3-1-2003

Tit for Tat in Cyberspace: Consumer and Website Responses to Anarchy in the Market for Personal Information

David L. Baumer
Julia Brande Earp
Pamela S. Evers

Follow this and additional works at: http://scholarship.law.unc.edu/ncjolt

Part of the Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncjolt/vol4/iss2/1
Article: Tit for Tat in Cyberspace: Consumer and Website Responses to Anarchy in the Market for Personal Information

David L. Baumer, Julia Brande Earp, and Pamela S. Evers

I. Introduction

Although the Internet has opened up new opportunities for both businesses and consumers, it also has made possible a tremendous expansion in the market for personal information that many regard as unfortunate and threatening. The computerization of information has made collecting, storing, processing, and transmitting information vastly cheaper. Since lower prices tend

---

1 David L. Baumer is an Associate Professor of Law and Technology at the College of Management, North Carolina State University ("NCSU"). He received a B.A. in Economics from Ohio University, J.D. from the University of Miami and a Ph.D. in Economics from the University of Virginia. Baumer is a licensed attorney in the State of North Carolina. He is the Director of the Cyberlaw Initiative at NCSU. Julia Earp is an Assistant Professor at the College of Management, North Carolina State University. She received her M.S. in statistics and Ph.D. in information technology from Virginia Polytechnic Institute and State University. Pamela S. Evers is an Attorney and Assistant Professor of Business Law, Cameron School of Business, University of North Carolina at Wilmington. Evers received an MBA, JD, and LLM, respectively, from Emory University, Southern Methodist University, and Northwestern School of Law at Lewis & Clark College. The authors wish to thank Blue Cross Blue Shield of North Carolina for providing a link from their website for the administration of the survey developed for this article.

2 The degree of concern among consumers about privacy in cyberspace is the focus of this paper. Protecting privacy in cyberspace is of such concern that lawmakers have responded by passing a number of laws, see text and notes infra, aimed at protecting privacy, academics have written extensively about the topic (a word search of "Internet Privacy" covering the last five years yielded 223 hits using Lexis-Nexis), and a cottage industry of websites has emerged that is devoted to chronicling battles on the privacy front, see, e.g., the Electronic Frontier Foundation, at http://www.eff.org.

3 Pamela Samuelson, Cyberspace and Privacy: A New Legal Paradigm? Privacy as Intellectual Property?, 52 STAN. L. REV. 1125, 1126 (2000); see also Jerry Kang, Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193, 1198–99 (1998). Kang contrasts the amount of data that is collected from
to provide greater access, it should be no surprise that several recent polls have confirmed that most people are very concerned that the Internet has facilitated a significant loss of privacy. Indeed, Internet privacy is a large and burgeoning topic that continues to change with each technological advance.

This paper focuses on voluntary transfers of personal information by consumers to websites and the measures that websites can take to alleviate consumer concerns about privacy. Admittedly, voluntary transfers are only part of the larger issue of Internet privacy, but consumer and website responses to questions about voluntary transfers reveal a great deal about an uncertain legal landscape for the protection of privacy. The survey

---

a hypothetical trip to a suburban mall with the amount collected from a visit in cyberspace to a virtual mall. Kang effectively points out that unless a person uses a credit card to make a purchase at the local mall, the visit is virtually anonymous and unrecorded. In contrast, almost everything about browsing through a cyber-mall can be recorded in minute detail, including websites visited, numbers of minutes spent at each website, and so on.


5 See supra note 2.

6 The paper does not analyze involuntary acquisitions of information such as those that occur when a website attaches a cookie to a web browser of a web visitor, even though involuntary acquisitions of information online pose a tremendous threat to privacy. See Kang, supra note 3, at 1198–99; see also A.
developed for this article at the website of a healthcare provider and through a server provided by North Carolina State University investigated how consumers and websites react when property rights to online personal information are ambiguous.\textsuperscript{7} The entire survey is available in the Appendix.\textsuperscript{8}

The survey had several objectives. First, it investigated the willingness of consumers to reveal personal information online to websites. The survey asked consumers to react to statements that dealt with various types of information, from demographic to very personal, such as social security numbers, credit card numbers, and medical records.\textsuperscript{9} Second, survey respondents were asked about their views of the efficacy of various measures that websites could take to allay consumer fears of the consequences of violations of privacy. Consumers were asked, for example, whether they would be more willing to reveal information to websites that had "opt out" policies for information collected from consumers and third party monitors of adherence to their own privacy policies. Third, respondents were asked about possible adverse consequences due to misuse of personal information acquired online. Finally, the survey asked what measures (e.g., game participation, discounts for online purchases, targeted mailings) websites could take to persuade consumers to reveal more information.

The survey instrument employed to investigate these issues was an online survey.\textsuperscript{10} Respondents were asked online what

\begin{itemize}
\item Michael Froomkin, \textit{The Death of Privacy?}, 52 STAN. L. REV. 1461, 1468 (2000) (discussing "privacy-destroying technologies" used in involuntary information acquisition). Froomkin usefully divides privacy-destroying technologies between those used to acquire raw data and those used to process and collate data.
\item Put differently, the survey investigated how people react on the Internet by questioning them while they were using the Internet, rather than by intercepting people at a local shopping mall and asking them what information they would provide to websites.
\item The survey was developed by Julia Brande Earp.
\item The complete list of the categories of information is listed in the Appendix.
\item The URL for one part of the survey was http://www.theprivacyplace.org/publications.html (last updated Nov. 30, 2002) (on file with the North Carolina Journal of Law & Technology). The website of Blue Cross Blue Shield of North Carolina, http://www.bcbsnc.com
\end{itemize}
information about themselves they would reveal in a realistic setting using actual screen captures, or actual screen displays, from well-known and less well-known websites. The survey developed for this article assumed that the use of an online survey with actual screen captures would be far more accurate than intercepting shoppers at a shopping mall and asking them to use pencil and paper to record what they would be willing to reveal to a website.\footnote{Authors of this article have had several previous surveys published in academic journals. \textit{E.g.}, David L. Baumer and Patricia Marschall, \textit{Willful Breaches of Contract: Can the Bane of Business Be an Economic Bonanza?}, 65 \text{TEMP. L. REV.} 159 (1992) (discussing the results of a survey of over 200 businesspeople). For discussion of other survey results, see David L. Baumer and Julia Brande Earp, \textit{Innovative Web Use to Learn about Consumer Behavior and Online Privacy}, \textit{COMMUNICATIONS OF THE ACM}, (forthcoming) (manuscript on file with authors); David L. Baumer, Julia Brande Earp, and Fay Cobb Payton, \textit{Privacy of Medical Records: IT Implications of HIPPA}, 30(4) \textit{COMMUNICATIONS OF ACM — COMPUTERS AND SOCIETY} 40 (Dec. 2000). It is submitted that the authors are experienced administrators of survey instruments on and offline and are aware of the strengths and limitations of survey research.}

Part I of this paper discusses the ambiguous legal landscape that provides context for website acquisition and the use of personal information supplied by consumers.\footnote{See Eugene Volokh, \textit{Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You}, 52 \textit{STAN. L. REV.} 1049, 1076–80 (2000) (focusing on the uncertain state of the law of privacy in cyberspace).} Drawing on an economic-analysis-of-law approach (also called the law and economics approach, or the property rights approach), Part I discusses the concept of market failures, which have been the subject of numerous economic journal articles and law reviews.\footnote{The Law and Economics school of thought is most closely linked with the University of Chicago, its economics, law, and business programs. Although this form of analysis may have begun at the University of Chicago, the influence is now worldwide. According to one source, "[a]ll of the major U.S. law schools — Harvard, Yale, Princeton [sic], Chicago, Stanford, and Berkeley among them — now offer courses in the Economic Analysis of Law and have professors with Ph.D.s in Economics on faculty." Christopher Bruce, \textit{Applying Economic Analysis to Tort Law}, 3 \text{The Expert Witness Newsletter} (Economica,
Standard economic analysis reveals some elements of market failure in the market for personal information. The implications of the law and economics approach to market failure are used to predict how consumers likely will react in cyberspace to the market for the acquisition and use of personal information.

Part II briefly reviews the survey literature about privacy in cyberspace and shows why the survey used is superior to most others because respondents were asked to respond in a setting that is virtually identical to that which they face on the Internet. Also, Part II develops hypotheses about how respondents will react to the economic and legal uncertainties surrounding personal information that is revealed online to websites.

Part III discusses the survey results and interprets them in light of the discussion of the market for personal information developed in Part I and the hypotheses developed in Part II. The
results of the survey developed for this article are sobering for both owners of websites interested in the economic aspects of the market for personal information and for policy makers who have a continuing interest in Internet privacy issues. In brief, the survey’s respondents exhibited a good deal of caution as to the personal information that they said they would reveal to websites depending on the potential for abuse of that information to them personally. There appears to be more willingness to reveal information to well-known websites than to less well-known websites. In several categories, women were more reluctant than men to reveal personal information. Slightly more than half of respondents indicated that they read and trust websites’ privacy policies. Respondents failed to differentiate between the three most-used, third-party monitors of website adherence to privacy policies: CPA WebTrust, BBB Online Privacy, and TRUSTe.15 Respondents were cognizant of the company brand name of the website and whether there was an option to opt out of databases. Most respondents, by a large majority, were aware of the possible negative consequences of revealing information to websites in terms of identity theft and exposure of their families to unscrupulous people. Finally, the typical inducements that websites offer online visitors to reveal personal information did not impress the survey’s respondents.

15 CPA WebTrust, BBB Online Privacy, and TRUSTe are the three most often used third party guarantors that websites adhere to their privacy policies. These websites are available at http://www.cpawebtrust.org (“CPA WebTrust”) (last visited Mar. 10, 2003), http://www.bbb.org/about/privacy.asp (“BBB Online Privacy”) (last revised June 4, 2001), and http://www.truste.org/ (TRUSTe) (last visited Mar. 10, 2003). In spite of these guarantors, skepticism about website adherence to their privacy policies is rampant. For an article about the value of a guarantee, in which the title indicates the content and editorial angle, see Carrier McClaren, Privacy for Dummies?: Corporations Hide Behind Fake Net Privacy Solutions, TRUSTe, at http://www.ibiblio.org/stayfree/archives/15/privacy.html (June 8, 1998) (on file with the North Carolina Journal of Law & Technology). See also infra note 46.
A. The Market for Personal Information and Uncertain Property Rights

Although there are some exceptions, economists generally assume that actors (sellers, buyers, and consumers) know what is best for themselves. This paper makes the modest assumption that both online and brick-and-mortar firms who sell products know that personal information about their customers, and consumers in general, is valuable. Websites that sell products to consumers not only acquire information from consumers themselves, but also frequently purchase consumer data from other firms that have acquired such data. The market for personal

16 The assumption made by economists that people and firms understand what is in their self-interest dates back at least to 1776, when Adam Smith wrote that "[i]t is not from the benevolence of the butcher, the brewer, or the baker, that we expect our dinner, but from their regard to their own interest." ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 26–27 (Roy Harold Campbell, Oxford Univ. Press 1976) (1776), available at http://socserv.socsci.mcmaster.ca/~econ/ugcm/3113smith/wealth/index.html.

17 According to Samuelson, there is at the moment a "lively market" in personal data, but it is a market in which individuals play at most a very small role. Many firms collect and process personal data because of its value and because information technology makes the collection and use of such data so much easier and cheaper. Samuelson, supra note 3, at 1132. The 2000 Report to Congress of the Federal Trade Commission states that "[a]lmost all sites (97% in the Random Sample, and 99% in the Most Popular Group) collect an e-mail address or some other type of personal identifying information." FTC Report, supra, note 4.

18 Samuelson, supra note 3, at 1127 ("Consider the incentives of a company that acquires private information. The company gains the full benefit of using the information in its own marketing efforts or in the fee it receives when it sells the information to third parties." (quoting PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998)). The Electronic Frontier Foundation ("EFF") keeps records of cutting-edge privacy actions. According to EFF, "Right now there is a lack of awareness about how extensively personal information that has been collected is used on the Net and to whom this information is shared. Most don't realize the vast information sharing chain that exists once a company or governmental agency obtains your personal information." Electronic Frontier Foundation, Marketing & Your Privacy, at http://www.eff.org/Privacy/Marketing/#intro (last visited Mar. 10, 2003) (on file with the North Carolina Journal of Law & Technology).
information has mushroomed because Internet technology has vastly lowered the costs of acquiring, storing, using, and transferring personal information about consumers.\(^{19}\)

Acquisition of personal information in cyberspace can be categorized as voluntary and involuntary. As previously stated, this paper focuses on the voluntary acquisition of information by websites, which occurs when consumers reveal information about themselves to websites in connection with the purchase of products, admission to various cyberclubs, participation in contests, or through other techniques. Consumer information acquired in such a manner costs firms virtually nothing after the appropriate software has been deployed. When consumers and website visitors click some buttons on their keyboards, consumer information is collected, stored, and categorized virtually without any expenditure of labor once the initial software configuration costs have been incurred.\(^{20}\) Among the information acquired in this manner is the consumer's name, which enables marketers to obtain addresses and phone numbers, thus providing a crossover point of contact between cyberspace and geography. Virtually all information acquired online is also linked to consumers' e-mail

---

\(^{19}\) Among the authors who analyze the privacy implications of improvements in information technology and the market for personal information are: Kang, supra note 3, at 1223–38; Froomkin, supra note 6, 1465–1501; and Samuelson, supra note 3, at 1132.

\(^{20}\) In a conversation that one of the authors had with an executive at a major healthcare insurer during the fall of 2000, the executive estimated that her organization expended $4.00 in costs, most of it labor, when a client called about a health problem, but the costs of online inquiries were estimated at $0.15. That magnitude of differential provides a powerful incentive to convert, whenever possible, to digital and software acquisition of information. See Medicine Online, at http://www.meds.com/about.html (last visited Mar. 10, 2003) (on file with the North Carolina Journal of Law & Technology) and Traffic Audit & Bureau Services ("TABS"), at http://www.tabsinfo.com/news.htm (last visited Mar. 10, 2003) (on file with the North Carolina Journal of Law & Technology) for examples of websites that advertise savings by responding to patient inquiries online relative to person-to-person responses.
addresses and web browsers, and such linkage enables sellers to have cyber-contact with website visitors.\textsuperscript{21}

Although very much a part of Internet privacy issues, involuntary acquisitions of information by websites are outside the scope of this paper.\textsuperscript{22} Websites attach cookies to web browsers, and these cookies enable websites to record clickstreams of the browsers from the time of a consumer's first visit to a website until the next visit.\textsuperscript{23} As with voluntary transmissions of personal

\textsuperscript{21}See The Center for Democracy and Technology, \textit{Doubleclick Puts Hold on Tying Personal Info To Online Habits}, at http://www.cdt.org/action/doubleclick.shtml (last visited Mar. 10, 2003) (on file with the North Carolina Journal of Law & Technology); see also Press Release, Doubleclick, Statement from Kevin O'Connor, CEO of Doubleclick, (Mar. 2, 2000), at http://www.cdt.org/privacy/000302doubleclick.shtml (on file with the North Carolina Journal of Law & Technology). According to O'Connor, "[i]t is clear from these discussions that I made a mistake by planning to merge names with anonymous user activity across Web sites [sic] in the absence of government and industry privacy standards." \textit{Id.} O'Connor did not rule out merging online and offline data in the future, and other companies may be tempted to do the same thing. The technology appears to exist to combine on and offline data.

\textsuperscript{22}Involuntary acquisition of information takes place when cookies, web bugs and other creations of software for tracking and reporting back to hosts are utilized without first asking permission of the operator of the browser. For most people, whose knowledge of cookies and other tools for surreptitious information acquisition is limited, information is acquired from them without their consent or even their knowledge. Froomkin takes readers through a terrifying journey when he discusses "privacy-destroying" technologies. Froomkin, \textit{supra} note 6, at 1468-1501. On the other hand, Froomkin makes the valid point that if an event takes place in public, then it is not an invasion of privacy to record the event with a camera. The First Amendment protects such data collection. An issue arises whether travels in cyberspace should be viewed as public events. In any event, there is little doubt that our travels in cyberspace are being recorded, and in virtually all cases, the information is being gathered without our consent. Froomkin, \textit{supra} note 6, at 1506.

\textsuperscript{23}Froomkin uses the term "clicktrail," but the concept is the same, namely that it allows "savvy Web designers to figure out what other sites their visitors patronize." Froomkin, \textit{supra} note 6, at 1486. According to Cookie Central, "[a] cookie is a text-only string that gets entered into the memory of your browser." Cookie Central, at http://www.cookiecentral.com/faq/ (last modified June 8, 2002) (on file with the North Carolina Journal of Law & Technology). According to one source, "[t]o put it more plainly, a cookie is a mechanism that allows a web site to record your comings and goings, usually without your
information from consumers to websites, information acquisition using cookies takes place automatically once the software is in place. It is involuntary in the sense that consumers do not manifest assent to this form of information collection before the information is collected. Indeed, disabling cookies causes some browsers to be unwelcome at many websites, thus severely restricting access in cyberspace. In addition, it is likely that the majority of Internet users has only a passing knowledge or interest in cookies, web bugs, spyware, and other surreptitious information gathering devices used by websites. Fortunately for the privacy interests of consumers, most involuntary acquisitions of information are tied to web browsers, rather than to individuals, but that line has also been crossed by some firms who have been able to link cookie data with names. It seems likely that connecting online behavior with

---


“Spyware,” as defined by a group called “Spychecker,” is advertiser-supported software. The downside, according to Spychecker, is that the software also installs additional tracking software on your system, which is continuously calling home, using your Internet connection and reports statistical data to the “mothership.” Spychecker claims that “you have a ‘live’ server sitting on your PC that is sending information about you and your surfing habits to a remote location.” Spychecker, What Is Spyware?, at http://www.spychecker.com/spyware.html (last visited Mar. 10, 2003) (on file with the North Carolina Journal of Law & Technology).

Judnick v. Doubleclick was scheduled to go to trial in Superior Court in San Rafael, California, in January of 2002. The plaintiff, on behalf of the General Public in the State of California, was seeking to enjoin Doubleclick “from unlawful, misleading, and deceptive business practices on the Internet that violate the privacy rights of the plaintiff and the General Public.” Judnick v. Doubleclick, No. 000421 (Cal. Super. Ct. filed Jan. 27, 2000), available at http://legal.web.aol.com/decisions/dlpriv/doubleclick.pdf. The case has since been withdrawn after Doubleclick CEO O’Conner agreed to stop the practice of merging online and offline personally identifying data. Supra note 21.
names, in addition to browsers, will become more frequent. Consumers’ privacy concerns are likely to increase as information gathered voluntarily online becomes merged with information acquired involuntarily from cookies and from other sources, such as grocery store purchases, credit card purchases, and even public records.  

1. Consequences of Losing Control of Personal Information

The technology that made the Internet possible offers a unique opportunity to investigate how consumers and website owners react when property rights are ambiguous. Websites acquire much personal information under circumstances in which consumers are required to trust that the website to which they reveal personal information will not take advantage of them by using the information in ways that are deleterious to their interests. The adverse consequences of misusing personal information are not limited to financial losses. They can also encompass simple corruption to serious problems such as harassment, violence, insurance cancellation, loss of job or home, and relationship issues with family and friends.

According to EFF, DoubleClick, an online advertising company, places banner ads and other website advertisements on behalf of its clients. The dispute concerns DoubleClick’s use of cookies and web bugs to track the web browsing behavior of individuals. Individuals are often unaware these technologies exist, what they can do to avoid a cookie or a web bug, or how they can prevent companies like DoubleClick from placing cookies on their computer hard drives. . . . The lawsuit alleges that by using cookies DoubleClick can store personally identifying information, resulting in a profile of individuals based on their surfing history. Online profiling and aggregation of data from different sources allows others to form opinions, to market items, and to discriminate based on a profile that may or may not be accurate. Unwanted disclosure of information may have harmful consequences, ranging from simple embarrassment to serious problems such as harassment, violence, insurance cancellation, loss of job or home, and relationship issues with family and friends.

Electronic Frontier Foundation, Judge Rules Alleged DoubleClick Privacy Violations Sufficient to Go to Trial, EFF Media Release, at http://www.eff.org/Legal/Cases/DoubleClick_cases/20010606_eff_doubleclick_pr.html (June 6, 2001) (on file with the North Carolina Journal of Law & Technology).

See Froomkin, supra note 6, at 1475.

On the Internet, there is an anonymity feature to revealing information that is not present in transactions with brick-and-mortar companies. Brick-and-mortar
information by websites include, but are not limited to, nuisance phone calls from telemarketers, a general feeling of loss of privacy, identity theft and credit card fraud, embarrassment, and stalking by undesirables. Given the ease of acquiring and transmitting information, it is not farfetched to imagine that prospective employers will someday be able to obtain medical records of prospective job applicants and even clickstream data.28

Although significant legal uncertainty surrounds the acquisition, use, and storage of information acquired online, the Internet should not be confused with a classic Hobbesian jungle where most activity is directed towards protecting oneself from predation by others.29 Although the risks of the inappropriate use of personal information are known to most Internet users, the transmission of information from consumers to websites takes place daily in many thousands of routine transactions.30

companies can be seen, and these companies generate substantial information that enables consumers to make rational choices about revealing information to that vendor.

28 See Samuelson, supra note 3, at 1172 ("For my doctor to send information about my medical condition to an insurance company so that it will cover the costs of treatment is appropriate, but for the doctor to give the same information to a prospective employer is inappropriate."). The issue of employers being able to obtain personal medical information is becoming more and more a concern. 29 "Hobbesian jungle" is a reference to the classic work by Thomas Hobbes, LEVIATHAN. Life in the Hobbesian jungle, according to Hobbes, is a place where there is no place for Industry; because the fruit thereof is uncertain: and consequently no Culture of the Earth; no Navigation, nor use of the commodities that may be imported by Sea; no commodious Building; no Instruments of moving, and removing such things as require much force; no Knowledge of the face of the Earth; no account of Time; no Arts; no Letters; no Society; and which is worst of all, continuall feare, and danger of violent death; And the life of man, solitary, poore, nasty, brutish, and short. THOMAS HOBBES, LEVIATHAN 62 (Richard E. Flathman & David Johnston, W. W. Norton & Comp., Inc. 1997) (1651), available at http://www.uoregon.edu/~rbear/hobbes/leviathan.html.

30 Apparently, the increasing popularity of the Internet has more than offset consumer fears as the number of Internet users grew more than tenfold from 1990 to early 2000, when there were over 300 million users. Andrea Goldstein and David O'Connor, E-Commerce and Development: Prospects and Policy
Apparently, for many consumers, revealing some personal information to some websites is a risk they are willing to endure: consumers protect themselves by being discriminating about the websites to which they reveal personal information.\textsuperscript{31} It should also be noted that growth in the online security industry shows no sign of abating.\textsuperscript{32}

2. Transfers of Personal Information in the Real World and in Cyberspace

There are many situations in everyday life when transmissions of personal information take place that have risks of misuse similar to those that occur in cyberspace. In those situations, there are expectations that such information will not be misused. For example, patients and clients regularly reveal personal information to their physicians and stockbrokers that could be misused, but there is an expectation that such information will be used only for specific purposes.\textsuperscript{33} In most cases,


\textsuperscript{31} This speculation is consistent with the results of the survey.

\textsuperscript{32} The Google search engine reveals ninety-seven websites that are equipped to offer Public Key Infrastructure (encryption) services. There are 471 entries next to Internet security on the same search engine. [Search date June 2002]. For an analysis of the interplay between security and the role of access controls, see Melissa Kern, \textit{Note: Paradigm Shifts and Access Controls: An Economic Analysis of the Anticircumvention Provisions of the Digital Millennium Copyright Act}, 35 U. Mich. J.L. Ref. 891 (2002).

\textsuperscript{33} Legal sanctions can be visited upon stockbrokers and doctors who violate a client's or patient's trust by making unauthorized secondary use of such information. Note, however, that much information is revealed to doctors and service providers by patients under circumstances that are less than optimal. Sometimes the patient does not have adequate time to make an informed judgment. If the patient or his relatives are at a hospital under emergency circumstances, they will generally sign most any authorization that is put in front of them. \textit{See, e.g.}, Sosa v. Paulos., 924 P.2d 357, 359 (Utah 1996) (At the time Ms. Sosa "consented" to arbitrate any claims that she may have against her physician, Dr. Paulos, it was less than one hour before her surgery, she was undressed, and she was given three separate agreements to sign. It is probable that consent to distribute her medical records to secondary sources was buried within the consent forms).
professionals such as doctors and lawyers do not violate informational expectations of patients and clients on a person-to-person basis.\textsuperscript{34} Of course, the legal system has been enlisted to punish service providers, such as doctors, lawyers, and stockbrokers, who breach their fiduciary obligations to their clients by using personal information for unauthorized purposes.\textsuperscript{35}

The fact that medical records are sometimes, and perhaps increasingly, acquired by those selling pharmaceutical drugs or other medical products concerns many people.\textsuperscript{36} Supporters of the Health Insurance Portability and Accountability Act ("HIPAA") of 1996 had twin aims: (1) the portability of health care insurance by employees when changing jobs; and (2) the protection of the privacy of medical records.\textsuperscript{37} By and large, the first aim has been achieved, but how best to protect the privacy of medical records has simply not been resolved. Although extensive work and revisions in the proposed HIPAA regulations regarding the privacy


\textsuperscript{35} Of course, many professionals are required to be licensed in order to practice, and if they lose their licenses and continue practicing, they can be fined or incarcerated.

\textsuperscript{36} Baumer, Privacy, supra note 11, at 45\textemdash 46; see also Bartley Barefoot, Comment, Enacting a Health Information Confidentiality Law: Can Congress Beat the Deadline? , 77 N.C. L. REV. 283 (1998).

of medical records took place during the Clinton Administration, implementation has been slow and uncertain.\textsuperscript{38} Most patients are willing to reveal their health records to health care providers for purposes of medical treatment and payment but would consider it a violation of privacy and a breach of trust by healthcare providers if those professionals revealed patients' medical information to third parties for commercial purposes.\textsuperscript{39} Indeed, inappropriate use and abuse of medical records has become an increasingly persistent problem as those records are computerized.\textsuperscript{40}

In cyberspace, consumers are frequently invited and requested by websites to reveal personal information. For some e-commerce transactions, consumers must reveal their name, address, and credit card number. Many popular websites create all sorts of reasons why consumers should reveal personal information, including allowing consumers to participate in games and interest groups and to qualify for discounts on products sold by particular websites and other websites (co-branding). Surveys by the Federal Trade Commission ("FTC") reveal that information acquisition takes place at more than 97% of websites.\textsuperscript{41}

\textsuperscript{38} The latest version of HIPAA regulations may be found at the Department of Health and Human Services website (http://www.hhs.gov/ocr/hipaa/privrulepd.pdf); 45 C.F.R. §§ 160, 164 (2002).
\textsuperscript{39} See Baumer, Earp, and Payton, supra note 11, at 45, which contains a survey of healthcare workers who had access to medical records as to their views of invasions of privacy. The practice most disapproved of by healthcare workers with regard to the privacy of medical records was unauthorized secondary use of medical records and distribution to commercial third parties for marketing purposes. On a scale of 1 to 7, with 7 being "Strongly Disagree," the average response was 6.36 indicating that virtually all of the healthcare workers in the sample Disagree or Strongly Disagree with the practice.
\textsuperscript{40} When medical information was stored as paper records in file cabinets, pilfering medical records was too risky and time-consuming to justify the effort, but the same cannot be said of medical records that are stored as computerized files.
\textsuperscript{41} See FTC Report, supra note 4.
3. Measures Frequently Taken by Websites to Allay Consumer Fears

When consumers interact with websites, they reveal personal information in an anonymous context, and many consumers are concerned about what happens to this information. Websites have responded to consumers' and website visitors' privacy concerns with Privacy Statements, which are now a staple of virtually all popular websites, especially those that involve e-commerce. In addition to privacy statements, websites make use of Terms of Use and Legal Notices links that provide additional legal boundaries.

Although website privacy statements and other legal notices may have been intended to allay consumer uncertainties about the use of information acquired from consumers, many of these privacy statements make use of turgid legalese that is undoubtedly confusing to the average reader. In addition to

42 According to the FTC Privacy Report, "[s]ixty-two percent of sites in the Random Group (compared with 44% in the 1999 GIPTS survey) and 97% of sites in the Most Popular Group (compared with 81% in the 1999 OPA survey) post a privacy policy." Id. at 10 (footnotes omitted).
43 For example, under the Conditions of Use for Amazon.com, the following sentence appears following Risk of Loss: "All items purchased from Amazon.com are made pursuant to a shipment contract. This means that the risk of loss and title for such items pass to you upon our delivery to the carrier." http://www.amazon.com/exec/obidos/tg/browse/-/508088/qid=1048823097/sr=1-4/104-9329659-5750358 (last visited Mar. 10, 2003) (on file with the North Carolina Journal of Law & Technology).
44 Legalese is very much in evidence in the eleven page Terms of Service at Yahoo!. Specifically, members of Yahoo! "agree" to indemnify Yahoo! for any content that is submitted by a member, and Yahoo! can cancel a member's password "for any reason" and "without limitation." Furthermore, all warranties are disclaimed and there is a limitation of liability in boldface capital letters. Finally, members agree that their relationship with Yahoo! is governed by the laws of the State of California and they are subject to the personal jurisdiction of the courts located within Santa Clara, California. Yahoo!, Privacy Policy, at http://docs.yahoo.com/info/terms/ (last visited March 10, 2003) (on file with the North Carolina Journal of Law & Technology). The Yahoo! Privacy Policy is a mere four pages, but Yahoo! reserves the right to change its privacy policy, which currently prohibits transmission of personal information collected by their cookies to third parties. Yahoo!, Terms of Service, at
uncertainty from customers about promises that websites are making with respect to information acquired from them, there is widespread skepticism about whether websites keep those promises.45 Aware that many consumers are skeptical about the reliability of promises made by websites, many websites make use of third-party guarantors, such as TRUSTe, BBBOnline, and CPA WebTrust Seal. These third-party guarantors monitor the websites’ adherence to the promises made in their privacy statements.46 Websites offer additional control over personal


45 Such skepticism is apparently with good reason because the FTC has prosecuted several websites for violating promises made in their privacy statements and other legal notices. See, e.g., Federal Trade Commission, Geocities: Analysis to Aid Public Comment (FTC File No. 982-3015), 63 Fed. Reg. 44624 (August 20, 1998). Also note the action of the FTC against an online auction that lied to its customers with respect to its use of information acquired from these customers. Federal Trade Commission, Online Auction Site Settles FTC Privacy Charges: Personal Identifying Information Hijacked From Competitor’s Site; Many Consumers Sent Deceptive Spam, at http://www.ftc.gov/opa/2000/01/reverse4.htm (January 6, 2000) (on file with the North Carolina Journal of Law & Technology).

46 According to TRUSTe, “A cornerstone of the TRUSTe privacy program is our branded online seal, or ‘trustmark.’ We award the seal to Web sites that adhere to established privacy principles and agree to comply with our oversight and consumer resolution process.” TRUSTe, at http://www.truste.org/about/truste/about_faqs.html (last visited Mar. 27, 2003) (on file with the North Carolina Journal of Law & Technology). Similar comments are made at the BBBOnline website, which, again, provides assurance that the website will live up to certain standards. BBBOnline, at http://www.bbbonline.com/about/press/2002/050602.asp (May 1, 2002) (on file with the North Carolina Journal of Law & Technology).

According to Web Trust,

WebTrust helps to make cyberspace a safer place to shop. E-commerce has been inhibited by concerns over the security and privacy of credit card and other confidential information transmitted when purchasing goods and services electronically, as well as the frequent inability of consumers and businesses to confirm the legitimacy of companies offering goods and services over the Web. WebTrust addresses these concerns while reducing the risk of fraudulent practices and privacy and security infringements.
information by providing an "opt out" option, which is a guarantee by websites that the personal information collected in one transaction will not be used for other purposes or that it will be erased following the transaction.47

Despite these and other measures that websites have taken to allay consumer trepidation about privacy and the misuse of personal information, consumers remain concerned about revealing personal information to websites.48 Consumer fears about revealing information to websites are justified for a number of reasons. First, numerous articles have provided anecdotal information about the negative consequences of revealing personal information online.49 Second, privacy statements that websites use to allay consumer fears about the misuse of personal information are typically loaded with exculpatory language in the forms of warranty disclaimers, arbitration clauses, choice of forum and law provisions, and a confusing number of other restrictions and qualifiers that are written in difficult-to-understand legalese.50 In


47 Again, opt outs are nothing if they are not enforced. In other words, in most opt out options, the website claims it erases personal information that it acquires. Whether in fact the website does erase the information it claims is subject to the opt out option is anyone's guess.

48 See FTC Report, supra note 4 and accompanying text.

49 See Electronic Frontier Foundation, at http://www.eff.org/privnow/ (last visited Mar. 11, 2003) (on file with the North Carolina Journal of Law & Technology) (citing a bushel basket full of anecdotes about breaches of privacy and the consequences of these breaches). There are several recent articles that discuss identity theft, which is one of the major negative consequences of revealing information online. See Miriam Albert, E-Buyer Beware: Why Online Auction Fraud Should Be Regulated, 39 Am. Bus. L.J. 575 (2002); Stephanie Byers, The Internet: Privacy Lost, Identities Stolen, 40 Brandeis L.J. 141 (2001); Michelle Hall, Internet Privacy or Information Piracy: Spinning Lies on the World Wide Web, 18 N.Y.L. Sch. J. Hum. RTS. 609 (2002).

50 Virtually all websites that involve substantial e-commerce will have the exculpatory terms in their privacy statements and other legal notices or terms of service. These terms often radically shift legal rights of customers. Examples are evident by looking at the Privacy Policies and Terms of Service agreements of Yahoo!. Yahoo!, Privacy Policy, at http://privacy.yahoo.com/privacy/us/
short, the guarantees provided by websites are likely to be more apparent than real. Third, when consumers are given a choice about the use of their personal information by websites, often they must agree to all of the provisions without negotiation. Finally,

(last updated 2003) (last visited Mar. 10, 2003) (on file with the North Carolina Journal of Law & Technology); Yahoo!, Terms of Service, at http://docs.yahoo.com/info/terms/ (last visited Mar. 10, 2003) (on file with the North Carolina Journal of Law & Technology). In its Terms of Service agreement, Yahoo! incorporates by reference its Privacy Policy. In both statements, Yahoo! reserves the right to modify unilaterally. Among other points of interest in the 11-page Yahoo! Terms of Service agreement are an agreement by subscribers to indemnify Yahoo! against any actions subscribers take that may generate liability for Yahoo! (Paragraph 9). Virtually every conceivable Warranty Disclaimer and Limitation of Liability are made in Paragraphs 17 and 18 of the Yahoo! Terms of Service agreement. By browsing the Yahoo! website, users agree that they are subject to the personal jurisdiction of the court within Santa Clara County, California. The Yahoo! website is typical of prominent commercial websites.

Note that there are attempts to allow for more interactivity between websites and browsers.

The P3P (Platform for Privacy Preferences Project) movement, developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web Sites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web Site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web Sites make this information available in a standard, machine-readable format. P3P enabled browsers can 'read' this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.

World Wide Web Consortium, Platform for Privacy Preferences (P3P) Project, at http://www.w3.org/P3P/ (last revised Mar. 11, 2003) (on file with the North Carolina Journal of Law & Technology). Getting the world to adopt and use the P3P will be a major project and success is certainly not assured. Also, there are critics of P3P who claim that it is nothing but a more efficient procedure for websites to gather even more information from visitors. See, e.g., Karen Coyle, P3P: Pretty Poor Privacy? A Social Analysis of the Platform for Privacy
if a website breaches promises it made not to distribute personal information to third parties, only those people who have advanced training in both computer hardware and software minutiae can detect the breach.\(^{52}\)

### 4. Federal Statutory Protection for Information Gathered or Used Online

Most websites are not subject to any specific statutory regulation, unless they target children, for acquiring information or are storing or transmitting medical information, and then they are subject to the Gramm-Leach-Bliley Act, which provides some protection for financial records held by banks.\(^{53}\) Websites that do not acquire financial or medical information or seek information

---

\(^{52}\) Although most of us are not equipped by training or temperament to investigate possible surreptitious high-tech means of acquiring information, Richard Smith is a free-lance privacy expert who has made a number of important discoveries. Smith, for example, discovered that RealNetworks Inc. ("RNWK") collected computer ID numbers from Web surfers who downloaded RealNetwork software to hear CDs. Smith also discovered that Microsoft Word contained an electronic marker that was stamped into every document created enabling employers to track whistleblowers more easily, before they blow the whistle. Amy Borrus, *The Privacy War of Richard Smith*, BUSINESSWEEK ONLINE (Feb. 14, 2000), available at http://www.businessweek.com/2000/00_07/b3668067.htm?scriptFramed (on file with the North Carolina Journal of Law & Technology). Someone with Richard Smith’s skills could possibly discover whether a website was not adhering to promises it made in its privacy policy, but most of the rest of us have to take websites at their word.

from children are basically unregulated in information acquisition, usage, and storage.

There have been websites that have breached promises made in privacy statements that subjected them to sanctions by the Federal Trade Commission. The FTC, however, does not have the resources to monitor millions of websites, nor does it have jurisdiction to prosecute fraud by websites based outside the U.S. In an effort to detect privacy violations and scams, the FTC, along with other agencies and private groups, devotes entire days to "surfing the web." When the FTC does surf the Internet, it finds literally hundreds of examples of fraud and dubious promises by websites. There are millions of promises made in cyberspace, and if the FTC surfing sample is representative, many of those promises are misleading or unfulfilled.

In short, legal remedies for the misuse of personal information by websites are in many cases nonexistent. If a

56 Prepared Statement of the Federal Trade Commission on "Internet Fraud": Hearing Before the Senate Committee on Finance, 106th Cong. 4 (April 5, 2001) (statement of Hugh Stevenson, Associate Director of the Division of Planning and Information in the Federal Trade Commission's Bureau of Consumer Protection, describing surf days), available at http://www.ftc.gov/os/2001/04/internetfraudstate.htm. The FTC developed the Consumer Sentinel, which is an online complaint web page. In the year 2000, Consumer Sentinel received over 100,000 complaints. During surf days, FTC officials and others literally uncover hundreds of websites making what the FTC labels "dubious" claims.
57 Id. at 4.
58 Id. at 5. The FTC has identified over 6,000 websites making dubious claims, but in many cases these websites surface and disappear with little or no warning.
59 Julie Cohen makes the point that [t]he present valuation placed on any given surrender of personally-identified information is, of course, also a matter of personal choice. Yet it is difficult to assess the future significance of a loss of privacy, much less to compare that future harm with a currently offered benefit . . . . The
website violates its privacy statement, it breaches its contracts with its consumers, but it is unlikely that damages will be sufficient to justify a suit unless consumers are somehow organized into a class action.\textsuperscript{60} Probably, the most potent weapon consumers and those who look out for their interests have is publicity.\textsuperscript{61}

The adverse publicity associated with a suit by the FTC or a state attorney general on behalf of consumers for breach of promises made in privacy statements could be devastating for a website's economic viability.\textsuperscript{62} In addition, there are a number of valuation problems compounded by the fact that the trivial and incremental character of each loss—information about a grocery purchase here, a magazine subscription there—tends to minimize its ultimate effect. A comprehensive collection of data about an individual is vastly more than the sum of its parts.

Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 STAN. L. REV. 1373, 1397–98 (2000) (citing A. Michael Froomkin, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases, 15 J.L. & Com. 395, 492 (1996)) (stating that as long as "in each individual transaction the cost of not providing the information is disproportionate to the loss (which is a function of the cumulation of the transactions, not any single transaction) a property rights approach appears unlikely to have much real influence on database creation").

\textsuperscript{60} According to Eugene Volokh,

Thus, I certainly do not claim that a contractual approach to information privacy, even with a large dollop of implied contract, is a panacea for information privacy advocates. As Paul Schwartz and others have pointed out, there is much that information privacy advocates may want but that contract will not provide.

Volokh, supra note 12, at 1062 (citing Paul M. Schwartz, Privacy and Participation: Personal Information and the Public Sector Regulation in the United States, 80 IOWA L. REV. 553 (1995)).

\textsuperscript{61} Adverse publicity generated by the discoveries of Richard Smith and other privacy sleuths caused (1) RealNetworks to change its software so that the musical preferences of users were no longer reported back to RealNetworks; (2) Intel to change its chips so that users of Microsoft Word could not be traced; and (3) DoubleClick to back off on merging online and offline data. See BUSINESSWEEK ONLINE, supra note 52 and accompanying text.

private watchdog groups that are active in investigating and publicizing breaches of promises made by websites in privacy statements. Still, to the average consumer, legal remedies are inadequate, and because they are inadequate, polls reveal that most consumers feel powerless to control what happens to personal information revealed to websites. For most consumers, their only power is the power to withhold information about themselves from websites, websites that need such information for their economic viability.

5. Markets and Market Failures

For most tangible goods, property rights are generally well-defined, in the sense that the legal ownership of such goods is not subject to competing claims. Purchasers reward those who acquire or produce goods efficiently to the extent that the producers' costs of production plus transfer costs are less than what transferees are willing to pay for the goods. Markets evolve to facilitate the appropriation of the value of goods by rewarding those who specialize in the acquisition, production, and sale of goods with minimum transaction costs.

of the World Wide Web is the plethora of alternatives. If you are not convinced about the integrity of a website, there are seemingly many substitutes just a few clicks away.

The Electronic Privacy Information Center, Privacy Resources, at http://www.epic.org/privacy/privacy_resources_faq.html (last updated May 6, 2002) (on file with the North Carolina Journal of Law & Technology) (listing 17 separate privacy watchdog groups, among which are its own operations, Electric Frontier Foundation, the ACLU, and many others).

See Samuelson, supra note 3 and accompanying text; see also Kang, supra note 3 and accompanying text.

The seminal article in the law and economics literature that deals with the importance of property rights was written by Nobel Prize winner, Ronald Coase, The Problem of Social Cost, 3 J.L. & ECON. 1 (1960).

A basic proposition of economics is that trade takes place when the value of the thing being traded is worth less to the seller than it is to the buyer. See, e.g., Jack Hirshleifer and David Hirshleifer, Price Theory and Applications 193–216 (6th ed. 1997) [hereinafter Hirshleifer and Hirshleifer].

Transaction costs are the costs above those associated with producing and transporting goods, such as the opportunity cost of time spent negotiating as to
It is apparent, of course, that not every market operates flawlessly. Market failures, often prompting governmental intervention, occur when property rights are not well-defined, transaction costs are high, and there are external costs borne by third parties associated with the production or consumption of goods, for which legal status is unclear. For example, clean air is a good for which property rights are not easily defined. If factories and car owners pollute air without incurring the costs of polluted air borne by society, there will be too much pollution and too little incentive among polluters, both producers and consumers, to take anti-pollution measures. In addition, as with many market failures, there is the free-rider problem. As a result, without

price. Id. at 410–19. Clarkson and Miller write that, "Exchange between two parties has its costs of offers, negotiations, acceptance, delivery, inspections, warranty, and other activities associated with the exchange of goods and services, generally called transactions costs." KENNETH CLARKSON AND ROGER MILLER, INDUSTRIAL ORGANIZATION: THEORY, EVIDENCE, AND PUBLIC POLICY 20 (1982).

"Market failure" has been explained in numerous articles by economists, and it is standard fare in most economics textbooks. See, e.g., HIRSHLEIFER & HIRSHLEIFER, supra note 66, at 484. Richard Posner, Chief Judge of the Seventh Circuit, states,

Monopoly, pollution, fraud, mistake, mismanagement and other unhappy by-products of the markets are conventionally viewed as failures of the market's self-regulatory mechanisms and therefore as appropriate occasions for public regulation. But this way of looking at the matter is misleading. The failure is ordinarily a failure of the market and of the rules of the market prescribed by the common law.

RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 343 (3d ed. 1986).

See HIRSHLEIFER & HIRSHLEIFER, supra note 66, at 485.

Readers of this journal undoubtedly are familiar with the concept of "free riders." Efforts to clean up the environment on a voluntary basis are plagued by the free rider problem because the activities of a single individual will not make the environment significantly cleaner or dirtier. Therefore, each individual has an incentive to "free ride" on others who bear the costs of a cleanup. A similar situation occurs in cyberspace. All websites would benefit if consumers were more forthcoming with information, but that is not going to occur as long as the legal environment for information acquisition and use is so nebulous. If a single website adheres to fair information principles, and most do not, the website is harmed because its customers are still reluctant to reveal information to that website. On the other hand, if nearly all websites adhere to fair information
government regulation, there is little incentive on the part of polluters not to pollute or to invest in pollution abatement technology.\textsuperscript{71} If a firm chooses not to pollute, it will not appreciably affect the environment, and the firm's profits will be lowered by the amount of extra costs incurred in polluting less.

6. Markets and Market Failure in Cyberspace

There have been many authors who have commented upon what they regard as the unsatisfactory state of affairs in the market for personal information acquired online by websites.\textsuperscript{72} In fact, the legal literature on Internet privacy is enormous, but the law is just one of several disciplines contributing to discussions of online privacy.\textsuperscript{73} The focus of this paper is not to provide a summary of the Internet privacy literature. Instead, the perspective employed in this paper is that the online acquisition of personally identifiable information should be viewed as a market because markets and market failures yield useful predictions that can be tested. In particular, this paper develops the notion that because property rights to personal information are not well-defined, a market

\begin{quote}
\textsuperscript{71} "As the group size increases, it is more likely that everyone will behave as a free rider, and the public good will not be provided." Id., at 25. Needless to say, the size of groups on the Internet, both websites and browsers, is well beyond the level in which negotiations among and between groups is feasible.
\textsuperscript{72} Using the Lexis-Nexis Legal Research search engine and the key terms, "Internet Privacy" generated 267 "hits" among law reviews. (June 2002).
\textsuperscript{73} The issue of privacy in cyberspace has attracted the attention of IT (information technology) academics and professionals, who often publish in various branches of the Association of Computing Machinery journal. See Association of Computing Machinery, at http://www.acm.org/ (last visited Mar. 11, 2003). Other IT journals have tackled the issue of privacy in cyberspace, as well. See Management Information Systems Quarterly, at http://www.misq.org/ (last updated Dec. 12, 2002); Journal of Management Information System, at http://jmis.bentley.edu (last visited Mar. 11, 2003).
\end{quote}
failure takes place similar to that which took place in the market for clean air before the Clean Air Act was enacted in 1971.74

Some have tried to make the best of a bad situation by viewing the very concept of Internet privacy as an oxymoron. This view was perhaps best articulated by the much-cited statement of Sun Microsystems, Inc. CEO Scott McNealy, who was quoted as saying, "You have zero privacy. Get over it."75 Other analysts, however, are not quite as pessimistic.76 It is one thing to recognize that the current situation is lamentable because privacy expectations are often defeated, but it is quite another thing to throw up one’s hands and declare the situation unsolvable.

One way of articulating what is wrong with the online market for personal information is to analyze it as a market failure.77 Personal information, obtainable in cyberspace, can be viewed in much the same light as many of the goods that have been subject to market failures in traditional markets. The failure of the market for personal information, according to Professor Samuelson, takes place because a company that acquires private information through a website derives the full benefit of "using the information in its own marketing efforts or in the fee it receives when it sells the information to third parties" without suffering the losses from disclosure of private information.78 Applying basic

76 Many of the authors of the law reviews cited in this article are cognizant of the magnitude of the threats high-tech innovation has posed to personal privacy, but have not raised a white flag and given up. See e.g., Samuelson, supra note 3.
77 It is contended that the laws of economics operate in cyberspace. A market failure in cyberspace has the same characteristics as those that occur in the "real" world.
principles of economic analysis of property rights that have been applied to numerous other market failures, Samuelson concludes that “[i]n economic terms, the company internalizes the gains from using the information but can externalize some of the losses and has a systematic incentive to overuse it.”79

The market for personal information in cyberspace is similar to the unregulated market for clean air: the polluter internalizes clean air and uses it for gain but largely externalizes the costs of polluted air.80 When websites acquire personal information, they normally do not pay consumers for the information, and consumers are not really sure of the uses made of that information.81 If personal information is abused, consumers suffer loss of utility in the same way they suffer loss when a factory dirties the air and consumers have to breathe the results. It could be argued that websites obtaining personal information from consumers are unjustly enriching themselves at the expense of consumers in the same way that factories are not paying the full costs of production when they pollute the air without paying for the social costs of air pollution.82

79 Samuelson notes that
This market failure is made worse by the costs of bargaining for the desired level of privacy. It can be daunting for an individual consumer to bargain with a distant Internet merchant . . . about the desired level of privacy. To be successful, bargaining might take time, effort, and considerable expertise in privacy issues.
Id. On the issue of overuse or excessive quantities being produced when the market produces negative, external effects, see BROWNING AND BROWNING, supra note 14, at 35–38.
80 On the economics of air pollution, see WERNER Z. HIRSCH, LAW AND ECONOMICS: AN INTRODUCTORY ANALYSIS 14–16 (2d ed. 1988).
81 According to the Federal Trade Commission, “The level of consumer unease is reflected in the results of a recent study in which 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential, and 82% agreed that government should regulate how online companies use personal information.” FTC Report, supra note 4, at 2 (footnote omitted).
82 See BROWNING AND BROWNING, supra note 14, at 24–35. When a negative externality occurs, third parties are harmed and essentially pay the consequences of the harm, costs that the producers of the harm avoid. In comparison, when information obtained from consumers is used in ways that the consumers do not
7. Self-Regulation and Free Riders

In an unregulated environment, a firm that installs air-pollution abatement equipment does not have a way of charging its customers extra for being a good corporate citizen, particularly if the goods sold are undifferentiated commodities. Steel, for example, produced in a less-polluting manner would not be differentiable from steel produced in the customary manner, as all would sell for the same price. Unless the government sets pollution standards, there will be a race to the bottom among polluters because the actions of any one polluter, producer, or consumer will have no perceptible impact on the atmosphere.

As with air pollution, the free-rider problem exists in cyberspace and effectively blunts efforts of responsible websites. Ethical website behavior is defined as that which corresponds to the five Fair Information Practices propounded by the FTC. Ethical behavior by individual websites will have no impact on the overall legal environment in cyberspace unless consumers can anticipate or authorize, they suffer the externalized costs of privacy invasion, while websites are able to capitalize monetarily from the sale or use of that information.

Certainly, upscale grocery stores carry premium (organic) food products that frequently advertise the lack of fertilizers or pesticides used in growing such foods, and such food products often carry premium prices. These food products are differentiated in a way that allows those who subscribe to these values to reward these producers.

If one website adheres to ethical standards, such as those proposed by the FTC, such actions will have no discernible impact on the overall public perception of the integrity of the cyberspace market environment. See FTC Report, supra note 4, at iii.

The FTC Fair Information Practices ("FIPs") are: Notice—people are entitled to be notified if an information file is being kept on them; Choice—people should be entitled to have a say in how personally identifying information is used; Access—websites should offer access so that errors can be corrected; Security— websites should be required to use commercially reasonable means to protect personal data from outside interception; and Enforcement—there should be a way for those harmed by collection of information about them to pursue legal remedies. Id.
THE MARKET FOR PERSONAL INFORMATION

recognize it. Since it can be presumed that no website advertises that it does not adhere to its own stated privacy policy, the important question is how websites can credibly signal to consumers that they are trustworthy and that personally identifying information can be safely disclosed to them.

A number of solutions come to mind. Websites could, in effect, tell consumers, "You don't need to trust us, because we have a third party monitoring our adherence to the promises made in our privacy statement. We are entitled to display the TRUSTe certification on our website. We can be trusted!" Not quite, according to Michael Froomkin and others who have studied the issue. As of March 2002, a TRUSTe "white paper" claims to have over 1,500 online merchants who pay up to $9,000 for the right to license and display the TRUSTe logo on their website. TRUSTe does not really monitor whether a website adheres to its privacy policy, but rather, it verifies that the website does indeed have a privacy policy. In addition, TRUSTe investigates complaints by consumers that a website is not adhering to its privacy policy, but according to Froomkin, the "meaningfulness of

86 The fact that a website claims to respect personal data does not distinguish the website. Virtually, all websites claim to respect personal data.
87 According to Froomkin,

Froomkin, supra note 6, at 1525. It should be noted that RealNetworks.com no longer displays the TRUSTe logo. The reason for this change is unknown to the authors.
88 See TRUSTe, at http://www.truste.org/ (last visited Mar. 11, 2003) (on file with the North Carolina Journal of Law & Technology). For multiple corporate brands, TRUSTe charges as much as $25,000 for the right to display its trustmark.
89 Froomkin, supra note 6, at 1525.
the 'trustmark' has been called into question." Froomkin and others question the integrity of the guarantees of TRUSTe and other third party monitors of websites that license the logo because there have been a number of well-publicized breaches of promises made by websites, and yet, these websites have retained their trustmark. In sum, third-party monitors, such as TRUSTe, face an inherent conflict of interest: every time they declare a website unworthy of licensing its logo, they reduce their licensing revenues by the amount received from that website. Not surprisingly, there have been few examples of websites that have been condemned by TRUSTe and other third party guarantors.

It is possible that the market will cure itself. The meaningfulness of the promises made by TRUSTe and other third party monitors could improve until the problem of lack of trust among consumers of website promises is significantly reduced. Self-regulation as an antidote to fraud has worked reasonably well in some markets, though often with governmental sanctions available to augment private actions. Satisfactory solutions to the

90 Id.
91 Froomkin states,

Critics suggest that TRUSTe's unwillingness to remove or suspend a trustmark results from its funding structure . . . If TRUSTe were to start suspending trustmarks, it would lose revenue; if it were to get a reputation for being too aggressive toward clients, they might decide they are better off without a trustmark and the attendant hassle.

Id. at 1526–27 (referencing website listing TRUSTe's corporate sponsors).
92 Note that TRUSTe is currently doing more than just monitoring whether a website has a privacy policy. One TRUSTe web page describes their "seeding" program that monitors whether websites are actually adhering to the claims made in their privacy statements. According to the company, "TRUSTe regularly 'seeds' Websites, which is the process of tracking unique identifiers in the site's database. We submit unique user information ourselves and monitor results to ensure that your site is practicing information collection and use practices that are consistent with its stated policies." TRUSTe, at http://www.truste.com/programs/pub_oversight.html (last visited Mar. 11, 2003) (on file with the North Carolina Journal of Law & Technology).
93 Froomkin opines that, "[w]ithout some sort of government intervention to encourage self-regulation, 'wolves self-regulate for the good of themselves and the pack, not the deer.'" Froomkin, supra note 6, at 1524 (quoting Roger Clarke, The Legal Context of Privacy-Enhancing and Privacy Sympathetic
misuse of information conveyed to websites could occur in the absence of explicit governmental regulations. Many pessimists, however, argue that the gains from cheating, in the form of unauthorized secondary uses of personal information, appear great relative to the costs, especially in light of the apparently small probability of detection.94 For most people, the value of defeated expectations of privacy is likely to be modest and not likely to justify filing a lawsuit. Given the difficulty of valuing losses of privacy and the rather modest damage figures due to breaches of promises made by websites in their privacy statements, the only real legal alternative may be class action suits or suits on behalf of citizens by states' attorneys general. Such litigation is likely to be long and unlikely to assuage consumer concerns that there are few effective remedies if websites do not adhere to their privacy policies.

8. The Current State of Affairs

Both commentators and polls of the general public agree that the acquisition of personal information online is potentially threatening. The results of the survey developed for this article confirm that most consumers are unaware that there are consequences associated with the misuse of personal information acquired online; such consequences can range from inconvenience and calls by telemarketers to more serious events, such as identity theft and credit card fraud.95 Most consumers are very concerned

94 Froomkin, supra note 6, is one author pessimistic about the efficacy of self-regulation curing privacy problems in cyberspace. The fact that so many lawmakers, academics, and privacy-related websites have examined this topic is a further indication that lack of privacy in cyberspace is a market failure. See e.g., the Electronic Frontier Foundation, supra note 2.

95 The survey results, discussed infra pp. 260–69, show that a large majority of the respondents were very aware of the downside risks of misuse of personal information gathered online.
Despite these concerns, millions of consumers disclose crucial information voluntarily every day to websites that appear reliable. Consumers routinely reveal credit card numbers to order merchandise online. They reveal their home addresses, business and home telephone numbers, and other personally identifying information in connection with business-to-consumer ("B2C") e-tailing. In addition, consumers reveal much information to websites in connection with various games and contests. There is no way of knowing at this point how much larger e-commerce would be if the legal environment for personal information in cyberspace were more stable and defined. Respondents' concerns, however, suggest that reducing legal uncertainty could significantly increase the size of the market.

---

96 The survey results reinforcing this contention are shown infra pp. 51–52. The U.S. Department of Justice has an excellent article about cyberstalking entitled 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY (August 1999), at http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (on file with the North Carolina Journal of Law & Technology). The article discusses statistics and provides anecdotes that illustrate the cyberstalking problem.

II. Literature Review of Online Surveys, Survey Design, and Hypotheses Generated

A. Recent Research Dealing with Online Privacy

Numerous major studies of Internet privacy have made use of surveys. In 1997, a survey by Westin of American computer users over the age of eighteen explored user concerns about issues ranging from communication by e-mail, fax, and telephone to marketing to computer users while online and offline. It also explored group differences between heavy and light Internet users, as well as the differences between male and female computer use. The general finding was that computer users tend to have fears about online privacy invasions that greatly exceed the actual occurrences of those invasions. The Westin survey also revealed that 58% of respondents indicated that information was requested from them while merely visiting websites. Although 79% of respondents refused at some point to provide some information requested by websites, 61% admitted that they provided some of the information requested. 71% of respondents who declined to reveal information to websites, or revealed false information to websites, also indicated that they would have revealed accurate information if they had had an on-

100 Id.
101 Id.
102 Id.
going business relationship with the website owner. In the same survey, 63% said that they would have supplied the information the website requested had the website clearly informed them how the information would be used before requesting the information.

In a follow-up telephone survey the next year, Westin addressed the privacy concerns of Internet users, specifically, their experiences, concerns, and policy preferences. It established the concrete steps Internet users want business websites to take to strengthen Internet users' confidence that the personal information users provide to websites will be properly managed. A striking result of the survey was that 96% of those who made purchases online said that it was important for websites to post privacy notices, and 72% of respondents indicated that posting privacy notices was "very important." It is important to note, however, that the survey was conducted in 1998. By the year 2003, privacy notices are clearly the industry norm for websites.

In a 1999 follow-up survey, Westin found that 12% of respondents felt that revealing their personal information for benefits, even if informed how the information would be used, would violate their individual privacy boundaries. On the other end of the scale, 13% of respondents agreed that if the website "informs me what will be done with my information, and I like the benefit and [will] not be offended by the use, I would be willing to trade my privacy for membership in the website sponsored

\[\text{Id.}\]

\[\text{Id.}\]


\[\text{Id.}\]

group." According to the same survey, three out of four Internet users said that when they are online, they want it all: privacy notices from websites, benefits from websites, and websites' adherence to their privacy policies.\textsuperscript{109}

The IBM Multi-National Consumer Privacy Study, published in 1999, was the first significant survey of consumer perceptions toward online privacy.\textsuperscript{110} The respondents included residents of the United States, the United Kingdom, and Germany. The IBM study measured consumer attitudes toward privacy in everyday business transactions and explored consumers' attitudes toward personalized marketing in general and their views of how companies handle personal information in different countries. Results from the survey indicated that banks and healthcare companies compared favorably with insurance companies, department stores, catalogs, and Internet companies in terms of enjoying the greatest degree of confidence from respondents.\textsuperscript{111} In addition, the survey revealed that the consumers most likely to take steps to protect themselves are precisely those that are of greatest interest to marketers: younger, more educated, and, generally, more affluent consumers in their peak earning years.\textsuperscript{112} The survey also revealed that privacy protection behaviors are more likely to occur at financial and insurance websites than at healthcare websites.\textsuperscript{113}

The Earp and Payton study, published in 2000, was based on a survey of financial and healthcare workers and revealed that privacy concerns are not confined to consumers but also include employees who access and collect consumer data.\textsuperscript{114} An interesting finding of Earp and Payton is that healthcare workers are concerned about organizational practices that they believe cause errors in patient information, as well as the unsanctioned use

\textsuperscript{108} Id.
\textsuperscript{109} Id.
\textsuperscript{110} IBM Privacy Survey, supra note 4.
\textsuperscript{111} Id. at 12.
\textsuperscript{112} Id. at 15.
\textsuperscript{113} Id. at 12.
\textsuperscript{114} Earp and Payton, supra note 98, as 51–54.
of patient information. Similarly, the study indicates that employees of financial institutions are concerned with organizational practices that allow improper access to customer information.

The Earp and Payton study surveyed healthcare workers who had access to medical records as to their views about the greatest threats to the privacy of those records. Using a Likert scale, respondents at a local hospital were asked a series of questions about privacy policies and practices of their employer. Among the major findings of the study was the respondents' emphatic agreement that:

1. The greatest threat to the privacy of medical records occurred when their employer made unauthorized secondary distribution of patient healthcare records to outside firms, and
2. That their "employer should devote more time and effort verifying the accuracy of the patient information in its databases."

Likert scales, first developed in the 1930s by R. Likert, are explained in detail in J. NUNNALLY, PSYCHOMETRIC THEORY (1978). The idea behind Likert scales is to transform ordinal variables into numeric variables. A short, online "all you need to know" article about Likert scaling is located at William M.K. Trochim, Likert Scaling, available at http://trochim.human.cornell.edu/kb/scallik.htm (last revised June 29, 2000) (on file with the North Carolina Journal of Law & Technology). Baumer, Earp, and Payton, supra note 11, used a seven-point Likert scale beginning with Strongly Disagree (1) and ending with Strongly Agree (7). If all the assumptions necessary for using Likert scales are satisfied, researchers can meaningfully calculate average responses to statements and make statistical comparisons. For example, if the survey average response to a statement was 1.5, the response would indicate that most respondents agreed or strongly disagreed with the statement. If the average response to a statement was 6.5, it would mean most respondents strongly agreed or agreed with the statement.

The survey results found by Baumer, Earp, and Payton, supra note 11, indicated that respondents strongly agreed (6.51 on a seven-point Likert scale) that their employer (a hospital) should not make unauthorized secondary distributions of patient healthcare records and agreed with almost equal emphasis (6.48) that more attention should be devoted to making sure healthcare records were accurate.
B. Shortcomings of Prior Studies of Online Behavior

Although these studies are informative and relevant, they treat threats to privacy as an aggregate issue and do not explore the elemental components of online privacy. None of the studies ask, component by component, about the willingness of consumers to reveal personal information. The survey developed for this article reveals that some people are very concerned about the privacy of their financial records, while others are more concerned about the privacy of their medical records. Personal privacy and its online protection have a number of components that should be examined individually, rather than as an overall concept. For example, asking respondents whether they would be willing to reveal their social security numbers to actual websites is much different than asking respondents whether they would reveal "personal information" about themselves online. The survey developed by the authors employed a component-by-component analysis of the concerns of people about online privacy issues, rather than lumping all the components of personal information together and treating the privacy issue in the aggregate.

Additionally, previous studies do not explain the impact privacy concerns will have on e-commerce and the willingness of consumers to supply information online to websites. More specifically, the survey developed for this article addresses whether websites could assuage consumers' privacy concerns by taking certain steps, such as opt out provisions, third party webseal monitors, offerings of targeted advertisements, and participation in games or offers of gifts, discounts, and cash. The survey developed by the authors asked respondents which measures taken by websites to assure their trustworthiness were in fact decisive and effective in gaining their trust so that they would reveal personal information. For example, using a five-point Likert scale, it asked respondents to respond to the following statement, "My level of confidence in the privacy practices of the website is

---

influenced by: If I were given the option to 'opt out' or disallow the distribution or sale of information about me.\textsuperscript{120} Consumer responses to actions and programs taken by websites to assure reliability have tremendous implications for the future expansion of B2C e-commerce.

C. Survey Design: Steps Taken to Assure Reliability

This study analyzed data collected from an online survey linked to several online resources, including the North Carolina State University E-Commerce website and the website of a major healthcare insurer.\textsuperscript{121} The data was collected during the latter half of 2000 through early 2001 and represents the opinions of 415 respondents. The respondents, although more educated than the population at large, are educationally and demographically comparable to the diversity found among Internet users in general and in other studies.\textsuperscript{122} The average web usage of the survey's respondents was approximately thirteen hours per week, with fifty-two percent of respondents having more than four years of prior Internet use.

The survey was administered online so that each respondent would face one of thirty randomly appearing web pages while responding to the survey questions.\textsuperscript{123} The thirty websites

\textsuperscript{120} This study used a five-point Likert scale: Strongly Agree, Agree, Unsure, Disagree, and Strongly Disagree.
\textsuperscript{121} The E-Commerce project at North Carolina State University ("NCSU") is headed by Professor Michael Rappa, Alan T. Dickson Professor of Information Technology. The E-Commerce Project website is located at http://ecommerce.ncsu.edu. E-Commerce.edu, at http://ecommerce.ncsu.edu (Mar. 11, 2003) (on file with the North Carolina Journal of Law & Technology).
\textsuperscript{123} When respondents took the survey, they were online and were not prompted in any way by the authors. Respondents encountered the surveys while browsing through the E-Commerce website at NCSU or while browsing through the website of a major healthcare insurer in North Carolina, Blue Cross Blue Shield of North Carolina, at Blue Cross Blue Shield of North Carolina, at http://www.bcbsnc.com (last visited Mar. 11, 2003) (on file with the North
were equally divided among retail, medical or health, and financial websites. This study focused on the aforementioned website categories because they tend to request more personal information from visitors. Within the three categories of websites, fifteen were well-known websites, and fifteen were lesser-known websites. A well-known website is defined as one listed in the top 1,500 websites, ranked by unique users, from PC Data Online, 2000. Lesser-known websites are those that are not listed in the top 1,500 websites.

The survey consisted of thirty-four responses to various statements such as, "I would provide my phone number to this website." The survey employed a five-point Likert scale anchored by "Strongly Disagree" (1) and "Strongly Agree" (5), providing five possible responses per question. Of the 415 respondents, 129 observed one of the ten retail websites, 159 observed one of the ten medical or health websites and 127 observed one of the ten financial websites.

D. Unique Features of this Survey

The survey developed for this article is unique in several ways, but like the other surveys, it suffers from limitations that caution against making strong statements about the survey results' implications for the general population of computer users. The Carolina Journal of Law & Technology). All responses were anonymous to the authors, and surveys were not taken in the authors' presence. The websites that respondents were shown were actual websites that can be accessed on the Internet.

124 PCDataOnline was a respected Internet website traffic rating company that released polling results on a monthly basis to its subscribers. The original website, at http://www.PCDataOnline.com, was eventually redirected to http://www.netscoreonline.com/. Netscore, What's Your NetScores?, at http://www.netscoreonline.com (last visited Mar. 11, 2003) (on file with the North Carolina Journal of Law & Technology). Now, NetScore provides these polling statistics online.

125 The science of surveys is sufficiently imprecise and random that researchers should be wary of making strong statements about the population based on the survey responses of a small sample. Using standard survey methodology, a sample of 415 enables one to perform most statistical tests, such as whether the means between females' and males' responses are so different that the
science of taking surveys online or in other settings makes use of a plethora of unverifiable, mainly mathematical, assumptions that are not often realized in the real world. Because reality is not always as random as is assumed in marketing research textbooks, experienced survey administrators know enough to be cautious about making strong inferences on the basis of a single survey.

1. **Disaggregation of Privacy Concerns**

The survey first investigated the elemental components of privacy by exploring the individual factors that influence online behavior, rather than treating the privacy issue in the aggregate. Instead of being quizzed about their general concerns about privacy, respondents in the survey were asked to consider whether they would provide their name, address, social security number, and other personal information to randomly displayed web pages (see Table 1 below).

2. **Realism**

Second, the survey design uses the flexibility of the World Wide Web to offer respondents a realistic visualization of websites to illustrate survey questions. By providing actual screen shots of well known and lesser-known retail, medical, and financial websites, the survey brings survey respondents closer to the situations they face in online sessions when they have to decide

difference is unlikely to be due to chance. Underlying the statistical tests, however, are a number of critical assumptions. One assumption, for example, is that the demographics of the general population are the same as those of the sample. Another assumption is that respondents understand the questions, even though there is no way of knowing whether this assumption is accurate because the respondents are anonymous. The assumptions commonly made in administering surveys are voluminous and there are additional challenges when administering online surveys.


---

\[126\] Id.
whether to reveal personal, demographic, medical, and financial information to a specific type of website. The realism of asking consumers to respond online to actual screen captures of websites considerably enhances the reliability of the survey's results relative to asking consumers, in the abstract, about their willingness to reveal personal information online.

3. Non-Recursiveness and Iteration

Third, the survey is non-recursive and iterative.\textsuperscript{127} It not only asked respondents to reveal what they would be willing to reveal to websites, but also whether websites can do anything to allay privacy-related concerns. In effect, the survey assumes by its questions that consumer reactions to the actions of websites vis-à-vis privacy will cause websites to react by changing their policies. As an added check, the survey asked respondents to reveal some personal information, although no information was demographic or personally identifying.\textsuperscript{128} The efficacy of self-regulatory actions by websites should be of interest to both businesses that maintain websites and policy-makers who have a difficult time striking the proper balance between freedom and government regulation.

\textsuperscript{127} A "non-recursive" relationship occurs when the following takes place: A affects B, but B then affects A. In other words, it may be characterized as a feedback loop. In this analysis, the authors hypothesize that policies of websites affect visitors, but visitors' reactions to those policies cause websites to change those policies. If websites do not respect privacy wishes of online visitors, then there will be fewer online visitors. Websites react to fewer online visitors by making more and more credible claims of caring for personal information revealed to them in a way that reflects the wishes of the information provider. The survey attempts to capture not only a measure of the privacy concerns of respondents, but also their reactions to measures websites use to entice them to reveal personal information. The survey is metaphorically iterative in the sense that it reveals how privacy concerns of consumers reverberate through the system. For a discussion of the difference between recursive and non-recursive models, see \textsc{Barbara G. Tabachnick and Linda S. Fidell}, \textit{Using Multivariate Statistics} 744 (3rd ed.1996).

\textsuperscript{128} In other words, respondents were asked whether they would be willing to reveal demographic information to a random sample of websites that the authors selected. Respondents were then asked to reveal their demographic information to us.
E. Hypotheses Generated from Legal and Economic Analysis of the Market for Online Personal Information

The hypotheses discussed below are based on the following assumptions:

1. The market for information acquisition and distribution in cyberspace is, with some significant exceptions, unregulated; and
2. Consumers really have no satisfactory legal recourse when personal information is lawfully and voluntarily acquired by websites but misused or distributed to third parties without authorization because, in general, damages are too small to justify a lawsuit, or jurisdictional issues prevent effective lawsuits.129

These two assumptions imply that anarchy reigns in the market for online voluntary acquisition of personal information. If personal information is requested from consumers by a website and respondents assume that they have no legal recourse if the information they provide to websites is misused, it is logical that some of the following factors may affect the willingness of consumers to supply personal information:

1. **Well Known Websites** (Brand Name Awareness) Consumers would be more willing to reveal information to websites with which they are familiar.

2. **Personally Identifying Information** Consumers would be more reluctant to reveal personally identifying information about

---

129 This prediction assumes that respondents are aware that medical and financial websites are more regulated than are other websites. Undoubtedly, many respondents were unaware of the Gramm-Leach-Bliley Act and the HIPAA regulations, but they and Internet users generally are more educated than the general population, so this assumption is not so extreme.
themselves than demographic information, such as age, race, sex, and email address.

3. **Identity Theft or Credit Card Fraud**

Consumers would be most reluctant to reveal information about themselves that could enable someone to steal their identity or gain access to their credit cards.

Using the model of an unregulated market with no legal recourse when fraud or deliberate contract breaches occur, other predictions about the willingness of consumers to reveal information are plausible.

4. **Gender** Cyberstalking is probably more threatening to women than to men, and therefore, it is predicted that women would be less willing to reveal information about themselves than men.

5. **Effect of Government Regulation** Since medical and financial records are subject to more government regulation, it is submitted that consumers would be more willing to reveal information to those kinds of websites relative to retail websites, which are the least regulated of the three.\(^{130}\)

Data from other surveys reveals that consumers are concerned about protecting and controlling their personal information.\(^ {131}\)

6. **Importance of Opt Out Options** It follows that consumers would highly prize opt out options by websites to allow them to retain more control over the use of personal information.

Consumers who reveal personal information are often disturbed by the feeling that someone else is making money from “their” personal information.

7. **Purchases or Trades for Personal Information** Since websites value personal

\(^{130}\) Froomkin, *supra* note 6.

\(^{131}\) See *Federal Trade Commission, supra* note 4; Westin, *supra* note 4; *IBM Privacy Survey, supra* note 4.
information, they could ameliorate consumer misgivings about revealing personal information by offering monetary and non-monetary incentives in the form of targeted advertisements that apprise consumers of bargains that may be of interest to them.

III. Survey Results

A. Demographic, Personal, Financial, and Medical Information

Respondents were shown one of thirty websites and were asked to respond using a five-point Likert scale, with 1 being Strongly Disagree and 5 being Strongly Agree, to the following statement:

I would provide the following information about myself to this website:

As is apparent from Table 1, respondents are least reluctant to supply basic demographic information, such as age, gender, race, and ethnicity, about themselves. Demographic information, of course, is not individually identifying. It is also clear that, on average, respondents were far less willing to supply personally

### Table 1
Willingness to Supply Information to this Screenshot (Average Responses in Boldface)

<table>
<thead>
<tr>
<th>Age</th>
<th>Gender</th>
<th>Race or Ethnic</th>
<th>Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.453</td>
<td>3.525</td>
<td>3.135</td>
<td>3.029</td>
<td>2.512</td>
</tr>
<tr>
<td>Phone #</td>
<td>E-mail address</td>
<td>Credit Card #</td>
<td>Employer name</td>
<td>Income</td>
</tr>
<tr>
<td>2.184</td>
<td>3.152</td>
<td>1.893</td>
<td>2.017</td>
<td>1.804</td>
</tr>
</tbody>
</table>

Social Security:
- Prescription
- Drug History
- Personal Medical Info

| 1.464 | 2.773 | 1.751 |

As is apparent from Table 1, respondents are least reluctant to supply basic demographic information, such as age, gender, race, and ethnicity, about themselves. Demographic information, of course, is not individually identifying. It is also clear that, on average, respondents were far less willing to supply personally
identifying information about themselves. The lowest stated willingness among respondents to supply information occurs with regard to social security numbers, income, credit card numbers, and medical records, each of which is individually identifying, with the exception of income. Respondents were also very reluctant to reveal the name of their employer and their phone number, each of which is information that could make consumers vulnerable if unscrupulous individuals possessed such data. Respondents were more willing to supply their name, e-mail address, and prescription drug history than the name of their employer. Certainly, giving out e-mail addresses is far less revealing than disclosing a credit card number, but respondents to the survey developed for this article seemed only slightly less willing to give out actual names compared to e-mail addresses. In ordinary offline transactions, it is common to give out one’s name to total strangers, but it is far less common to reveal one’s social security number, credit card numbers, or income.

The ordinal rank of customer willingness to supply various types of information exhibited in Table 1 seems plausible. It is likely that the reluctance of respondents to supply a social security number reflects a fear of identity theft. Also, most people are very reluctant to release medical information about themselves, except to their physicians or other medical personnel. Similarly, most people regard information about their income as private, and since they are concerned about their jobs, they are very reluctant to reveal their employer. Respondents were less concerned about basic demographic data and were more willing to reveal their e-mail address and name than the very personal and traceable information listed above.

---

132 “In common usage, an ordinal number is an adjective which describes the numerical position of an object, e.g., first, second, third, etc.” Eric W. Weisstein, Wolfram Research, at http://mathworld.wolfram.com/OrdinalNumber.html (last visited Mar. 11, 2003) (on file with the North Carolina Journal of Law & Technology). If a person prefers A to B and B to C, the ordinal rank of preference is A B C. Ordinal rank says nothing, however, about how much more A is preferred relative to B or C. Given the stochastic nature of survey responses, the most important statistic in Table 1 is probably the ordinal rank rather than the absolute value of responses based on a Likert scale.
The mean differences in respondents' willingness to supply information by category reflect the uncertain legal environment of e-commerce. If the legal environment in cyberspace were secure, if there was adequate legal redress for the breach of promises made in privacy statements, and if privacy statements themselves were understandable and balanced, mean scores in Table 1 would be expected to be in the 4 to 5 range. The fact that mean scores for some types of information are in the 1 to 2 range indicates that respondents in the survey viewed the legal environment in cyberspace as being very insecure.

B. Additional Statistical Relationships

1. Well-Known versus Less Well-Known Websites

The range in mean responses in Table 1 indicates that consumers are very selective about the type of information that they will and will not supply to websites. This selectivity is further evidenced when compared with respondents' willingness to supply personal information based on whether the website was well-known or not well-known, according to the criteria discussed above. Of the 415 respondents, 217 observed one of the fifteen lesser-known sites while 198 observed one of the fifteen well-known sites. The stated willingness of respondents to provide telephone numbers, home addresses, e-mail addresses, social security numbers, and credit card numbers to websites was significantly different (p<.05) with respect to whether the website was well-known or not well-known. Although the respondents

---

133 All statistical tests based on survey sample results are based on a number of underlying assumptions that may or may not be satisfied. When statistical analysis reveals that the difference in sample means is significant at the .05 level, it means that there is less than a one in twenty chance that the difference in the means is due to chance—assuming the survey sample is truly random and representative of the population. If, for example, people willing to complete online surveys were different from the general population in some way, then the sample results would not be representative of the general population. Statisticians often make what are termed “heroic” assumptions because there is
as a whole reacted negatively to providing these five categories of information to the observed website, they were much more negative towards the lesser-known websites. It can be inferred from this that consumers are more willing to provide their home address, phone number, email address, social security number, and credit card number to a well-known website compared to a lesser known website. Such a distinction is in part because consumers do not have confidence that the e-commerce legal environment is secure enough for them to have a remedy if less well-known websites misuse their personal information. Apparently, investing in goodwill is a valuable asset for websites.

2. Differences Based on Type of Website

Overall, there is a statistically significant difference (p<.05) in respondents’ average willingness to supply information attributable to the type, retail, financial, or medical or health, of website at issue.\textsuperscript{134} Put differently, the survey’s respondents were more willing to divulge information to medical or health websites than to retail or financial websites. Individually, there were significant differences for five individual categories of personal information: age, gender, race, employer, and medical records. Respondents were more likely to provide their age, gender, race, employer, and medical information to health websites than retail websites.\textsuperscript{135} When comparing health websites with financial websites, the differences were less striking, but respondents were more inclined to provide their employer and medical information to health websites. These results could possibly be attributed to legislation that protects bank records and medical records, as well as the lack of legislation surrounding retail websites.

---

\textsuperscript{134} Again, these differences are significantly different at the .05 level (p<.05).

\textsuperscript{135} These differences are significantly different at the .05 level (p<.05).
3. Differences in Willingness to Supply Personal Information Based on Gender

The survey not only asked respondents if they would be willing to share certain types of personal information, but it also asked respondents to actually share some of that information. In particular, the survey asked respondents their gender. If a respondent refused to reveal his or her gender, then his or her gender was recorded as 0 (zero). Females who revealed their gender were recorded as “1,” and males willing to reveal their gender were recorded as “2.” Of those respondents who did state their gender, there were statistically significant differences between men and women with respect to their stated willingness to divulge personal information. By statistically significant margins, women were more reluctant than men to divulge their names, addresses, phone numbers, e-mail addresses, employers, and social security numbers, and these differences were statistically significant. Many of the aforementioned components of privacy (e.g., names, etc.), of course, could place women at risk physically from stalkers, a risk about which many men are not concerned. Again, if the legal environment in cyberspace were insecure, one would expect that the more vulnerable members of society, women, for example, would be more reluctant to share information that could be misused.

4. Age-Related Differences in Willingness to Supply Personal Information

The survey developed for this article also asked respondents their ages. A comparison of respondents in the fifteen to thirty-five year age group with those over thirty-five years of age revealed that the younger group was much more willing to provide their name, age, and gender, read privacy policies, and give personal information in exchange for cash or a gift offered by websites. These differences were significant at the .05 level (p<.05). The latter two categories, “reading privacy policies” and willingness to “provide personal

---

136 These differences were significant at the .05 level (p<.05). The latter two categories, “reading privacy policies” and willingness to “provide personal
about identity theft, losing control of their information, the unauthorized redistribution of their information, and exposure to unscrupulous people. All of these differences based on age were statistically significant. Older respondents were more cautious and more fearful of the downside risks associated with the loss of control over personal information. Again, these results appear plausible and reflect the uncertain legal environment in the market for personal information. Younger respondents were willing to take more risks by providing more information, but as a group, they probably have less to fear from identity theft because their financial assets are typically far less significant than the financial assets of respondents over the age of thirty-five.

C. Privacy Policies, Brand Names, Website Design, and Third-Party Monitors

The next series of questions were directly related to the issue of self-regulation with regard to privacy and the trust that customers place in privacy policies, the brand names of websites, and third-party monitors. Respondents were asked to respond to the following statements.\(^{137}\)

If this were my first visit to the site, I would read the privacy policy:

I trust that this website adheres to its privacy policy:

My level of confidence in the privacy practices of the website is influenced by:

I am familiar with privacy seal programs (such as, CPA WebTrust, BBBOnline and TRUSTe):

\(^{137}\) The statements have been edited for brevity in the text. The actual questions, reproduced in the Appendix, provide explanations of some of the terms, such as CPA WebTrust, BBB Online Privacy, and TRUSTe, as well as other additional details.
I would be more likely to share personal information with the above website if it carried the (CPA Web Trust, or BBBOnline, or TRUSTe—three separate questions):

Table 2
Privacy Practices of Websites
(Average Responses in Boldface)

<table>
<thead>
<tr>
<th>Read Privacy Policy</th>
<th>Trust Privacy Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.345</td>
<td>3.427</td>
</tr>
<tr>
<td>Company or Brand Name</td>
<td>Privacy Statement Provided</td>
</tr>
<tr>
<td>3.875</td>
<td>3.592</td>
</tr>
<tr>
<td>Option to Opt Out</td>
<td>Web Seal Is Present</td>
</tr>
<tr>
<td>3.877</td>
<td>3.234</td>
</tr>
<tr>
<td>CPA WebTrust</td>
<td>BBB Online Privacy</td>
</tr>
<tr>
<td>3.369</td>
<td>3.336</td>
</tr>
</tbody>
</table>

The survey results in Table 2 suggest that only slightly more than half of the respondents read privacy statements when they first visit a website. About the same number trust that websites adhere to their privacy policies. If those figures reflect the general population, it suggests a great deal of skepticism among consumers visiting websites. According to the results of the survey developed for this article, consumer confidence increases when the website is a company or brand name and when the website has an opt out option. The fact that a website has a privacy policy is viewed as being important, but interestingly, respondents indicated that the design of a website does not significantly instill more confidence. The factor that most promotes confidence is having the option to opt out, which reveals that consumers most highly value the ability to control use of the personal information that they provide to websites. Among the respondents, all of the third-party monitors of adherence to privacy policies were viewed as mildly increasing confidence in the website. There was, however, no perceived difference between the three services by respondents in terms of an increasing willingness to share personal information.
Overall, the results in Table 2 suggest that consumers have more confidence in websites that are brand names and those that offer opt out options. Slightly more than half of the respondents indicated that they read privacy policies the first time they visit websites and about the same number indicated that the presence of web seals and web seal companies (TRUSTe and the others) would make them more willing to reveal personal information. The ubiquity of privacy policies and third-party web seals suggests that most websites are cognizant of consumer fears regarding personal information and have responded in ways that somewhat allay those fears.

D. Identity Theft, Unsolicited Communication, and Other Exposure

Among the concerns that consumers and other visitors to websites have is that personal information will be acquired and used in unauthorized ways. Some of the unauthorized uses of personal information result in the victim becoming an unwanted target of advertisers, invasions of privacy, and having one’s identity stolen through acquisition of social security or credit card numbers.

The next question asked respondents to respond to the following statement:

My concern about sharing information about myself with the above website is:

<table>
<thead>
<tr>
<th>Table 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consequences of Revealing Information to Websites</strong></td>
</tr>
<tr>
<td><strong>Average Responses in Boldface</strong></td>
</tr>
<tr>
<td>Identity Theft</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>3.8895</td>
</tr>
<tr>
<td>Lack of Control over Personal Information</td>
</tr>
<tr>
<td>4.2431</td>
</tr>
</tbody>
</table>
Table 3 reveals some strong reactions by respondents to each of the possible negative consequences listed associated with providing personal information online to websites. Respondents seemed most troubled about the unauthorized distribution of personal information to third parties and the lack of control over personal information, but they were also very concerned about identity theft, theft of credit card numbers, receiving unsolicited advertising, and having their families exposed to unscrupulous people. The results posted in Table 3 reflect not only the concerns of Internet travelers to websites, but also an awareness of how their information can be misused. The high scores indicate that most of the respondents agree or strongly agree that they are concerned about the various negative consequences of revealing personal information to websites.

E. Willingness of Websites to Share Information with Third Parties

The next question asked respondents to respond to the following:

I would allow the website to share personal information about me with a third party:

<table>
<thead>
<tr>
<th>Table 4</th>
<th>Willingness to Share Information with Third Parties (Average Responses in Boldface)</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Receive Targeted Advertising via Mail</td>
<td>To Receive Targeted Advertising via e-mail</td>
</tr>
<tr>
<td>1.901</td>
<td>2.00</td>
</tr>
<tr>
<td>To Receive Cash, Coupons, or a Free Gift</td>
<td>To Participate in a Prize or Lottery</td>
</tr>
<tr>
<td>2.50</td>
<td>2.243</td>
</tr>
</tbody>
</table>

It appears from Table 4 that respondents were less than enthusiastic about receiving either targeted advertising delivered by the post office or transmitted as e-mail. Unsolicited
conventional mail is often labeled "junk mail" and unsolicited e-mail is derisively called "spam." Respondent enthusiasm for giving third parties access to their personal information increased somewhat if the respondents were offered cash, coupons, or a free gift by the website. Respondents were somewhat less excited about the prospect of sharing personal information with third parties in return for the opportunity to participate in a prize or lottery. Overall, the respondents were unenthusiastic about the secondary distribution of their personal information, even if they received the incentives most commonly awarded by websites to their members and visitors. Again, the results of this portion of the survey indicate the importance individuals attach to maintaining control over their personal information.

F. Hypotheses Check

The responses to this survey were consistent with virtually all of the hypotheses posed. By statistically significant margins, respondents indicated that they were more willing to reveal personal information in several categories to well-known websites as compared with less well-known websites. The vast differences in willingness to reveal certain types of personally identifying information as compared to demographic information can be attributed to anarchy in cyberspace. Respondents seemed to be quite aware of the possible serious consequences of identity theft, credit card fraud, and the unauthorized distribution of personal information to third parties. As predicted, women were more reluctant to reveal information than men for a number of categories of personal information. Most respondents viewed very favorably the option offered by many websites to opt out.

IV. Conclusion

Vast skepticism about the legal status of personal information revealed to websites caused the respondents in the survey to be very cautious in their stated willingness to reveal personal information online. Outside of cyberspace, there are many situations in which personal information is requested of
clients, patients, and others in confidential or contractual relationships with professionals and retail establishments. These requests meet nowhere near the reluctance to provide such information as do online requests. For example, whether wise or not, loan applicants routinely provide a complete financial history to banks, and the applicants are not concerned that banks will resell that information or that identity theft will take place as a result. Also, patients regularly provide comprehensive medical histories to physicians and do not expect to have that information used for other purposes such as qualifying for insurance policies or applying for jobs. Similarly, job applicants fill out forms that request phone numbers, addresses, former employers, and social security numbers, and yet, there is little fear among job applicants that the information they provide will be sold to third parties.

On the other hand, the same level of consumer confidence cannot be said to exist for Internet transactions. In addition to involuntary acquisitions of information that take place through cookies, web bugs, spyware, and other surreptitious devices, voluntary disclosures to websites are often accompanied by major uncertainty. This uncertainty is so great that privacy policies are now part of standard operating procedures for most websites. Website privacy policies, however, are not always user friendly; typically, they are heavy on legalese, including exclusions, waivers, and limitations of liability. Also, they change from time to time, so that even if a website's stated policy satisfied a consumer's preference at the time the information was given, the policy could change and, thereby, thwart the consumer's confidence. It is unrealistic to expect consumers to repeatedly read the privacy policies of a website that they have already visited and inspected, and yet, prudence demands that they do so. In addition, not all websites adhere to their privacy policies. Lack of adherence is apparently such a problem that websites prominently advertise third party monitoring of adherence to their own privacy policies.

Outside of cyberspace, visual inspection of the business and the people one deals with provides information as to the reliability of the business and its operators. Such inspections are not always possible in cyberspace. The consequences of this loss of control of personal information in cyberspace can be devastating, and
awareness of these consequences appears to be very much on the minds of consumers.

Some claim that the Internet exploded precisely because its architects did not have to wait for the approval of government bureaucrats. The lack of government regulation is a claimed hidden asset of the Internet, but government is increasingly stepping in and beginning to regulate some Internet uses as the number of people participating in e-commerce rises and abuses receive wider publicity. Although websites that are primarily financial, medical, or targeted towards children are subject to comprehensive regulation and prohibitions, most websites are unregulated and continue to collect, process, and distribute personal information. Currently, consumers are protecting themselves by being selective as to which websites they provide information to and what information they provide. Whether this state of affairs is stable, efficient, or long lasting, however, is anyone's guess.

Appendix
Survey Instrument

*Items 1 – 11 were placed on a 5-point Likert scale anchored by “Strongly Disagree” (1) and “Strongly Agree” (5).*

1. I would provide the following information about myself to this website:
   a. ...My age
   b. ...My gender
   c. ...My race or ethnicity
   d. ...My name
   e. ...My address
   f. ...My home phone number
   g. ...My email address
   h. ...My buying preferences
   i. ...The name of my employer
   j. ...My Income
   k. ...My social security number
   l. ...My prescription drug history
   m. ...Medical information about myself

2. If this were my first visit to the site, I would read the privacy policy.

3. I trust that this website adheres to its privacy policy.

4. My level of confidence in the privacy practices of the website is influenced by:
   a. The company or brand name.
   b. If a privacy statement were provided.
   c. The design of the site.
   d. If I were given the option to “opt-out” or disallow the distribution or sale of information about me.
   e. If a web seal were present on the site.

5. I am familiar with privacy seal programs (such as BBBOnline, CPA WebTrust, and TRUSTe).

6. The CPA WebTrust Seal is a service of the American Institute of Certified Public Accountants. It assures consumers that a CPA has examined and approved a website’s business practices and controls. The site is tested for compliance at least every 90
days. I would be more likely to share personal information with the above website if it carried the CPA WebTrust Seal.

7. The BBB Online Privacy Seal Program assures consumers that the website adheres to established privacy principles and business practices and agrees to random monitoring by Underwriters’ Laboratory. I would be more likely to share personal information with the above website if it carried the BBB Online Privacy Seal.

8. The TRUSTe Seal assures consumers that a website adheres to established privacy principles and has agreed to comply with ongoing TRUSTe oversight. I would be more likely to share personal information with the above website if it carried the TRUSTe Seal.

9. How often do you visit websites that request personal information? (e.g.: name, e-mail address, credit card number, home address, phone number, etc.). Do not count multiple visits to the same website.

10. My concern about sharing information about myself with the above website is:
   a. Theft of my identity.
   b. Theft of my credit card number.
   c. Receiving unsolicited communication.
   d. Lack of control over who sees my personal information.
   e. Unauthorized redistribution or sale of my personal information to a third party.
   f. My family being exposed to unscrupulous people or inappropriate information.

11. I would allow the website to share personal information about me with a third party:
   a. To receive targeted advertising via postal mail.
   b. To receive targeted advertising via my computer.
   c. To receive cash, coupons, or a free gift.
   d. To participate in a prize contest or lottery.