"Building Consumer Trust in Online Environments: The Case for Information Privacy"

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

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

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

Marcos Peralta (marcos.peralta@owen.vanderbilt.edu) is a second-year Electronic Commerce M.B.A. student at the Owen Graduate School of Management, Vanderbilt University.

Moving Web consumers along to the "purchase click" is proving to be difficult. Current consumer online shopping revenues are meager, though the industry is optimistic, thanks to bullish forecasts of cyberconsumer activity for the new millennium. In 1996, Internet shopping revenues for United States users, excluding cars and real estate, were estimated at approximately $707 million, but are expected to hit nearly $37.5 billion by 2002 [1]. Meanwhile, the business-to-business side is taking off with over $8 billion logged in revenues for 1997 and $327 billion predicted by 2002, for the United States alone [2]. On the consumer side, a variety of barriers are invoked to explain the difficulties.

To be sure, numerous barriers *do* exist. Oft-cited factors like too few online consumers interested in the few available online offerings, no standardized technologies for secure payment mechanisms, and the lack of profitable business models play important roles in the relative dearth of commercial activity among businesses and consumers on the Internet. Granted, the commercial development of the Web is still in its infancy, so few expect these very real barriers to continued commercial development to persist forever. Yet, the successful commercial development of the Web faces a far more formidable barrier to ultimate commercialization.

At its core, the reason online consumers have yet to shop online in large numbers, or even provide information to Web providers in exchange for access to information offered onsite, 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.

Our research reveals that this lack of trust arises from cyberconsumers' perceived lack of control over the access others have to their personal information during the online navigation process. These concerns of control over information privacy span the dimensions of *environmental control* and *secondary use of information control* [3].

Environmental control directly affects consumers' perceptions 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 mail-order company. On the Web, a consumer may fear typing in her 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 reflects the consumer's perceived ability to control the use of personal information for other purposes, subsequent to the transaction during which the information was originally collected [4]. On the Web, this is manifested by consumers' concern that Web providers are selling their personal information to third parties without their knowledge or permission.

Unlike traditional retail environments in the physical world where consumers perceive little choice, these perceptions of little control over information privacy on the Internet have a striking influence on consumer willingness to engage in relationship exchanges online.

Key Consumer Perceptions of Privacy

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 [5] and the 1997 GVU 7th WWW User Survey [6]. The Nielsen study is representative of the United States as a whole so the sample of 1,555 Web users we examined projects to the approximately 45 million Web users 16 and over in the United States.

The GVU survey is based on a self-selected sample of respondents to a Web fill-out form and tends to represent more experienced Web users from all over the globe. It is not representative or population projectable, but the large sample size of 14,014 Web users we analyzed provides important insight into many Web users' attitudes toward privacy. We summarize our findings from our analysis of the GVU data first.

We found, first, that consumer expectations of privacy depend on the medium. In traditional media, it is well known that consumer attitudes toward privacy invasions range from tolerance to resigned disgust. But in electronic media, consumers are making it clear that 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% believe there should be new laws to protect their privacy online.

While almost one-fifth of Web users believe that magazines have a right to sell their demographic data to other firms for direct marketing purposes, only 12% think that Web sites and third-party agencies have the same right. Similarly, almost 21% of Web users like receiving junk mail, but only a mere 6% of Web users want to receive electronic junk mail.

Current commercial Web provider behavior 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 consumers poorly online, 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 relate to trust and the nature of the exchange relationship. Nearly 63 percent of consumers who decline to provide personal information to Web sites report that it is because they do not trust who is collecting the data. Sixty-five percent additionally report that providing such information is not worth the risk of revealing it and 69 percent of Web users that 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 eighty-six percent of commercial Web sites provide no information of any kind regarding how any demographic data collected will be used, or even if data *are* being collected [7]. Consumers respond accordingly, either by withholding their personal data and/or providing false data. Fully 94 percent of Web users have declined to provide personal information to Web sites at one time or another when asked and 40 percent who have provided demographic data have gone to the trouble of fabricating it.

Despite this, our research suggests that consumers *do* realize that personal data are 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 percent) would, in principle, give demographic data to Web sites? Further, most consumers (over 62 percent) also understand that Web sites need information about their visitors in order 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, fully two-thirds to three-quarters of all Web users are decidedly uninterested in selling their personal data to Web sites for monetary 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, we found that Web consumers report wanting another type of exchange; one 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 percent of Web users said they would give Web sites their demographic information if the Web sites would only provide a statement regarding how the information collected was to 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 policies is that unless the Web site is otherwise informed, it is free to use the consumer’s data in any (presumably legal) way it sees fit. Opt-out information privacy policies thus place the entire information protection burden on the consumer, offer none of the control, and set up an environment of ipso facto mistrust between the Web provider and the consumer.

Although security concerns are a major deterrent to online shopping, concerns regarding the secondary use of information loom large and also discourage consumers from engaging in online relationship exchanges. Secondary use of information control is likely to be a sticking point. Eighty-one percent of Web consumers do not want Web sites to resell personal information to other businesses.

Consumer Attitudes Affect Cyber-Behavior

The Internet threatens consumer information privacy in new and extreme ways. In contrast to consumer behavior in the physical world (after all, when was the last time a consumer refused to shop for groceries because of 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 concerns between 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 is also true in the physical world, the issue takes on a greater urgency online, owing to the unique characteristics of the Internet medium.

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.

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 physical world transactions - identity data, credit history, employment data and public record information - but also additional information such as electronic address, specific history of goods and services searched for and requested, other Internet sites visited by the consumer, and contents of the consumer’s data storage device.

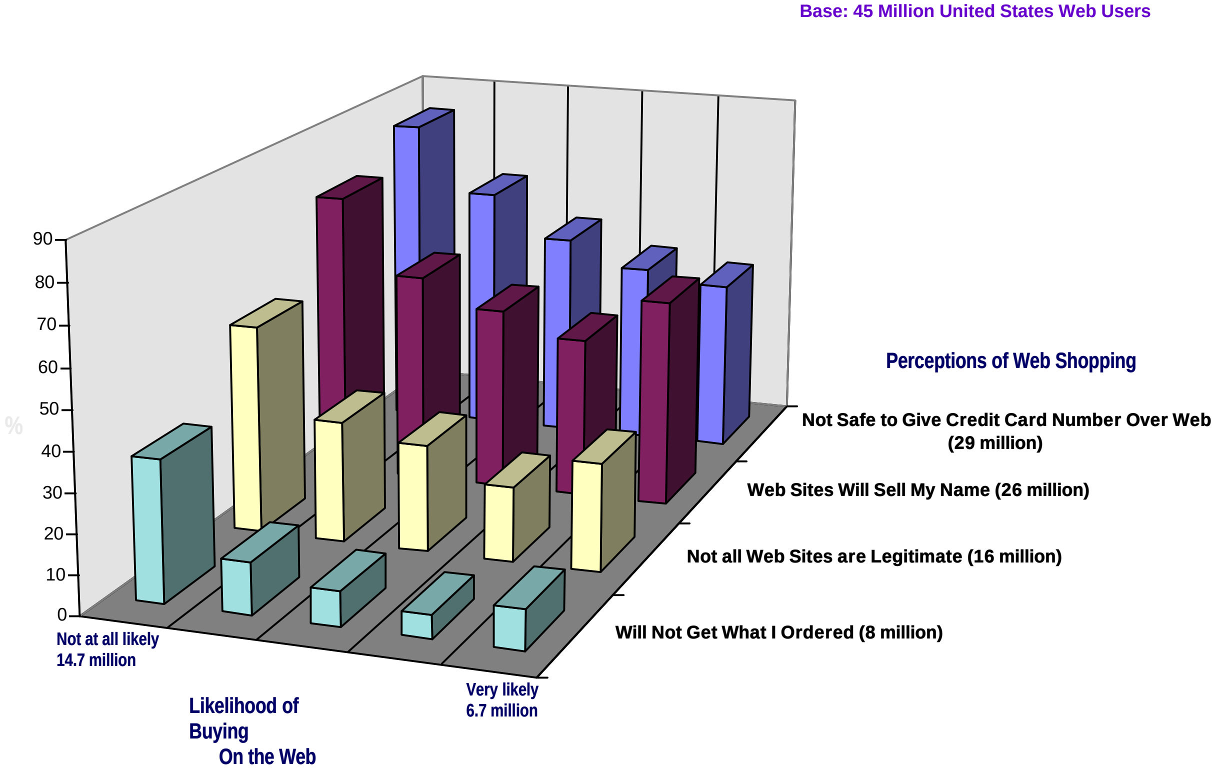
Finally, except for the notable exception of single-source data like supermarket scanner data, most secondary uses of information in the physical world have been limited to aggregate data, involving generalizations across groups of consumers, or inferences and assumptions about behavior based on broad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

Secondary use of information captured online can more easily take advantage of individual-level information. Highly touted is the idea that data specifically linked to a single identifiable person can be used to customize an offer to a potential customer, in the interest of maximizing the likelihood of consumer acceptance of the offer. Despite the growing consumer awareness that the potential for such customization exists, the practice generally proceeds without explicit consumer permission of exactly when it is being done, by whom, and for what purpose.

It should come as no surprise, then, that most consumers currently avoid engaging in relationship exchanges online. In 1997, although over 45 million individuals 16 and over had used the Web in the United States at least once, only 4.5 million or 10 percent 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 percent 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.

Exhibit 1

Attitudes Impact Consumer Intent to Buy On the Web



Analyses based on data from the 1997 CommerceNet/Nielsen Internet Demographic Survey

As Exhibit 1 shows, Web consumers’ top online shopping concerns relate to control over information privacy and trust, as opposed to the operating risks of remote shopping, and these concerns impact consumers’ stated purchase likelihoods. As security concerns (environmental control) rise, the likelihood of purchasing online decreases.

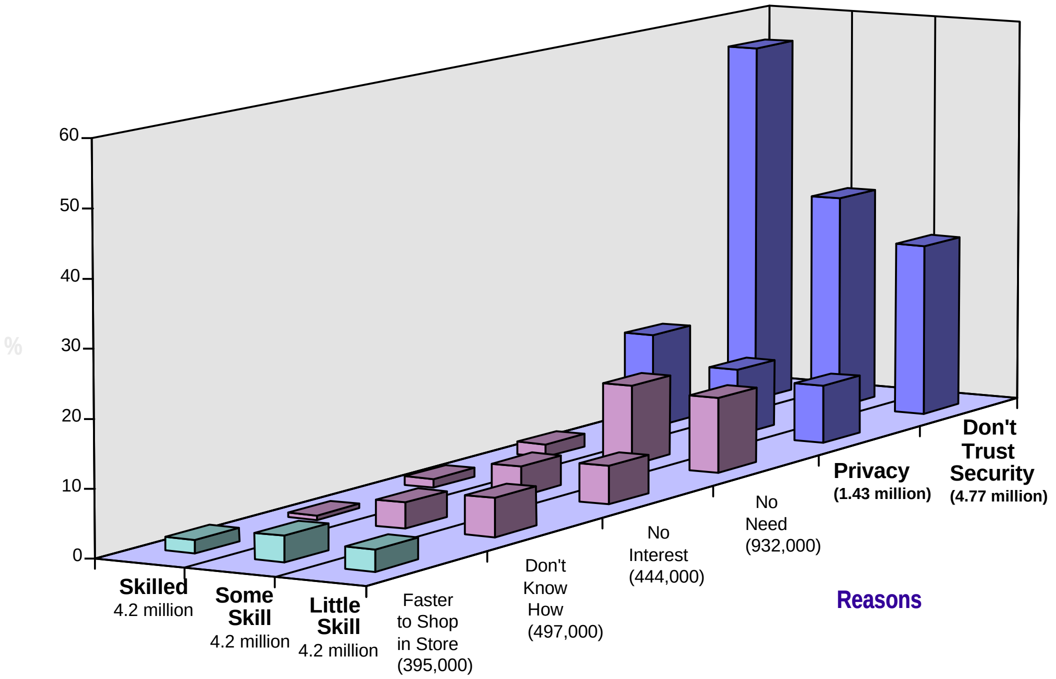
The same is true for secondary use of information control and trust, except that concerns are most pronounced for those *both most and least likely to shop online*.

Exhibit 2

Skill Interacts with the Reasons Consumers Do Not Buy On the Web

Base: 12.6 million Nonbuyers *Not At All* Likely to Buy in the Future
Who Gave Reason(s) for Nonbuying
(31% of all Nonbuyers)

N.B. Nonbuyers are 90% of all Web Users



Analyses based on data from the 1997 CommerceNet/Nielsen Internet Demographic Survey

In Exhibit 2, we examine the relationship between online experience, closely correlated with and reported here as skill, and the reasons for not shopping online. We examine only that combination of 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 related to issues of control over personal information.

It is dramatically apparent that negative perceptions regarding security and privacy *increase* with increasing 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 physical stores. 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.

The Commercial Development of the Web in the Short-Run

Each stage of the online purchase process presents consumers and commercial Web providers with dissimilar and conflicting interests [9]. During the search stage, for example, the Web provider wishes to glean consumer information, the better to build a database of customer navigation and eventual purchase profiles, while the consumer wishes 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 easily be solved, but in the short run we can address it by giving consumers the opportunity to be *anonymous* and/or *pseudonymous* when engaging in information exchanges and online transactions. Traceable anonymity gives the Web providers no clues about the consumer's identity, but leaves this information in the hands of a third party. Traceable pseudonymity attaches a *nom de plume*, which can be traced back to the consumer (by someone), although not necessarily by the Web provider [10]. These functions can be ensured through the use of pseudonymous and third parties acting as mediators. At the same time, consumer anonymity or pseudonymity must allow Web providers to receive the minimum information necessary, and only the *minimum* necessary, in order to complete the exchange; for example, authentication, certification, confirmation, payment, and non-repudiation in the case of an online transaction.

The short-term solution is appealing because it is likely to stimulate commercial online transactions among consumers that preserve their information privacy. It has the added attraction of opening the door to a long-term solution.

The Commercial Development of the Web in the Long-Run

Ultimately, *the most effective way for commercial Web providers to develop profitable exchange relationships with online customers is to earn consumer trust.* The mechanism for achieving trust is simple, though it departs radically from traditional business practice and will be difficult for many firms to implement. Trust will be best achieved by allowing the balance of power to shift toward a more cooperative interaction between the online business and its customers [11].

Recognizing consumers’ rights to data ownership on the Internet is an important first step in this re-balancing process. At a minimum, this means market-driven industry acceptance and enforcement of *stated* 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. It is likely that regulatory effort may be required.

A more consumer-oriented information privacy model will lead to commercially valuable exchange relationships with important benefits for consumers and firms doing business on the

Internet [12]. Consumers will be in control of their personal information - a notion consistent with the customization of customer needs in online environments. Firms will be rewarded with consumer trust, the willingness to disclose, and greater levels of loyalty. Finally, as with open standards, cooperative models promote the healthy development of the electronic marketplace.

References

1. Achs, Nicole R. "1998 Online Shopping Report: Strategies for Driving Consumer Transactions," Jupiter Communications, Digital Commerce Group, http://www.jup.com. (November 1997).

2. Erwin, Blane, Modahl, Mary, and Johnson, Jessee. "Sizing Intercompany Commerce: Business Trade & Technology Strategies," The Forrester Report, Forrester Research Inc., Volume One, Number One, July 1997.http://www.forrester.com/

3. Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right", *Journal of Public Policy & Marketing* 12 (Spring), 106-119.

4. Culman, Mary J. (1995), "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing* 9 (2) (Spring), 10-19.

5. Nielsen Media Research (1997), "Nielsen Media Research/CommerceNet Internet Demographics Study," Spring. [http://www.nielsenmedia.com/commercenet/]

6. Pitkow, James and Colleen Kehoe (1997), "GVU's 7th WWW User Survey," Georgia Tech Research Corporation, June.[http:// www.gvu.gatech.edu/user_surveys/]

7. Landesberg, Martha K., Levin, Toby Milgrom, Curtin, Caroline G., and Ori Lev. Privacy Online: A Report to Congress, Federal Trade Commission, June 1998. Www.ftc.gov

8. 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," August 5, 1997.

9. Driscoll, M., C. Roberts, E. Lyons, G. Jain, and J. Nuckols (1997), "Secure Online Payment Systems." Owen Electronic Commerce Student Working Paper [URL:http://mba.vanderbilt.edu/student/mba98/jeffrey.nuckols/secure_ online_ payment/secure_payments_frames.html]

10. Froomkin, Michael (1996a), "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases", *University of Pittsburg Journal of Law and Commerce* 395. [URL: http://www.law.miami.edu/~froomkin/articles/ ocean.html].

11. Hoffman, D.L. and Novak, T.P. (1997a), "A New Marketing Paradigm for Electronic Commerce," *The Information Society: An International Journal*, 13(1), 43-54.

12. Wang, Huaiqing, Lee, Matthew K.O., and Wang, Chen. "Consumer Privacy Concerns About Internet Marketing," Communications of the ACM, March 1998, Volume 41, Number 3, 63-70.