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

Building Con
Trust Online

How merchants can win back lost consumer trust in the interests of e-commerce sales.

Moving some Web consumers along to the purchase click is proving to be difficult, despite the impressive recent growth in online shopping. Consumer online shopping revenues and related corporate profits are still meager, though the industry is optimistic, thanks to bullish forecasts of cyberconsumer activity for the new millennium. In 1996, Internet shopping revenues for U.S. users, excluding cars and real estate, were estimated by Jupiter Communications, an e-commerce consulting firm in New York, at approximately $707 million but are expected to reach nearly $37.5 billion by 2002 [1]. Meanwhile, the business-to-business side is taking off with more than $8 billion in revenues for 1997 and $327 billion predicted by 2002 just in the U.S., according to Forrester Research, an information consulting firm in Cambridge, Mass. [4]. On the consumer side, a variety of barriers are invoked to explain the continuing difficulties.

There are, to be sure, numerous barriers. Such factors as the lack of standard technologies for secure payment, and the lack of profitable business models play important roles in the relative dearth of commercial activity by businesses and consumers on the Internet compared to what analysts expect in the near future. Granted, the commercial development of the Web is still in its infancy, so few expect these barriers to commercial development to persist. Still, commercial development of the Web faces a far more formidable barrier—consumers' fear of divulging their personal data—to its ultimate commercialization.

The reason more people have yet to shop online or even provide information to Web providers in exchange for access to information, is the fundamental lack of faith 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" involving money and personal information with them.

Our research reveals that this lack of trust arises from the fact that cyberconsumers feel they lack control over the access that Web merchants have to their

sumer

personal information during the online navigation process. These concerns over privacy span the dimensions of environmental control and secondary use of information control [6].

Environmental control, or the consumer's ability to control the actions of a Web vendor, directly affects consumer perception of the security of online shopping. In the physical world, a consumer may be concerned about giving out credit card information over the telephone to an unknown voice within a mail-order company. On the Web, consumers may fear typing in credit card information to any commercial Web provider. Similarly, a commercial Web provider may fear the efforts of a hacker intent on stealing credit card numbers.

Control over secondary use of information reflects consumers' perceived ability to control the use of their personal information for other purposes subsequent to the transaction during which the information is collected [2]. On the Web, this lack of trust is manifested in consumers' concern that Web providers will sell their personal information to third parties without their knowledge or permission.

Unlike traditional retail environments in the physical world, where consumers feel they have only limited choices, such perceptions concerning information privacy on the Internet have a striking negative influence on consumer willingness to engage in relationship exchanges online.

PETER HOEY

Consumer Privacy Perceptions

We investigated key consumer perceptions of privacy by analyzing consumer responses to two biannual surveys: the spring 1997 *Nielsen Media Research/CommerceNet Internet Demographics Study* [10] and the 1997 Georgia Tech Graphics, Visualization, and Usability Center's *GVU 7th WWW User Survey* [11].

The Nielsen study is representative of the U.S. as a whole, so the sample we examined (1,555 Web users) projects to the approximately 45 million Web users ages 16 and over in the U.S. at the time of the survey. The GVU survey is based on a self-selected sample of respondents to a Web-based form and tends to represent more experienced Web users from around the world. It is not representative or projectable to the larger Web user population, but the large sample size we analyzed (14,014 Web users) provides important insight into many Web users' attitudes toward privacy.

Analyzing the GVU data, we found that consumer expectations of privacy depend on the medium. In traditional media, it is well known that consumer attitudes toward privacy invasion range from tolerance to resigned disgust. But in electronic media, consumers are making it clear their need for control and protection is intense. A whopping 87% of Web users think they should have complete control over the demographic information Web sites capture, and over 71% feel there should be new laws to protect their privacy online.

While almost 20% of Web users in the survey (international in scope, though most respondents were from the U.S.) say magazines have a right to sell their demographic data to other firms for direct-marketing purposes, only 12% say Web sites and third-party agencies have the same right. Similarly, almost 21% of Web users like receiving direct mail solicitations, but only 6% of Web users want to receive junk email.

The behavior of today's commercial Web providers is responsible for these attitudes. Many cybermarketers lack faith in consumers, thinking that if they ask consumers to opt in, most will opt out. Some cybermarketers treat online consumers poorly, in ways that bring to mind the practices of unscrupulous direct marketers in the physical world. Our analysis revealed that the primary barriers to consumers' providing demographic data to Web sites are related to trust and the nature of the exchange relationship. Nearly 63% of consumers who decline to provide personal information to Web sites report it is because they do not trust those who are collecting the data. Moreover, 65% report that providing such information is not worth the risk of revealing it, and 69% of Web users who do not provide data to Web sites say it is because the sites provide no information on how the data will be used.

The strength of these responses is hardly surprising, considering that 86% of commercial Web sites provide no information of any kind on how any demographic data collected will be used, or even whether data is being collected [9]. Consumers respond accordingly, either by withholding their personal data or by providing false data. Almost 95% of Web users have declined to provide personal information to Web sites at one time or another when asked, and 40% who have provided demographic data have gone to the trouble of fabricating it.

Despite this consumer resistance, our research suggests that consumers do realize that personal data is important to Web marketers and, perhaps surprisingly, report being interested in providing such information. Would it shock many marketers to know that almost all Web users (92%) would, in principle, give demographic data to Web sites? And that most consumers (over 62%) also understand that Web sites need information about their visitors to market their sites to advertisers.

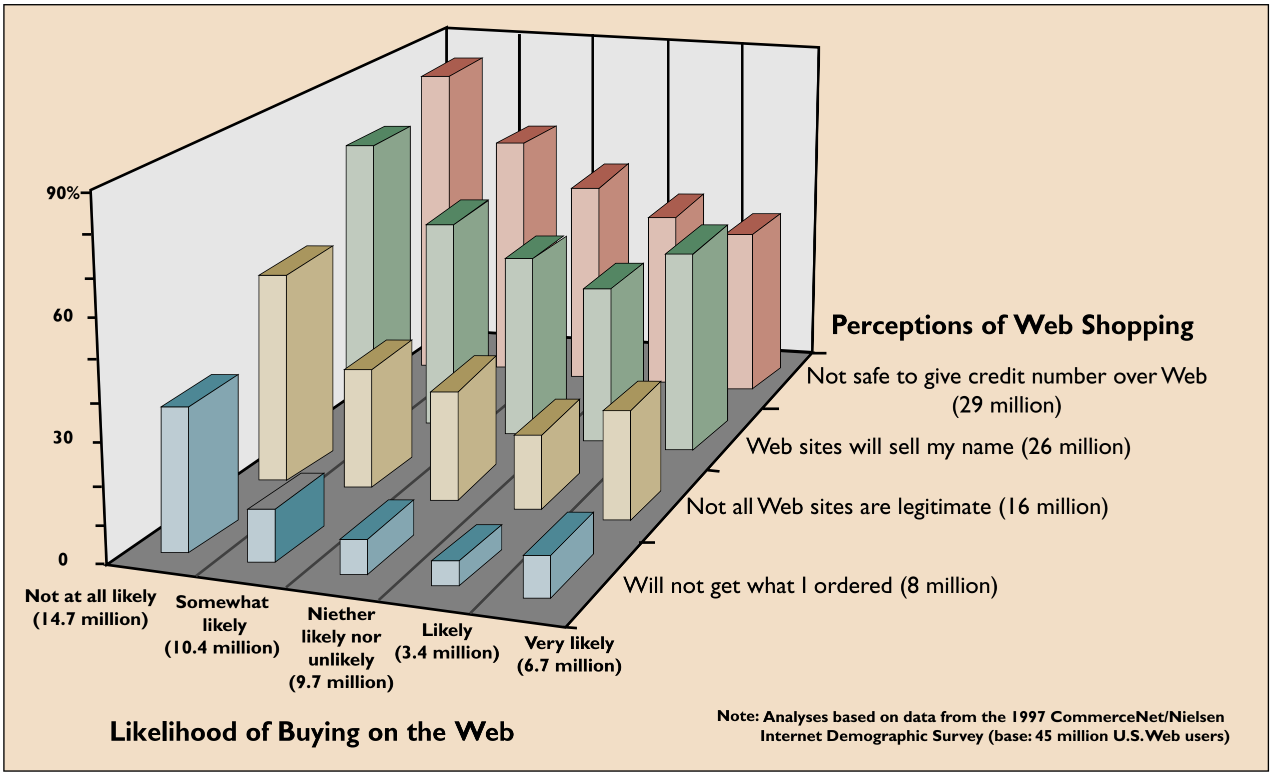
But commercial Web sites are their own worst enemies. Contrary to the conventional wisdom, the enabling conditions for giving up information are not product discounts, access to the site, or value-added services. Indeed, 67%–75% of all Web users are decidedly uninterested in selling their personal data to Web sites for financial incentives or access privileges. In other words, consumers do not view their personal data in the context of an economic exchange of information, as many commercial Web providers believe.

Instead, Web consumers report wanting another type of exchange—characterized by an explicit social contract executed in the context of a cooperative relationship built on trust. The enabling condition for providing personal data is clear: Over 72% of Web users said they would give Web sites their demographic information if the sites would only provide a statement regarding how the information collected would be used.

But while consumers clamor for full disclosure and informed consent, the few Web sites that do tell their visitors they are tracking them and recording their data follow the traditional opt-out model. The default position of even the best opt-out policy is that unless the Web site is otherwise informed, it is free to use consumers' data in any (presumably legal) way it sees fit. Opt-out information privacy policies thus place the entire information-protection burden on the consumer while offering none of the control and setting up an environment of ipso facto mistrust between Web provider and consumer.

Although questionable security is a major deterrent to online shopping, concerns regarding the secondary use of information loom large, discouraging consumers from engaging in online relationship exchanges. Control over secondary use of information is likely to be a sticking point. Over 80% of

ALMOST 95% OF WEB USERS HAVE DECLINED TO PROVIDE PERSONAL INFORMATION TO WEB SITES AT ONE TIME OR ANOTHER WHEN ASKED.



Note: Analyses based on data from the 1997 CommerceNet/Nielsen Internet Demographic Survey (base: 45 million U.S. Web users)

Figure 1. How consumer attitudes influence intent to buy on the Web.

Web consumers simply do not want Web sites to resell their personal information to other businesses.

Consumer Attitudes and Cyber Behavior

The Internet threatens consumer information privacy in new and extreme ways. Unlike the case with consumer behavior in the physical world (When was the last time a consumer refused to shop for groceries over privacy invasion fears?), this threat has pushed many consumers to opt out of various forms of commercial participation in the Internet, including providing personal information to Web sites for marketing purposes.

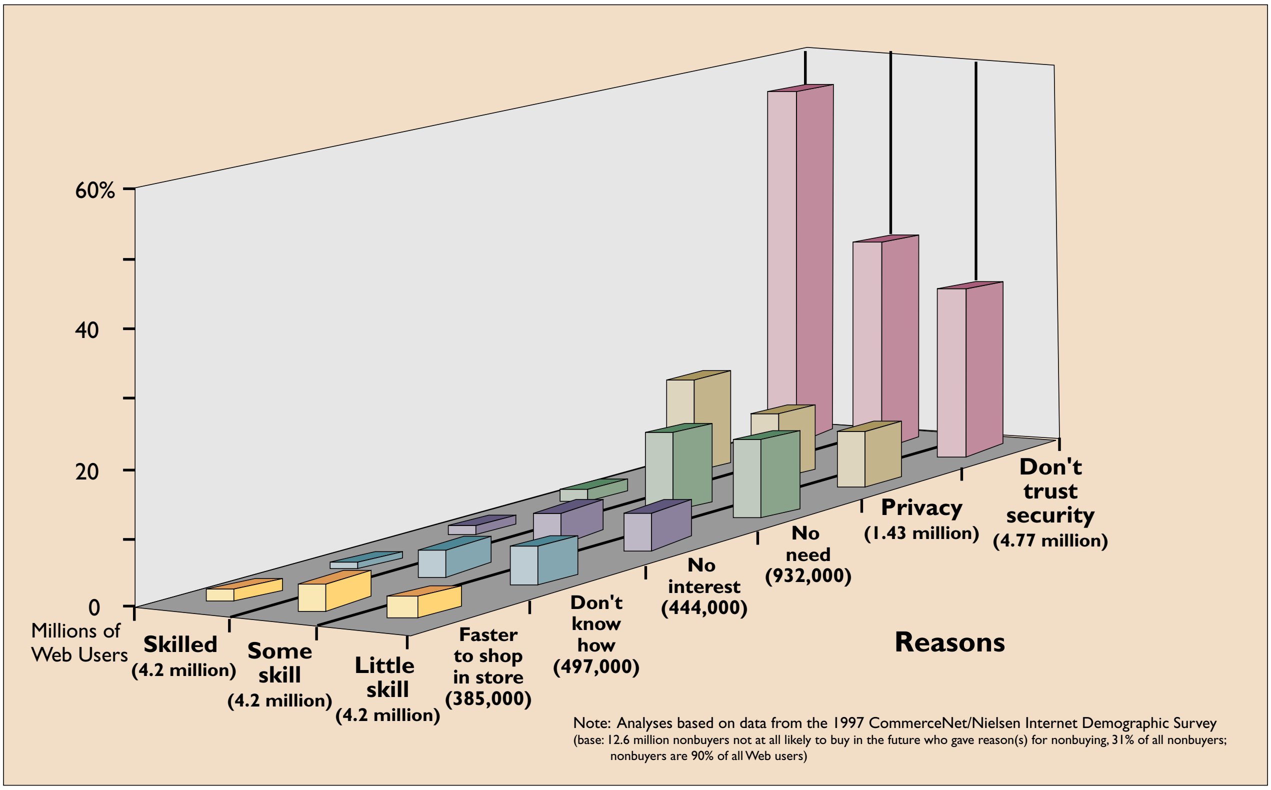
The security issues raised by environmental control are shared by commercial Web providers and consumers. In contrast, the secondary use of information is a source of conflict between commercial Web providers and consumers. Although this conflict also exists in the physical world, the issue takes on greater urgency online, owing to the special characteristics of the Internet.

Data mining and data warehousing opportunities are being exploited as never before due to the capabilities of the Internet, high-speed networks, and terabyte data storage. In contrast, consumer information in the physical world is stored in a much wider variety of databases and data formats and is much more difficult to combine, analyze, and access.

Online shopping potentially allows commercial Web providers to collect much more detailed consumer behavior information than they can from most physical shopping trips. Commercial Web providers can collect not only the same information available in most physical transactions—identity, credit history, employment status, legal status—but also such additional information as electronic address, specific history of goods and services searched for and requested, other Internet sites visited, and contents of the consumer's data storage device.

Finally, with the notable exception of single-source data, such as supermarket scanner data, most secondary uses of information in the physical world have been limited to aggregate data involving generalizations across groups of consumers or inferences and assumptions about behavior based on broad indicators, such as geography or demographics.

Secondary use of information captured online can more easily follow individual-level behavior. Highly touted by many Internet marketers is the idea that data specifically linked to a single identifiable person can be used to customize a product or service to a potential customer, in the interest of maximizing the likelihood of consumer acceptance of the offer.



Note: Analyses based on data from the 1997 CommerceNet/Nielsen Internet Demographic Survey (base: 12.6 million nonbuyers not at all likely to buy in the future who gave reason(s) for nonbuying, 31% of all nonbuyers; nonbuyers are 90% of all Web users)

Figure 2. How consumers' online skills influence the reasons they don't buy on the Web.

Despite the growing consumer awareness of the potential for such customization, the practice generally proceeds without explicit consumer permission or knowledge.

It should come as no surprise that most consumers therefore avoid engaging in relationship exchanges online. In 1997, although more than 45 million individuals age 16 and over had used the Web in the U.S. at least once, only 4.5 million, or 10%, had ever purchased a product or service on the Web [8]. It is also worth noting, for the sake of perspective, that almost 123 million people, or nearly 62% of the U.S. 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.

Figure 1 shows that Web consumers' top online-shopping concerns are related to control over information privacy and to trust, as opposed to the operating risks of remote shopping, and that these concerns influence their stated likelihood of buying something. In light of increasing security concerns, the likelihood of buying online decreases.

The same is true for secondary use of information control and trust, except that these concerns are most pronounced for both those Web users most likely and those least likely to shop online.

Figure 2 shows the relationship between the degree of online experience (closely correlated with and described by us here as "skill") and the reasons for not shopping online. We considered only Web users who have never shopped online and never plan to. Overall, the most important reasons nonbuyers uninterested in online shopping give for not shopping online are not functional but are related to issues of control over their personal information.

It is dramatically apparent that negative perceptions regarding security and privacy *increase* along with levels of online proficiency. The reverse is true for the functional reasons Web users do not shop online, including no perceived need, no interest, no knowledge of how to shop online, and the belief that it is faster to shop in stores made of bricks and mortar. In essence, the more experience one acquires online, the less important are the functional barriers to online shopping and the more important are concerns of control over personal information.

Commercial Development of the Web (Short- vs. Long-Term)

Each stage of the online purchasing process involves dissimilar and conflicting interests for consumers and commercial Web providers [3]. During the search stage, for example, the Web provider wants to glean consumer information—the better to build a database of customer navigation and eventual purchase profiles. And the consumer wants to minimize the amount of personal information disclosed while maximizing the amount of information obtained about the product.

In the near term, this conflict of interest cannot be easily resolved, but we can address it by giving consumers the opportunity to be anonymous or pseudonymous when engaging in information exchanges and online transactions. Traceable anonymity gives Web providers no clues about consumers' identities but leaves this information in the hands of a third party. Traceable pseudonymity attaches a nom de plume, or pseudo-identity, that can be traced back to the consumer by someone, not necessarily the Web provider [5]. These functions can be ensured through the use of pseudonymous and third parties acting as mediators. At the same time, consumer anonymity or pseudonymity has to allow Web providers to receive the minimum information necessary—but only the minimum—to complete the exchange; for example, authentication, certification, confirmation, payment, and nonrepudiation in the case of an online transaction.

This short-term solution is appealing because it is likely to stimulate consumers' commercial online transactions by preserving their information privacy. It has the added attraction of opening the door to a long-term solution.

Ultimately, the most effective way for commercial Web providers to develop profitable exchange relationships with online customers is to earn their trust. The way to achieve trust is simple, though it departs radically from traditional business practice and will be difficult for many companies to implement. Trust is best achieved by allowing the balance of power to shift toward a more cooperative interaction between an online business and its customers [7].

Recognizing consumers' rights to data ownership on the Internet is an important first step in this rebalancing process. At a minimum, it means market-driven industry acceptance and enforcement of opt-out policies regarding information exchange. Eventually, the industry should accede to consumer demand and move toward opt-in, informed-consent policies in computer-mediated environments. However, it is likely that U.S. federal regulatory effort will be required.

A more consumer-oriented information privacy model will lead to commercially valuable relationship exchanges with important benefits for consumers and companies doing business on the Internet [12]. Consumers will be in control of their personal information—a notion consistent with customization of customer needs in online environments. Companies will be rewarded with consumer trust, willingness to disclose personal information, and increased loyalty. Moreover, as with open standards in computing and networking technology, cooperative models promote the healthy development of the electronic marketplace.

References

1. Achs, N. *1998 Online Shopping Report: Strategies for Driving Consumer Transactions*. Jupiter Communications, Digital Commerce Group, New York, 1997 (www.jup.com).
2. Culman, M. Consumer awareness of name removal procedures: Implications for direct marketing. *J. Dir. Mark. 9,* 2 (Spring 1995), 10-19.
3. Driscoll, M., Roberts, C., Lyons, E., Jain, G., and Nuckols, J. *Secure Online Payment Systems.* Owen Electronic Commerce Student Working Paper, 1997 (mba.vanderbilt.edu/student/mba98/ jeffrey.nuckols/ secure_online_payment/secure_payments_frames.html).
4. Erwin, B., Modahl, M., and Johnson, J. Sizing intercompany commerce: Business trade and technology strategies. *The Forrester Report 1,* 1 (July 1997) (www.forrester.com).
5. Froomkin, M. Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases. *Univ. Pittsburgh J. Law and Commer. 395,* 15 (1996) (www.law.miami.edu/~froomkin/ articles/ocean.htm).
6. Goodwin, C. Privacy: Recognition of a consumer right. *J. Public Policy Mark. 10,* 1 (spring 1991), 106–119.
7. Hoffman, D., and Novak, T. A new marketing paradigm for electronic commerce. *Inf. Soc.: An Int. J. 13,* 1 (1997), 43–54.
8. Hoffman, D., and Novak, T. *Privacy and electronic commerce.* Handout prepared for Electronic Frontier Foundation/Silicon Valley Industry Briefing with Ira Magaziner on Global Electronic Commerce and Personal Privacy Protection (Aug. 5, 1997).
9. Landesberg, M., Levin, T., Curtin, C., and Lev, O. *Privacy Online: A Report to Congress.* Federal Trade Commission, June 1998 (www.ftc.gov).
10. Nielsen Media Research. *Nielsen Media Research/CommerceNet Internet Demographics Study.* Spring, 1997 (www.nielsenmedia.com/commercenet/).
11. Pitkow, J., and Kehoe, C. *7th WWW User Survey.* Georgia Tech Research Corp., June 1997 (www.gvu.gatech. edu/user_surveys/).
12. Wang, H., Lee, M., and Wang, C. Consumer privacy concerns about Internet marketing. *Commun. ACM 41,* 3 (Mar. 1998), 63–70.

Donna L. Hoffman (donna.hoffman@vanderbilt.edu) is an associate professor of marketing and codirector of Project 2000 (www2000.ogsm.vanderbilt.edu/) at the Owen Graduate School of Management, Vanderbilt University, Nashville, Tenn.

Thomas P. Novak (tom.novak@vanderbilt.edu) is an associate professor of marketing and codirector of Project 2000 (www2000.ogsm.vanderbilt.edu/) at the Owen Graduate School of Management, Vanderbilt University, Nashville, Tenn.

Marcos Peralta (marcos.peralta@owen.vanderbilt.edu) is an M.B.A. student at the Owen Graduate School of Management, Vanderbilt University, Nashville, Tenn.