to enable and accept anonymous and/or pseudonymous transactions in the Web. As we show next, this implies that (1) commercial Web providers will accept some restrictions in the information they receive, (2) consumers will relinquish the opportunity to be completely anonymous, and (3) the government will not regulate attempts to preserve commercial anonymity in the Web.

The Feasibility of the Short-Run Solution

If we analyze carefully the commercial Web providers' requirements outlined in Table 1, only authentication, certification, confirmation, payment assurance, and nonrepudiation are strictly necessary to complete a transaction. Knowing a consumer's identity and possessing consumer information for data mining may be important for commercial Web providers but are not absolutely necessary to conclude a discrete transaction. Moreover, the necessary functions may be performed without knowing the real identity of the consumer, using the following mechanisms.

Buyer's Authentication. In low volume/value transactions, knowing the identity of the buyer to guarantee the

purchase is not necessary for transactions conducted in the physical world, so it sounds reasonable not to require it in computer-mediated commercial environments. In high volume/value transactions, a traceable anonymity/pseudonymity scheme can be implemented, where the seller may trace the consumer identity only in case of dispute.

Buyer's Certification. Consumers may declare some attributes of their profile relevant to the transaction—age, nationality, state of residence, and so on—without giving the seller their physical identity. In those cases where the seller requires confirmation of these attributes, a traceable pseudonymity scheme may be implemented in which each person has one or various pseudonyms and associated profiles.

Confirmation and Payment Assurance. The availability of digital cash may solve this issue, allowing anonymous payments and confirmation (Driscoll et al., 1997).

Nonrepudiation. A traceable anonymity/pseudonymity scheme can be implemented where the seller may trace the consumer's identity only in the case of dispute.

Under such a scheme, consumers will be able to preserve their anonymity when making small purchases by using digital cash mechanisms. These discrete transactions are akin to buying "unbranded gasoline, out of town at an independent station, paid for with cash" in the physical world. For larger transactions, consumers will be able to preserve only a part of their information privacy by using pseudonymous schemes.

From the public policy perspective, this solution implies that the government should not attempt to regulate or forbid commercial anonymous communications on the Web. Such regulation will have only a very limited effect, due to the inherent difficulties of controlling online behavior globally and developing technologies for such control that are sustainable over time. Regulation could conceivably have the additional negative consequence of diminishing the number of discrete transactions. This would be unfortunate, as discrete transactions are one of the most important alternatives for the further development of shopping in computer-mediated environments.

Pros and Cons of This Approach

The main virtue of this short-term solution is that the volume of online shopping may increase because consumers will have the opportunity to conduct discrete transactions while preserving their information privacy. Furthermore, it opens the door to a long-term solution.

The weakness of this short-term solution is that it is a short-term solution. It does not solve the cause of the problem: the conflict of interest between online consumers

TABLE 1
Seller/consumer conflict of interest at stages of the purchasing process

Stage	Seller interests	Consumer interests
Search	Data mining: Knowing consumers' data to build up a database of customers and their searching/buying profiles.	Anonymity: Consumers want to minimize the information disclosed to the seller.
Negotiation	Buyer's identity: Knowing a buyer's identity before entering a negotiation may affect the commercial Web provider's commitment to finish the negotiation.	Authentication: Confirming the seller's identity prior to purchase helps ensure that goods will be genuine, and that service or warranties will be provided as advertised. Anonymity: Consumers want to minimize the information disclosed to the seller.
Decision	Buyer's authentication: Knowing a buyer's identity before making a sale may assist in proof of order and guarantee of purchase. Buyer's certification: The merchant may need proof that the buyer possesses an attribute required to authorize the sale. For example, some goods may only be sold to those licensed to use them; other goods require that the purchaser be over eighteen. Some products cannot be sold in some parts of the country, while others cannot be exported.	Anonymity: Consumers want to minimize the information disclosed to the seller Or Secondary use of information control: The consumer may want control over the amount of buyer/transactional information disclosed to third parties.
Payment	Confirmation: The merchant needs to be able to prove to any third party involved in the transaction (such as a credit-card company) that the customer did indeed authorize the payment. Payment assurance: This can be achieved by having payment before sale, at time of sale, or by provision of a payment guarantee. A credit reference by a trusted third party provides a lesser form of assurance, but it at least demonstrates that the buyer is capable of making the payment.	Confirmation: The consumer will want some form of irrefutable proof of the transaction, such as a receipt. Integrity: The consumer desires protection against unauthorized payments. Anonymity: Consumers will want control over the amount of transactional information disclosed to the merchant.
Fulfillment/ delivery	Nonrepudiation: The commercial Web provider wants protection against the customer's unjustified denial that he or she placed the order, or that the goods were not delivered.	Recourse: Comfort that there is recourse if the seller fails to perform or deliver.
Postpurchasing relationship	Develop an exchange relationship: The seller wants the consumer to repurchase in the future, engaging in a long-term relationship.	Recourse: Comfort that there is recourse if the product fails to perform or doesn't comply with the specifications. Develop an exchange relationship: The consumer may want to have a reliable provider where he or she can buy repetitively, with a certain price and quality.

and commercial Web providers. Both parties will have to rely on a third party that will act as a mediator in case of conflict during the payment, fulfillment/delivery, and postsales steps. In truth, certification authorities are performing some of these functions, and are among those candidates for the relied third party in traceable anonymous/pseudonymous commercial exchanges. Unresolved are issues such as who these third parties should be, what are their responsibilities, and who will reinforce their obligations in case of dispute.

THE COMMERCIAL DEVELOPMENT OF THE WEB IN THE LONG RUN

If consumers and commercial Web providers can make anonymous discrete online transactions, why would either be willing to engage in more extensive exchange relationships in the long run? The answer is that exchange relationships imply economic and social benefits for both parties that go beyond the obvious economic utility generated by the simple exchange of goods or services for money.

Yet an analysis of the conflicts of interest between consumers and commercial Web providers shows that the two parties are diametrically opposed in their positions. If commercial Web providers want to develop exchange relationships in the long run, which are much more profitable than discrete transactions, commercial Web providers will have to balance the power relationship with customers and gain their trust. Even though the cost may look very high, the reward is stable, loyal exchange relationships that today simply do not occur, and will not occur, if things do

not change. These rebalancing actions include recognizing the consumers' rights over data ownership by giving opt-in chances in a market-driven environment, and accepting and enforcing opt-out regulations.

The Information Privacy Matrix

We analyze the various possibilities of the different parties involved in the information privacy debate along the dimensions of policy and regulation. These public positions are rendered graphically in the information privacy matrix shown in Figure 1.

Policy. The distinction along this dimension concerns the mechanisms used to administer consumers' rights of data ownership. There are two alternative approaches: opt-out and opt-in. The opt-out model posits that the best policy is to offer consumers the alternative of declining to disclose only when they do not want the seller to use their information for secondary use purposes. The default position of the opt-out model is that unless the seller is otherwise informed, the seller is free to use the consumer's data in any legal way that the seller sees fit. Opt-out privacy policies thus place the entire information protection burden on the consumer and set up an environment of ipso facto mistrust between the Web provider and the consumer.

The opt-in model states that the best policy is to offer consumers the alternative of disclosing by explicitly authorizing commercial Web providers to make secondary or other stated use of their information. Thus, the opt-in model does not assume the consumer wishes his or her data used for any purpose, but instead requires the consumer

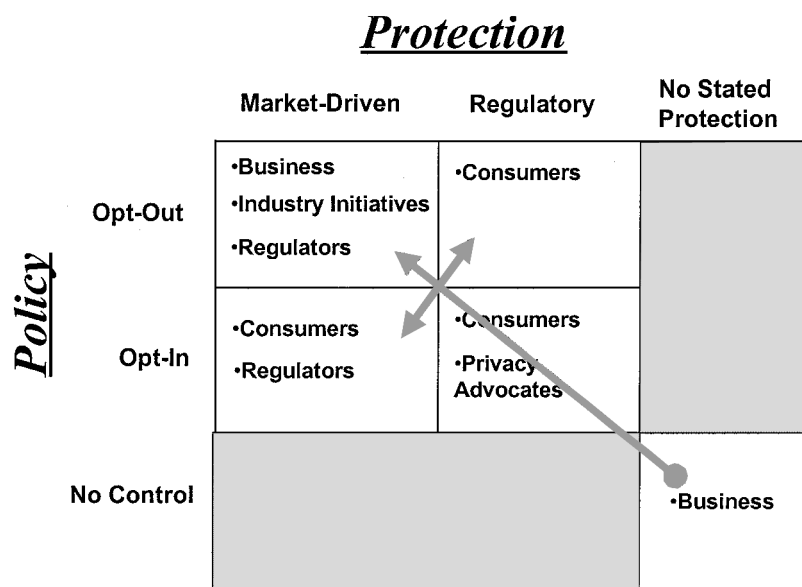


FIG. 1. The information privacy matrix.

to inform the seller that he or she accepts such a position. Such policies shift more of the information protection burden to the seller and require cooperation and trust between the consumer and Web provider.

Protection. The distinction along this dimension is how the policy will be directed and enforced. Again, we have two models: market-driven and regulatory. The market-driven model posits that companies protect consumer privacy in order to enhance reputation and sales. The regulatory model posits that government rules deter improper disclosure of personal information. Both approaches have their own limitations in the protection of privacy. A chief failure of the market-driven approach is that customers find it costly or impossible to monitor how companies use personal information. Moreover, as a form of voluntary regulation, it is impossible to guarantee 100% compliance. Government regulation is subject to the well-known possible failures of rigid, costly, and/or ineffective rules (Swire, 1997).

Current business and industry initiatives essentially propose to continue with the direct marketing policies originated in the physical world, based on market-driven opt-out practices. Consumers, on the other hand, are currently clamoring for new models based on new regulation and either opt-in or opt-out alternatives.

Currently, however, except for a handful of commercial Web sites, most commercial Web providers' information privacy practices do not position them in the "market-driven opt-out" cell, but rather in the cell defined by "no stated protection" and "no control." The likely trend is for commercial Web providers to migrate toward the market-driven opt-out model, while consumer segments will adopt positions that combine both market-driven opt-in and regulatory opt-out protection policies. For example, regulatory opt-in has been called for by numerous consumer advocacy groups that want to require providers of commercial Web sites targeted to children to obtain parental permission prior to collecting information from them (Center for Media Education, 1996a, 1996b). A bill comprising FTC regulations to that effect was recently enacted into law (U.S. Senate, 1998).

A Feasible Long-Run Solution

Our solution is simple, though it departs radically from traditional practice and will be difficult for many firms to implement. We believe that in the long run, the most effective way for commercial Web providers to develop profitable exchange relationships with online customers is to gain consumer trust. This trust is best achieved by allowing the balance of power to shift toward a more cooperative interaction between the firm and its customers.

The concept of relationship marketing argues that consumers will have increased commitment to the relationship if they perceive that commercial Web providers share their information privacy values and that commercial Web providers will not engage in opportunistic behavior. Such cooperative behaviors require a paradigm shift on the part of marketers (Hoffman & Novak, 1996), but are more appropriate in the new interactive medium defined by the Web.

SUMMARY

Currently, revenues from consumer online shopping have yet to reach large numbers, and a number of reasons have been advanced for the relative dearth of commercial activity between businesses and consumers on the Internet. Often cited is the fact that there are still relatively few consumers online in general and relatively few offerings available for their online purchase, especially compared to the physical world of sophisticated retail environments and direct-mail shopping. Additionally, the technology for secure payment mechanisms has yet to mature, and is a contributing factor inhibiting consumer behavior. Even among those firms that have set up shop online, most are still searching for the best strategies and business models for conducting electronic commerce.

Yet at its core, the reason online users have yet to shop online in large numbers, or even provide information to Web providers in exchange for access to information offered on-site, is because of the fundamental lack of faith that currently exists between most businesses and consumers on the Web today. In essence, consumers simply do not *trust* most Web providers enough to engage in relationship exchanges with them.

In the short run, the commercial development of the Web depends on giving consumers the opportunity to be anonymous and/or pseudonymous when engaging in information exchanges and online transactions. At the same time, it depends on Web providers receiving the minimum information necessary, and only the minimum necessary, in order to complete the exchange: for example, authentication, certification, confirmation, nonrepudiation, and payment in the case of an online transaction. These functions can be ensured through the use of pseudonyms and third parties acting as mediators. Under such an inherently cooperative system, which explicitly recognizes the rights and responsibilities of both parties in the exchange, we expect that many more consumers may choose to engage in information exchanges and conduct discrete online transactions.

Recognizing consumers' rights to data ownership on the Internet is an important first step in this process. At a minimum, this means industry acceptance and enforcement of stated opt-out policies regarding information exchange.

Ultimately, however, we believe that opt-in, informed consent policies are likely to reap the greatest rewards for firms doing business on the Internet. Even though such cooperative behaviors require new ways of thinking about what it means to do business, the likely benefit of stable exchange relationships among trusting and loyal cybercustomers is well worth it.

Ultimately, commercial Web providers must come to realize that the Internet dramatically shifts the balance of power between a business and its customers, and therefore, radical new business strategies will be required for long-term success. Because the Web offers unprecedented opportunities for interacting with customers, strategies that take advantage of the medium's unique features are likely to reap important rewards in customer satisfaction, loyalty, and retention. However, unlike the physical world, the willingness of consumers to enter into exchange relationships on the Web is not assured, and trust cannot be assumed. Indeed, terrestrial businesses, through direct marketing activities, have trained their customers that they cannot trust firms to protect their privacy nor to look out for their interests.

Despite the fact that the number of people using the Internet is growing dramatically, until the Web is seen as "ready for prime time," many consumers will be unmoved by popular appeals to go online, and many of those already online will be inhibited from engaging in transaction relationships. The problem is acute, with few easy solutions in sight. But if the difficult solutions are not attempted, society runs the risk of letting the revolutionary opportunities promised by the Internet slip away.

NOTES

1. Group-level data involve generalizations across groups of consumers and often involve inferring characteristics and behaviors from broad indicators such as geography and demographics, and usually necessitate making more as well as broader assumptions about consumers (Novak & Phelps, 1995).

2. Individual-specific information refers to data that pertain, or specifically relate, to a single identifiable person (Novak & Phelps, 1995).

3. We understand by *exchange* the transfer of something tangible or intangible, actual or symbolic, between two or more social actors (Bagozzi, 1975).

4. Trust exists when one party has confidence in an exchange partner's reliability and integrity (Morgan & Hunt, 1994).

5. We define *relationship commitment* as an exchange partner believing that an ongoing relationship with another is so important as to warrant maximum efforts at maintaining it (Morgan & Hunt, 1994).

REFERENCES

Andrews, Edmund L. 1998. European law aims to protect privacy of data. *New York Times* 26 October:A1.

- Bagozzi, Richard P. 1975. Marketing as exchange. *Journal of Marketing* 39(October):32-39.
- Blau, Peter. 1964. *Exchange and power in social life*. New York: John Wiley and Sons.
- Bloom, P., G. Milne, and R. Adler. 1994. Avoiding misuse of new information technologies: Legal and societal considerations. *Journal of Marketing* 58(1):98-110.
- Boston Consulting Group. 1997. eTRUST Internet privacy study. 24 March. [<http://www.truste.org/>]
- Business Week*. 1998. BW/Harris Poll: Online insecurity. Conducted by Louis Harris & Associates, Inc., and Alan F. Westin, 18-23 February, ed. Keith H. Hammonds. *Business Week*, 16 March. [<http://www.businessweek.com/1998/11/b3569107.htm>]
- Caruso, Denise. 1998. An online tug of war over consumers' personal information. *New York Times* 13 April:C5.
- Cavoukian, Ann, and Don Tapscott. 1996. *Who knows: Safeguarding your privacy in a networked world*. New York: McGraw-Hill.
- Center for Media Education. 1996a. CME's campaign to protect children from harmful cyber-advertising. *infoActive* 2(2). [<http://epn.org/cme/infoactive/22/22nweb.html>]
- Center for Media Education. (1996b). Invading children's privacy: Exhibit A. *infoActive*. 2(2). [<http://epn.org/cme/infoactive/22/22nweb.html>]
- Cespedes, F., and J. Smith 1993. Database marketing, new rules for policy and practice. *Sloan Management Review* (Summer):7-22.
- Choi, Soon-Yong, Dale O. Stahl, and Andrew B. Whinston. 1997. *The economics of electronic commerce*. New York: Macmillan Technical Publishing.
- Culnan, Mary J., and Pamela K. Armstrong. 1999. Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation. *Organization Science*. 10(1):104-115.
- Culnan, Mary J., and Sandra J. Milberg. In press. Consumer privacy. In *Information privacy: Looking forward, looking back*, eds. Mary J. Culnan, Robert J. Bies, and Michael B. Levy. Washington, DC: Georgetown University Press.
- Donaldson T., and T. Dunfee. 1994. Toward a unified conception of business ethics: Integrative social contract theory. *Academy of Management Review* 19(June):252-284.
- Driscoll, M., C. Roberts, E. Lyons, G. Jain, and J. Nuckols. 1997. Secure online payment systems. [http://mba.vanderbilt.edu/student/mba98/jeffrey.nuckols/secure_online_payment/secure_payments_frames.html]
- Dwyer, Robert F., Paul H. Schurr, and Sejo Oh. 1987. Developing buyer-seller relationships. *Journal of Marketing*. 51(April):11-27.
- Foxman, Ellen R., and P. Kilcoyne. 1993. Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing* 12(Spring):149-166.
- Froomkin, Michael. 1996a. Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases. *University of Pittsburgh Journal of Law and Commerce* 395. [<http://www.law.miami.edu/~froomkin/articles/ocean.html>]
- Froomkin, Michael. 1996b. The essential role of trusted third parties in electronic commerce. *Oregon Law Review* 75:49. [<http://www.law.miami.edu/~froomkin/articles/trusted.htm>]
- Garcia, Linda. 1997. Networked commerce: Public issues in a deregulated communication environment. *The Information Society* 13(1):17-31.
- Goodwin, Cathy. 1991. Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing* 12(Spring):106-119.

- Green, Heather. 1998. A little Net privacy, please. *Business Week*, 16 March: [<http://www.businessweek.com/1998/11/b3569104.htm>]
- Hearst, Marti. 1997. Distinguishing between Web data mining and information access. Presentation for the Panel on Web Data Mining KDD 97, Position Statement, 16 August, Newport Beach, CA. [<http://www.sims.berkeley.edu/~hearst/talks/data-mining-panel/index.htm>]
- Hoffman Donna L., and Thomas P. Novak. 1996. Marketing in hypermedia computer-mediated environments: Conceptual foundations. *Journal of Marketing* 60(3):50–68.
- Hoffman, D. L., and T. P. Novak. 1997a. A new marketing paradigm for electronic commerce. *The Information Society* 13(1):43–54.
- Hoffman, D. L., and T. P. Novak. 1997b. Privacy and electronic commerce. Handout prepared for EFF/Silicon Valley Industry Briefing with Ira Magaziner on “Global Electronic Commerce and Personal Privacy Protection,” 5 August.
- Hoffman, D. L., and T. P. Novak. 1998. Bridging the racial divide on the internet. *Science* 280(April 17):390–391.
- Hoffman, D. L., T. P. Novak, and P. Chatterjee. 1995. Commercial scenarios for the Web: opportunities and challenges. *Journal of Computer-Mediated Communication* (December) URL: <http://www.dscusc.org/jcmc/vol1/issue3/vol1no3.html>
- Hoffman, D. L., T. P. Novak, and M. Peralta. 1999. Building consumer trust in online environments: The case for information privacy. *Communications of the ACM*. 42(4):80–85.
- Houston F., and J. Gassenheimer. 1987. Marketing and exchange. *Journal of marketing* 51(October):3–18.
- Jupiter Communications. 1998. 1998 Online shopping report. 14 April. [<http://www.jup.com/>]
- Landesberg, Martha K., Toby Milgrom Levin, Caroline G. Curtin, and Ori Lev. 1998. *Privacy online: A report to Congress*. Federal Trade Commission, June. [<http://www.ftc.gov/reports/privacy3/toc.htm>]
- MacNeil, Ian R. 1980. *The new social contract: An inquiry into modern contractual relations*. New Haven, CT: Yale University Press.
- Marshall, Nancy. 1974. Dimensions of Privacy References. *Multivariate Behavioral Research* 9(July):252–271.
- Miller, Cyndee. 1995. Concern raised over privacy on Infohighway. *Marketing News* 29(1):1–11.
- Milne, George, and Mary E. Gordon. 1993. Direct mail privacy–efficiency trade-offs within an implied social contract framework. *Journal of Public Policy and Marketing* 12(Fall):206–216.
- Morgan, Robert M., and Shelby D. Hunt. 1994. The commitment-trust theory of relationship marketing. *Journal of Marketing* 58(July):20–39.
- Nielsen Media Research. 1997. Nielsen Media Research/CommerceNet Internet demographics study. Spring. [<http://www.nielsenmedia.com/commercenet/>]
- Novak G., and J. Phelps. 1995. Direct marketing and the use of individual-level consumer information: Determining how and when privacy matters. *Journal of Direct Marketing* 9(3):46–60.
- Peppers, Don, and Martha Rogers. 1997. *Enterprise one-to-one: Tools for competing in the interactive age*. New York: Currency/Doubleday.
- Pitkow, James, and Colleen Kehoe. 1997. GVU’s 7th WWW user survey. Georgia Tech Research Corporation, June. [http://www.gvu.gatech.edu/user_surveys/]
- Rayport, Jeffrey, and John Sviokla. 1994. Managing in the marketplace. *Harvard Business Review*, November–December:141–150.
- Swire, Peter P. 1997. Markets, self-regulation, and government enforcement in the protection of personal information. In *Privacy and self-regulation in the Information Age*, U.S. Department of Commerce. [http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm]
- U.S. Senate. 1998. S 2326. Children’s online privacy protection act of 1998 (Bryan). 105th Congress. 2d session. October 23. [<http://www.cdt.org/legislation/privacy/coppa.html>]
- Westin, Alan F. 1967. *Privacy and freedom*. New York: Atheneum.
- Wigand, Rolf. 1997. Electronic commerce: Definition, theory and context. *The Information Society* 13(1):1–16.