



**PROTECTING ONLINE PRIVACY:
GOVERNMENT REGULATION
OR FREE MARKET INITIATIVES?**

by
Douglas J. Wood
*Hall Dickler Kent
Goldstein & Wood LLP*

W L F

**PROTECTING ONLINE PRIVACY:
GOVERNMENT REGULATION
OR FREE MARKET INITIATIVES?**

by
Douglas J. Wood
*Hall Dickler Kent
Goldstein & Wood LLP*

Washington Legal Foundation
Critical Legal Issues
Working Paper Series No. 101
January 2001

**Washington Legal Foundation
on the World Wide Web:**

<http://www.wlf.org>

TABLE OF CONTENTS

ABOUT WLF'S LEGAL STUDIES DIVISION	ii
ABOUT THE AUTHOR	iii
INTRODUCTION	1
I. THE CURRENT STATE OF AFFAIRS	4
II. THE COLLECTION OF CONSUMER INFORMATION AND ITS APPLICATION ON THE INTERNET	8
III. THE PROGRESS OF SELF-REGULATION	14
IV. THE FEDERAL TRADE COMMISSION'S REVERSAL	16
V. FIRST AMENDMENT CONSIDERATIONS	17
VI. PRIVACY LEGISLATION EFFORTS IN CONGRESS	19
VII. THE EUROPEAN DIRECTIVE AND ITS SAFE HARBORS	21
VIII. THE MARKETPLACE REALITY AND ITS RESPONSE UNDER CURRENT LAW	24
A. Federal Regulatory Actions	26
B. State Regulatory Actions	31
C. Suits by Consumers	33
CONCLUSION	37

ABOUT WLF'S LEGAL STUDIES DIVISION

The Legal Studies Division of the Washington Legal Foundation (WLF) is dedicated to expanding the pro-free enterprise legal idea base. It does this by conducting original research and writing; delivering a diverse array of publication products to businessmen, academics, and government officials; briefing the media; organizing key policy sessions; and sponsoring occasional legal policy conferences and forums.

Washington is full of policy centers of one stripe or another. But WLF's Legal Studies Division has deliberately adopted a unique approach that sets it apart from other organizations.

First, the Division deals almost exclusively with legal policy questions as they relate to the business/corporate community and the economic well-being of the American free enterprise system.

Second, its publications focus on a highly select legal policy-making audience. Legal Studies aggressively markets its publications to federal and state judges and their clerks; members of the United States Congress and their legal staffs; government attorneys; business leaders and corporate general counsel; law school professors and students; influential legal journalists; and major print and media commentators.

Third, Legal Studies possesses the flexibility and credibility to involve talented individuals from all walks of life — from law students and professors to sitting federal judges and senior partners in established law firms — in its work.

The key to WLF's Legal Studies publications is the timely production of a variety of readable and challenging commentaries with a distinctly common-sense viewpoint rarely reflected in academic law reviews or specialized legal trade journals. The publication formats include the provocative COUNSEL'S ADVISORY, topical LEGAL OPINION LETTERS, concise LEGAL BACKGROUNDERS on emerging issues, in-depth WORKING PAPERS, useful and practical CONTEMPORARY LEGAL NOTES, law review-length MONOGRAPHS, and occasional books.

WLF's LEGAL OPINION LETTERS and LEGAL BACKGROUNDERS appear on the LEXIS/NEXIS[®] online information service under the filename "WLF." All WLF publications are also available to Members of Congress and their staffs through the Library of Congress' SCORPIO system.

To receive information about previous WLF publications, contact Glenn Lammi, Chief Counsel, Legal Studies Division, Washington Legal Foundation, 2009 Massachusetts Avenue, NW, Washington, D.C. 20036, (202) 588-0302. Material concerning WLF's other legal activities may be obtained by contacting Daniel J. Popeo, Chairman.

ABOUT THE AUTHOR

Douglas J. Wood is Co-Executive Partner in the New York-based law firm Hall Dickler Kent Goldstein & Wood LLP. He has over 20 years' experience representing national and multinational companies in advertising, marketing and Internet matters and serves as legal adviser to several worldwide advertising industry trade organizations. Mr. Wood has been actively involved in the protection of online consumer privacy for CASIE, a coalition of the Association of National Advertisers (ANA) and the American Association of Advertising Agencies (4As). He is listed in *The International Who's Who of Internet and E-Commerce Lawyers* and is the founder and U. S. member of the Global Advertising Lawyers Alliance (GALA). Mr. Wood is the author of *Please Be Ad-vised: The Legal Reference Guide for Advertising Executives*, published by the Association of National Advertisers; co-author of *Legal Problems in Advertising*, published by Matthew Bender & Co.; and co-author of *The Internet and Advertising Law*, a chapter in *Advertising Law in Europe and North America*, published by Kluwer Law International.

Mr. Wood received his law degree from the Franklin Pierce Law Center, where he is Chair of the Board of Trustees. He received a Masters in Law degree in Trade Regulation from New York University School of Law and a Bachelor of Arts degree in Political Science from the University of Rhode Island.

Author's Note: While my representation of the advertising industry may affect my views on the privacy debate, I have strived to remain objective without compromising the conclusions I have reached. I have received no compensation from any source in the research and preparation of this paper. It was written at my own expense in response to marketplace developments I consider important to a robust and fairly regulated economy.

I would like to express my sincerest appreciation to Carolyn L. Hann, Jennifer V. Koester, and Lindsay M. Schoen for their efforts in the researching, organizing and drafting of this paper. Without their skill, energy and dedication, it would not have been possible.

The views expressed here are those of the author and do not necessarily reflect those of the Washington Legal Foundation. They should not be construed as an attempt to aid or hinder the passage of legislation.

PROTECTING ONLINE PRIVACY: GOVERNMENT REGULATION OR FREE MARKET INITIATIVES?

by

Douglas J. Wood
Hall Dickler Kent Goldstein & Wood LLP

INTRODUCTION

The rapid expansion of the Internet as a medium for business, entertainment, communication and education has been unprecedented. We have truly entered into a new era of information dissemination and communication. The expanded use of the Internet has brought about a vocal and emotional debate over the enactment of consumer privacy regulation and legislation. Advocates on both sides of this heated controversy have taken positions that leave little room for compromise. As a result, questions central to the debate remain largely unresolved. What is the actual threat to consumer privacy on the Internet? What evidence exists to support each side's position in the debate? What is the reality as opposed to the perception?¹

Those advocating regulation and legislation are homing in on the

¹This Working Paper does not attempt to delve into any psychological research in what fears consumers may have regardless of reality, nor how such fears should be properly handled at that level. What it does, however, is review the true dynamics of the marketplace. While the author fully respects pundits and critics, he believes his research is extensive and well-founded. He welcomes critical review of the research and conclusions.

commercial use of personal information collected online.² The demand for “privacy on the Internet” has resulted from accusations that the ability to easily collect consumer information online is injurious to the consumer. The alleged violations of consumer privacy by online marketers and advertisers have been written about extensively.³ Clearly, the perception in the marketplace is that abuse of privacy on the Internet is widespread and in desperate need of legislation and regulation. As Senator John McCain noted while introducing the Consumer Privacy Enhancement Act⁴ in Congress, “chief among those [privacy] concerns is the ability of the Internet to further erode our individual privacy.”⁵

Those advocating a “hands off” philosophy place their faith in self-regulation and industry initiative as the solutions to privacy concerns. They argue that responsible marketers do not want to abuse the rights of their customers and that industry self-regulatory bodies are addressing concerns with

²A distinction needs to be made between privacy concerns in the context of commercial transactions on the Internet and privacy concerns in the context of personal safety of children and others in connection with criminal acts using the Internet. This Working Paper does not attempt to address the concerns regarding personal safety. Regulation in that respect must address the circumstances under which Internet users willingly disclose personal information about themselves in conversations with those engaged in criminal behavior. Such concerns should not be confused with the concerns regarding commercial use of consumer information. It is entirely unjustified to combine the two concerns as one, despite the desires of some to do so. Such combination only serves to feed unfounded paranoia and unreasonably characterizes commercial users. A distinction needs to be made between privacy concerns in the context of commercial transactions on the Internet and privacy concerns in the context of personal safety of children and others in connection with criminal acts using the Internet. This Working Paper does not attempt to address the concerns regarding personal safety. Regulation in that respect must address the circumstances under which Internet users willingly disclose personal information about themselves in conversations with those engaged in criminal behavior. Such concerns should not be confused with the concerns regarding commercial use of consumer information. It is entirely unjustified to combine the two concerns as one, despite the desires of some to do so. Such combination only serves to feed unfounded paranoia and unreasonably characterizes commercial users.

³See, e.g., Bloomberg News, Amazon.com Revises Privacy Policy on Consumer Concern, NYTimes.com (Sept. 1, 2000), available at <<http://www.nytimes.com/library/tech/00/09/biztech/articles/01amazon-privacy.html>>; Toysrus.com Accused of Privacy Violation, USA Today (Aug. 3, 2000), available at <<http://www.usatoday.com/life/cyber/tech/cti334.htm>>.

⁴S. 2928, 106th Cong. § 2 (2000), available at <<http://thomas.loc.gov/cgi-bin/bdquery/z?d106:5.02928:>>>.

⁵Senate, *Statements on Introduced Bills and Joint Resolutions (July 26, 2000)*, available at <<http://thomas.loc.gov/cgi-bin/query/D?r106:5./temp/wr106p18d0J:3110933>>.

specific guidelines on appropriate collection and use of demographic information. In addition, they argue that innovative protection for consumers will come from the business community in the form of software designed to empower the consumer to decide what he or she will allow marketers to know. Finally, they argue that regulation at this early stage of the Internet's development will only serve to dilute the ultimate value of the new media for both consumers and marketers.

There are no simple answers to the questions posed in this debate. One reality, however, is evident. The abuses of privacy on the Internet appear to be de minimis when compared to the huge volume of transactions that occur online every day.⁶ The concerns that seem to have gripped consumers and legislators, justified or not, appear to be based mostly upon anecdotal evidence insufficient to justify aggressive legislation or regulation.

After analysis of the issues and the current state of affairs, this WORKING PAPER concludes that legislators and regulators need to be a bit more circumspect in their approach to privacy. The Internet has the potential to deliver goods and services with unprecedented efficiency, offering opportunities for businesses and consumers beyond anything experienced in the past. Legislators and advocates need to educate, not regulate, and allow the marketplace time to address consumer concerns in a reasoned environment.

⁶Approximately \$400 billion in e-commerce sales will occur worldwide in 2000. See Privacy... A Weak Link in the Cyber-Chain, Price WaterHouse Coopers. However, 48% of online retailers do not track consumer information online and of those who do track user information only 40% actually use it. See Kevin G. Coleman, Chief Strategist, iPlanet Netscape, Privacy and the Global Digital Economy, Global Privacy Summit (2000).

At this stage, self-regulation, coupled with developing technology addressing consumer concerns about privacy, offer the most effective approach to curb online privacy abuses while supporting the robust growth of the Internet.

I. THE CURRENT STATE OF AFFAIRS

At present, there is no legislation in the United States that generally governs the collection, transmission and use of personal information concerning adults on the Internet.⁷ Despite the lack of specific legislation, however, an individual's privacy on the Internet has not gone unprotected. Violations of privacy in the online area have been addressed by existing legislation governing communications and unfair trade practices.⁸ In addition, self-regulation and competitive market forces have attempted to balance privacy concerns with the fast pace and accessibility of the online market.⁹ The advertising and marketing industries have embraced privacy concerns by maintaining self-regulatory limitations on the use of demographic data on consumers, thus going further than the industry has ever before gone.¹⁰

⁷Congress has passed legislation governing the collection, transmission and use of personal information on the Internet from children under 13. Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. §§ 6501 et seq.

⁸A detailed review of these cases appears later in this paper.

⁹Several organizations have issued self-regulatory guidelines for industry members to follow. For example, the Direct Marketing Association ("DMA") Committee on Ethical Business Practice investigates complaints against its members for failing to follow its Privacy Compliance Guide, available at <<http://www.the-dma.org/library/privacy/privacypromise.shtml>>. The Coalition for Advertising Supported Information and Entertainment ("CASIE") has also formulated Goals for Privacy to serve as a framework for marketers to address consumers' privacy as the virtual marketplace grows. The CASIE Privacy Goals are available at <<http://www.casie.org/goals.htm>>. Numerous companies, such as Clicksure and Privista, have emerged to promote software privacy protection tools.

The Federal Trade Commission, however, has issued a number of reports criticizing the slow progress of self-regulation and requesting federal legislation.¹¹ State and federal legislators have responded with the adoption of special legislation to protect children and the introduction of numerous other bills to address the breadth of privacy issues.¹² At the international level, the United States has negotiated with the European Union, agreeing to unprecedented limitations on the use of consumers' demographic information.¹³

¹⁰The Direct Marketing Association and the Privacy Leadership Initiative will fund a campaign to educate consumers about the positive uses by marketers of consumer information collected online. The Global Business Dialogue on E-Commerce (the "GBDE"), a group of 72 corporations, has also exceeded the expectations traditionally associated with self-regulation. The GBDE has proposed global privacy guidelines requiring Internet vendors to post clear privacy notices providing customers with an opportunity also to not have their personal information disclosed. Additional information about these guidelines is available at <<http://www.gbd.org>>. Major industry players have created a new position in their corporate structure, the privacy officer, to oversee the company's privacy practices. For instance, DoubleClick hired a former New York City commissioner of consumer affairs to act as its Chief Privacy Officer. See D. Eviator, Wanted: Chief Privacy Officer, Law.com (Sept. 19, 2000).

¹¹ See Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress (May 2000), available at <<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>>; Online Profiling: A Federal Trade Commission Report to Congress Part I (June 2000), available at <<http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>>; and Online Profiling: A Federal Trade Commission Report to Congress Part II (July 2000), available at <<http://www.ftc.gov/os/2000/07/onlineprofiling.pdf>>.

¹²For example, the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 *et seq.*, was passed to govern the collection of information online from children under 13. The following bills regulating privacy on the Internet are currently pending in Congress: Consumer Privacy Protection Act, S. 2606, 106th Cong. § 2 (2000); Online Privacy Protection Act, S. 809, 106th Cong. § 1 (1999); Online Privacy Protection Act, H.R. 3560, 106th Cong. § 2 (2000); and Consumer Internet Privacy Enhancement Act, S. 2928, 106th Cong. § 2 (2000).

¹³On July 21, 2000, the U.S. Department of Commerce and the European Union issued the Safe Harbor Privacy Principles governing the transfer of personal data from the EU. The Safe Harbor Principles are available at <<http://www.export.gov/safeharbor/shprinciplesfinal.htm>>.

Regrettably, many privacy advocates and legislators fail to consider how online information collection benefits both the consumer and the marketer. Advertising provides a major revenue source on the Internet. Without paid advertising, access to Internet sites most likely would not be free.¹⁴ Furthermore, the use of digital marketing technologies, such as cookies, allows for effective “real-time” marketing and an enhanced understanding of the consumer. The technology of the Internet, coupled with detailed consumer information, allows marketers to better serve consumers by personalizing messages to each consumer’s specific interests and presenting consumers with the opportunity to instantly respond to marketing messages. Thus, the interactivity allows for a more efficient and interactive marketplace.¹⁵

Legislators and privacy advocates also fail to recognize a crucial part of the debate — the global reach and continuous growth of the Internet. There is a consensus that this new medium needs to be allowed time to grow. The advent of the Internet is tantamount to an entire sea change in how we communicate and receive goods and services. Furthermore, most experts agree

¹⁴Advertising on the Internet has almost entirely replaced the original financing model on the Internet, the subscription “pay as you go” model. See Daniel Jaffe, *Panel Discussion Mercer Law Review*, 51 MERCER L. REV. 861 (Spring 2000); *Business-to-Consumer Electronic Commerce Survey of Status and Issues*, Organization for Economic Co-operation and Development, available at <<http://www.oecd.org/dsti/sti/it/ec/prod/gd97219.htm>>. Keyword advertising essentially supports search engines. See *Trademark Practice in a Dynamic Economy*, 10 FORD. IP MEDIA & ENT. L.J. 331 (Winter 2000). By 2005, spending for online advertising is expected to be almost \$28 billion. See *Report on Global Advertising*, Reuters (June 18, 2000). In the third quarter of 2000, DoubleClick, the largest network advertising company, served 162 billion online ads globally. *DoubleClick Reports Profitable Quarter*, DoubleClick Press Release (Oct. 2000).

¹⁵The Internet makes it faster to collect consumer information, enabling the marketer to personalize the consumer’s Web experience. See Richy Glassberg, *Don’t Fear the Cookie*, ADWEEK (Oct. 2, 2000).

that regulation of the Internet is a complicated matter given its global reach, and that a country's borders largely limit effective legislation.¹⁶ Moreover, the Internet itself has not fully matured, thus making it difficult to establish a privacy model for the United States, much less one for the world. Technological advancements are progressing at a much faster pace than that with which legislation would be able to maintain.

Finally, the Internet affords entrepreneurs with an unprecedented ability to enter the marketplace. Unlike all conventional methods of product and service distribution, the Internet has a very low barrier to entry, i.e., the cost of effective entry into a market. Indeed, for less than \$1,000, a would-be Internet marketer can establish a Web site and begin taking orders. Legislation and regulation have the tendency to increase barriers to entry and discourage marketplace competition at the entrepreneurial level. Regulation can even push established marketers out of a business sector.¹⁷ Witness the decision of a number of Web marketers to shut down sections of their Web sites that offered goods and services to children, citing vaguely written federal legislation and

¹⁶Usage of the Internet in the United States does not operate in a vacuum. There are approximately 300 million online users worldwide, however, the United States does not have the greatest percentage of online users. In addition, more Web sites are operated in Japan and the United Kingdom than the United States. These statistics are evidence that privacy issue is not limited to the United States, rather it is a global issue that requires a global solution. See Kevin G. Coleman, Chief Strategist, iPlanet Netscape, *Privacy and the Global Digital Economy*, Global Privacy Summit (2000).

¹⁷The Dallas Federal Reserve Bank's 1998 Report, states, "By making it cheaper to personalize during production, information age tools remove the last barriers to providing goods and services for individual customers." Declan MuCullagh, *Expert: Go Easy on Privacy Regs* (Sept. 19, 2000), available at <<http://www.wired.com/news/politics/0,1283,38893,00.html>> .

their inability to comply despite the best of intentions.¹⁸

II. THE COLLECTION OF CONSUMER INFORMATION AND ITS APPLICATION ON THE INTERNET

For years, it has been standard practice in the direct marketing industry to buy and sell detailed consumer databases.¹⁹ Retailers purchase lists based on highly detailed categories to insure that they are marketing to their target consumers. With the invention of the Internet and its technologies, specialized consumer information is even more readily accessible and detailed. Yet, consumer advocates and regulators have voiced concerns that online marketing practices such as monitoring surfing patterns, restricting access to Web sites unless the user provides personal information in the dialog box, and spamming consumers' in-boxes, invade consumer privacy.²⁰ They argue that massive amounts of personal data can be collected through a keystroke, often without

¹⁸Recently, Disney.com decided to prohibit access to unmoderated chat rooms to children under 13. See Evan Hansen, *Disney Locks Children Out of Some Chat Rooms*, News.com (Oct. 11, 2000). Zeeks.com ceased operating its chat room and e-mail features due to the difficulty of these areas complying with the COPPA requirements. See Lisa Vaas, *Customer Privacy Lockdown*, EWeek (Oct. 17, 2000).

¹⁹Information vendors, such as Hart, Hanks and Acxiom, collect personal information from various sources, such as sweepstakes entries and questionnaires, combine the information, and resell it to companies such as retailers and telemarketers. See *Selling is Getting Personal*, CONSUMER REPORTS (Nov. 2000).

²⁰The opposition to creating an online profile came to the forefront of many privacy advocates' agendas when the FTC initiated an investigation against DoubleClick when it began to combine online consumer profiles with personal data from other sources. See *Network Advertising Initiative: Principles not Privacy*, Electronic Privacy Information Center (July 2000), available at <http://www.epic.org/privacy/internet/NAI_analysis.html>.

the user's knowledge.²¹ Consumer advocates fear that this collection of data, if left unregulated, could even lead to discriminatory practices such as Weblining, i.e., the exclusion of certain consumers from high-end online marketing.²²

By contrast, at least one recent report argues that businesses will be more likely than the government to safeguard consumers' privacy from abuse.²³ A recent study found that thirteen government agencies are secretly tracking

²¹Many privacy commentators state that the most significant concern with online profiling is the consumer's lack of knowledge. See *Online Profiling: A Federal Trade Commission Report to Congress Part I* (June 2000), available at <<http://www.ftc.gov/os/2000/07/online-profilingreportjune2000.pdf>>. In addition, privacy advocates are concerned with the ability of online marketing companies, such as DoubleClick, to create profiles of Web users with whom they have no relationship. See *Network Advertising Initiative: Principles not Privacy*, Electronic Privacy Information Center (July 2000), available at <http://www.epic.org/privacy/internet/NAI_analysis.html>.

²²Marcia Stepanek, *Weblining*, Bus. Wk. (Apr. 3, 2000). The Center for Democracy and Technology commented at the Electronic Frontier Foundation that profiling gives companies the ability to base pricing upon consumer profiles. See *Online Profiling: A Federal Trade Commission Report to Congress Part I* (June 2000), available as <<http://www.ftc.gov/os/2000/07/onlineprofilingreportJune2000.pdf>>.

²³The report published by Privacilla.org, a newly-established online libertarian organization, makes the following observations:

Businesses . . . have a fundamental interest in protecting their relationships with customers. A business that . . . unwittingly reveals personal information about consumers to others is wasting its own assets, driving down future revenues, and violating its duties to stockholders. . . . [Moreover,] a business that offends customers with its use of personal information spoils its relationship with them.

In short, businesses take and hold consumer information with an obligation to treat that information carefully, with sensitivity and tact. Consumers and investors will penalize them heavily, taking dollars out of their bottom lines and market capitalizations, if they do not.

Privacilla.org, *Assessing Threats to Privacy: The Government Sector - Greatest Menace to Privacy By Far* (Sept. 2000), available at <<http://www.privacilla.org>>.

users' habits on their Web sites, presumably to better perform the tasks assigned to them.²⁴ Furthermore, there is no overwhelming public demand for the enactment of privacy legislation governing the commercial use of customer data collected online. Consumer polls regarding consumer demand have yielded inconclusive results.²⁵ While some surveys show that when given the choice, consumers will choose that their information be kept private, it is unclear how many consumers are concerned about online privacy absent the request to make such a choice.

Well-respected scholars on privacy law believe that privacy advocates have exaggerated the ramifications of collecting data online. For instance, Richard Epstein, a University of Chicago law professor, recently commented, "There is in cyberspace a Cassandra movement out there that sees in this the death of civilization . . . I just don't think most people care about [privacy] to the extent that the privacy mavens do."²⁶

Although the collection of personal information online may not always be in a form as obvious to the user as registration pages and surveys, many traditional marketing practices also collect and use information without giving

²⁴See *Most Federal Sites Fail Privacy Test*, MSNBC (Sept. 12, 2000) available at <<http://www.msnbc.com/news/458591.asp>>.

²⁵A recent UCLA Center for Communication Policy Study found that 63.6% of US users felt that logging onto the Internet put their privacy at risk. See Jim Wolf, *Data Privacy Fears Haunt Internet, Study Shows*, Reuters (Oct. 25, 2000). Despite surveys reporting that Internet users are overwhelmingly concerned about privacy violations on the Internet, a study by Andersen Consulting Institute for Strategic Change and the Owen School of Business at Vanderbilt University found that almost two thirds of Web surfers have submitted hugely personal information on the Internet. See *Survey Finds People Willing to Give Info Online*, Reuters (Sept. 13, 2000).

²⁶Declan MuCullagh, *Expert: Go Easy on Privacy Regs*, WIRED (Sept. 19, 2000), available at <<http://www.wired.com/news/politics/0,1283,38893,00.html>>.

notice to consumers. Whenever consumers use their credit card, respond to a direct mail campaign, or use a check-cashing card at their grocery store, data is collected. Quite often, this data is then sold to others with the intention of targeting offers to certain consumers based upon preferences exhibited by the consumers' behavior. Such activities have existed in one form or another for decades.

Internet technology now allows for the collection of personal information without first informing the user. For instance, cookies and Web bugs involve the invisible recording of online behavior for the purpose of formulating a profile or representation of users' habits and interests. Cookies are small text files that Web sites create and store on users' hard drives. A Web site's server may write cookies and read existing cookies that the Web site has previously placed on a user's computer.

Cookies vary in their duration. Whereas "session cookies" expire after the user's Internet session ends, "persistent cookies" are stored on a user's hard drive and may be retrieved during future browsing sessions by the Web site that installed the cookies. Cookies can store a variety of information, including personal information or a unique identifier that tracks a user's browsing behavior. A third party, such as an advertiser, may also place its own cookies on a user's computer while the user is browsing a Web site. If, for example, a user's browser is directed to retrieve an advertisement from a third party's server, that third party can then drop a cookie on the user's hard drive.

Web bugs, also known as "pixel tags," "clear GIFs," and "invisible GIFs," are invisible tracking devices embedded in the source code of Web pages which allow third parties to track consumers' browsing behavior. Web bugs send back to the server information about a user, such as the Internet Protocol address of the user's computer and the identification number of any

cookies the server previously dropped on the user's hard drive. Web bugs can also transmit to the Web site information about the particular products or services that an individual user was viewing on that Web page, as well as which sites the user visited prior to accessing that Web site. Like banner advertisements, Web bugs facilitate interaction between the advertiser's server and the user's browser, but the graphic files requested by Web bugs remain invisible to the user.

In combination, cookies and Web bugs enable Internet marketers to create a profile of a given consumer. This process has created much objection among privacy advocates, who fear that such activities are too intrusive, particularly because the consumer is largely unaware of the information gathering activity.²⁷ In reality, however, creation of a profile through the use of demographic and behavioral information about consumers has been a constant in the marketing industry. Use of such information has been central to many marketers' decisions about products and services introduced in the marketplace and improvements in those products and services offered. The concepts behind cookies and Web bugs are not new to the marketing world. The digital mechanisms used online are simply new and improved ways in which the innovative marketer can implement well-established marketing procedures. In the end, the information is used to make the marketplace more efficient. Admittedly, there may have been abuses in the past that warranted regulatory

²⁷Shortly after the FTC initiated an investigation against DoubleClick, a poll measuring consumers' reaction to online profiling was conducted by Business Week/Harris. The poll found that 35% of those polled were "not at all comfortable" with anonymous profiling and 28% of those polled "were not very comfortable." See *A Growing Threat*, Business Week/Harris Poll (Mar. 20, 2000).

scrutiny.²⁸ This practice, however, clearly creates a more responsive and efficient marketplace.

Despite the non-obvious nature of cookies and Web bugs, numerous tools exist that can be installed to detect and block the dropping of these tracking devices.²⁹ Furthermore, unlike in many forms of traditional marketing, consumers are given a choice regarding the collection of their information online. Although some Web sites may not engage in fair information collection practices, many sites provide the user with choices regarding the collection of personal information. For instance, the “opt-in” approach adopted by some marketers precludes the Web site operator from collecting or using a user’s personal information absent that consumer’s prior consent.³⁰ By contrast, the “opt-out” approach, adopted by most Web site operators that have addressed the issue, provides a broad default, allowing Web site operators to collect or use information about consumers unless a particular consumer decides to take affirmative steps to contact the Web site to have his or her name removed from the list.

²⁸Federal legislation exists restricting the use of information derived from credit reporting agencies and banks. See Fair Credit Reporting Act, 15 U.S.C. § 6801 *et seq.* (1999).

²⁹Web users can install various programs to block unwanted advertising, delete cookies and cache files and detect Web cookies. A list of some of these software tools is available at <<http://privacy.net/software/>>.

³⁰The privacy guidelines by the Internet Advertising Bureau (“IAB”) urge organizations to provide an “opt-in” to users regarding the collection and redistribution of especially sensitive information, such as medical or financial information. The IAB Privacy Guidelines are available at <<http://www.iab.net/privacy>>.

³¹TRUSTe, a privacy seal organization, suggests the following opt-out language:

“Our users are given the opportunity to ‘opt-out’ of having their

³¹ More importantly, many Web sites use cookies and Web bugs solely for the purpose of speeding up the consumer's surfing time on their Web site and do not sell the data to third parties.³²

III. THE PROGRESS OF SELF-REGULATION

The Federal Trade Commission ("FTC") traditionally has favored self-regulation of the online industry and in 1998 issued the Fair Information Practice Principles (the "Principles"), summarizing widely accepted principles concerning the collection and use of personal information online.³³

The Principles are as follows:

- **Notice:** Online marketers must post their privacy policies;
- **Choice:** Consumers must be able to "opt-out" of disclosures;
- **Access:** Individuals must have "reasonable access" to their information provided to online marketers; and
- **Security:** Online marketers must adequately secure the collected information.

information used for purposes not directly related to our site at the point where we ask for the information. For example, our order form has an 'opt-out' mechanism so users who buy a product from us, but don't want any marketing material, can keep their email address off of our lists.

Users who no longer wish to receive our newsletter or promotional materials from our partners may opt-out of receiving these communications by replying to unsubscribe in the subject line in the email or email us at support@thisweb site.com."

³²One survey has found that only 40% of Web sites that track user information actually use such information. See Kevin G. Coleman, Chief Strategist, iPlanet Netscape, *Privacy and the Global Digital Economy*, Global Privacy Summit (2000).

³³<<http://www.ftc.gov/reports/privacy3/priv-23.htm>>.

The Online Privacy Alliance,³⁴ the Direct Marketing Association,³⁵ the Internet Alliance (formerly the Interactive Services Association),³⁶ TRUSTe,³⁷ and BBB Online³⁸ have developed suggested privacy guidelines. These guidelines generally require Web sites to disclose: (1) the fact that personal information is being collected; (2) the type of information being collected; (3) the intended use of the information; and (4) the extent to which such information may be shared with third parties. The guidelines also suggest that visitors should be given the option to limit the disclosure or resale of such information either through an "opt-in" or "opt-out" procedure and be provided with a mechanism to correct any inaccurate or incomplete personal information. In July 2000, the Federal Trade Commission and the Network Advertising Initiative, a collective body of Internet advertisers, reached an agreement regarding the online collection of consumer information.³⁹ Under the agreement, Web users will be explicitly informed about advertisers' attempts to profile potential consumers and Web users will be given the option of not participating.

³⁴The Online Privacy Alliance's Guidelines for Online Privacy Policies, available at <<http://privacyalliance.org/resources/ppguidelines.shtml>>.

³⁵The DMA's Marketing Online Privacy Principles and Guidances, available at <<http://www.the-dma.org/library/guidelines/onlineguidelines.shtml>>.

³⁶Principles on Notice and Choice Procedures for Online Information Collection and Distribution by Online Operators, available at <http://www.internetalliance.org/policy/privacy_guidelines_online.html>.

³⁷TRUSTe Program Principles, available at <http://www.truste.org/webpublishers/pub_principles.html>.

³⁸Better Business Bureau BBBonline Code of Online Business Practices, available at <<http://www.bbbonline.org/code/code.asp>>.

³⁹<<http://www.ftc.gov/OS/2000/07/onlineprofiling.htm>>.

In addition to the self-regulatory guidelines, the industry has developed privacy protection tools. In June 2000, industry members unveiled a technology called Platform for Privacy Preferences (“P3P”), which alerts computer users as to the level of privacy protection provided on a particular Web site before they visit that site.⁴⁰ P3P sets standards that will automatically allow browsers to read the privacy policies on participating Web sites. The browser will only go to sites that follow the preferences pre-selected by the user. The user can then decide whether he or she would like to enter a site that does not provide the level of privacy protection desired. For this technology to work, however, each Web site on the Internet must adopt it. Most of the companies involved in this project already have privacy policies that can be read by P3P-enabled software.

The utilization of technological solutions, such as P3P, and compliance with posted privacy policies are viable competitive tools in the online marketplace. Consumers can choose which Web sites to visit. If a consumer does not want his or her information shared, he or she has the choice to deal only with Web sites that will not share personal information. If a consumer, however, wishes to have personal information distributed so that he or she may receive targeted advertising, the consumer can decide whether to deal with a Web site employing such practices.

IV. THE FEDERAL TRADE COMMISSION REVERSAL

Surprisingly, the Federal Trade Commission abandoned its initial position

⁴⁰ <<http://www.w3.org/p3p/>>.

supporting self-regulation. In May 2000, in a 200 page report entitled "Privacy Online: Fair Information Practices in the Electronic Marketplace," the FTC released findings that "only" twenty percent of Web sites complied with the Principles outlined above.⁴¹ Based on these findings, the Commission recommended that Congress adopt strict Internet privacy protection regulations, which are based on the Principles.

The Federal Trade Commission's focus on the minimal Web site compliance rate, however, may have been misplaced. An eighty percent non-compliance rate does not necessarily equate to an eighty percent consumer injury rate. More importantly, the FTC report lacks any quantified evidence of consumer injury to justify the need for legislative intervention.⁴²

V. FIRST AMENDMENT CONSIDERATIONS

Lurking in the background of the privacy debate is the First Amendment and the protection it affords marketers and their commercial speech. Developments on the Internet have highlighted the need for balancing online marketers' constitutional rights under the First Amendment with consumers' interests.

⁴¹Privacy Online: Fair Information Practices in the Electronic Marketplace, available at <<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>>.

⁴²In this respect, it is most interesting to contrast the vociferous dissent to legislation led by Federal Trade Commission Commissioner Orson Swindle. From the outset of the debate and FTC reports, Commissioner Swindle has advocated more time be given to the development of self-regulation. See, e.g., *Self-Regulation and Privacy Online, A Report to Congress*, available at <<http://www.ftc.gov/os/1999/9907/privacy99.pdf>>; *Privacy Online: A Report to Congress*, available at <<http://www.ftc.gov/reports/privacy3/toc.htm>>; *An FTC Commissioner Looks at Internet Privacy*, Privacy in America Business Conference (1999), available at <<http://www.ftc.gov/speeches/swindle/westin.htm>>.

43 Although no cases to date have focused specifically on the collection of personal information regarding consumers in general, a recent case challenging the Federal Communication Commission's ("FCC") interpretation of the Telecommunications Act of 1996 ("TCA")⁴⁴ may serve as a gauge signaling the treatment of constitutional issues surrounding the online privacy debate.

In *U.S. West, Inc. v. Federal Communications Commission*,⁴⁵ the Court of Appeals for the Tenth Circuit vacated an Order and Regulations (collectively, the "Order") promulgated by the FCC pursuant to Section 222, "Privacy of consumer information,"⁴⁶ of the TCA. The FCC issued the Order restricting the use of, disclosure of, and access to customer proprietary network information ("CPNI"), such as information on the use patterns and bills of customers, for the purpose of marketing services to which the customer did not already subscribe absent a customer's prior approval. For example, if a customer subscribed to a carrier's long distance service, the carrier could not market its

⁴³For example, the Supreme Court held the Communications Decency Act of 1996, 47 U.S.C. § 223 (1996), which criminalized the publication of "indecent" and "patently offensive" material on the Internet unless the site screened for minors, to be unconstitutional. See *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997), available at <http://www2.epic.org/cda/cda_decision.html>. In addition, the United States Court for the Third Circuit recently found the Child Online Protection Act ("COPA"), 47 U.S.C. § 231 (1998), which established community standards to determine whether material transmitted via the Internet was considered "harmful to minors," to be unconstitutional. See *American Civil Liberties Union v. Reno*, 217 F.3d 162 (2000), available at <http://www.epic.org/free_speech/copa/3d_cir_opinion.html>.

⁴⁴47 U.S.C. § 222(a) (1999).

⁴⁵182 F.3d 1224 (10th Cir. 1999), *cert. denied sub nom.*, *Competition Policy Inst. v. U.S. West, Inc.*, 120 S. Ct. 2215 (2000).

⁴⁶Specifically, Section 222 imposes a duty on telecommunications carriers to "protect the confidentiality of proprietary information of, and relating to . . . customers." *U.S. West, Inc.*, 182 F.3d at 1227 (quoting the TCA, 47 U.S.C. § 222(a)).

cellular service to that customer without prior consent. The Order also imposed an “opt-in” requirement for consent, under which a carrier must obtain prior express approval from a customer through written, oral or electronic means.

In vacating the Order on constitutional grounds, the court held that the FCC’s Order was not properly tailored to justify its restriction on commercial free speech and, thus, violated the telecommunications carriers’ right to free speech under the First Amendment. The court specifically criticized the FCC’s use of an “opt-in” approach, noting, “The FCC record does not adequately show that an opt-out strategy would not sufficiently protect consumer privacy.”⁴⁷ The court opined that the “FCC’s failure to consider an obvious and substantially less restrictive alternative, such as an opt-out strategy, indicates that it did not narrowly tailor [its Order] regarding customer approval.”⁴⁸ It also noted in dicta, “[a]lthough we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely.”⁴⁹

VI. PRIVACY LEGISLATION EFFORTS IN CONGRESS

Numerous bills have been proposed addressing privacy on the Internet. Identical bills entitled “Online Privacy Protection Act” were currently pending in committees in both houses of Congress at the end of its 106th session.

⁴⁷*U.S. West, Inc.*, 182 F.3d at 1239.

⁴⁸*U.S. West, Inc.*, 182 F.3d at 1238-39.

⁴⁹*U.S. West, Inc.*, 182 F.3d at 1235.

The Senate bill⁵⁰ was introduced in April 1999 and the House of Representatives bill⁵¹ was introduced in January 2000. Both bills require the Federal Trade Commission to establish regulations to protect the privacy of personal information collected on the Internet from individuals not covered by the Children's Online Privacy Protection Act of 1998 ("COPPA")⁵² and to provide the individual greater control over the collection and use of that information.

On July 26, 2000, Senator McCain introduced the Consumer Internet Privacy Enhancement Act in an effort to create enforceable standards for Web site operators regarding the online collection and use of consumer's personal information.⁵³ The Act would essentially codify the "Four Fair Information Practices" currently recognized by the Federal Trade Commission and various seal programs.⁵⁴ Under the Act, commercial

⁵⁰S. 809, 106th Cong. § 1 (1999), available at <<http://thomas.loc.gov/cgi-bin/bdquery/z?d106:s.00809>>.

⁵¹H.R. 3560, 106th Cong. § 2 (2000), available at <<http://thomas.loc.gov/cgi-bin/bdquery/z?d106:h.r.03560>>.

⁵²15 U.S.C. §6501 *et seq.* (1998), available at <<http://www.cdt.org/legislation/105th/privacy/coppa.html>>. In general, COPPA requires any operator of a Web site or online service directed or targeted to children that collects, or has actual knowledge that it is collecting, personal information (name, physical and e-mail address, telephone number, social security number) from children under 13, to provide notice on the Web site about what information is collected, how the operator uses such information, and the operator's disclosure practices for such information. Except for a few limited exceptions, the Rule requires operators to obtain verifiable parental consent before collecting information from children under 13.

⁵³S. 2928, 106th Cong. § 2 (2000), available at <<http://thomas.loc.gov/cgi-bin/bdquery/z?d106:s.02928>>.

⁵⁴*See, e.g.,* TRUSTe, available at <<http://truste.org>>, BBBOnline, available at <<http://www.bbbonline.org>>.

Web site operators would be prohibited from collecting personally identifiable information from a user of their Web site, unless the operator provides the user with (1) adequate notice regarding the information collection practices of the site and (2) an opportunity to limit the use or disclosure of personally identifiable information for purposes other than fulfilling the products and services offered on the site or as required by law. Violations of the Act would be treated as an unfair or deceptive trade practice and would be actionable by the Federal Trade Commission.

In addition, enforcement actions could also be brought by numerous other agencies such as The National Credit Union, the Secretary of Transportation, and state attorneys general. The Act also provides for the creation of safe harbor programs. Under these safe harbor programs a Web site operator who complies with self-regulatory guidelines issued by a seal program or industry members and approved by the Federal Trade Commission will be protected.

The Consumer Privacy Protection Act was introduced in the Senate in June 2000.⁵⁵ The proposed legislation would require commercial Web sites to notify consumers as to what information is collected about them and how it is used. It would also permit consumers to choose whether this data can be used, give consumers access to the data, and make sure the information is secure.

VII. THE EUROPEAN DIRECTIVE AND ITS SAFE HARBORS

The European Union Data Protection Directive (the "Directive"), which took effect in 1998, mandates certain minimum standards for, among other things, the collection, disclosure, and transmission of personal data.⁵⁶

⁵⁵S. 2606, 106th Cong. § 2 (2000), available at <<http://thomas.loc.gov/cgi-bin/bdquery/z?d106:s.02606:>>.

It was implemented through legislation passed in each member state of the European Union. This Directive will restrict the flow of personal data not only within the European Union, but also from member states to countries outside the European Union. Furthermore, the Directive prohibits the transmission of personal data to non-European Union countries deemed by the European Commission to have inadequate levels of protection for personal data.⁵⁷

Although the United States has enacted national legislation restricting the disclosure of certain limited types of information,⁵⁸ the European Union felt

⁵⁶Directive 95/46/EC, Official Journal of the European Communities of 23 November 1995 No. L281 p. 31. The European Union Data Protection Directive can be viewed online at <<http://www.privacy.org/pi/intl-orgs/ec/eudp.html>> and <<http://www.cdt.org/privacy/eudirective/eu-directive-.html>>.

⁵⁷Viewed as a middle ground in the debate over the protection of personal information, Canada enacted the Personal Information Protection and Electronic Documents Act, S.C., ch. 5 (2000) (can.), available at <http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/c-6/c-6_4/90052bE.html>. This law requires certain organizations to develop and implement required policies and procedures and, more importantly, to cease using personal consumer data which has not been collected with the consent required under the new law for disclosure to marketing partners, third parties, or the organizations' own marketing purposes. Phase 1, effective January 1, 2001, applies this new law to federal works, undertakings or businesses and those who disclose personal data to parties outside of their province for consideration. Phase 2, which covers all other organizations, will go into effect on January 1, 2004. Although this law does not apply directly to foreign companies, in many instances foreign companies will have to comply in order to do business with Canadians.

⁵⁸Internet-oriented privacy legislation includes the Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. §§6501 et seq. (1998) (regulates the collection of personal information by commercial Web sites which are directed towards, or knowingly collect information from, children under 13) and the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et. seq. (1999) (requires a financial institution to disclose its privacy policies and practices to its customer, prohibits the disclosure of its customer's non-public personal information to non-affiliated third parties unless certain requirements are met, and requires it safeguard customer records and information). Privacy concerns are not, however, a new issue for Congress. Over the years Congress has enacted a number of privacy statutes to protect particular types of data. For example Congress has enacted the following laws: in 1970, the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq. (1999) (enumerates permissible purposes for which a credit reporting agency may release personal information about a consumer without his or her permission); in 1984, the Cable Communications Policy Act, 47 U.S.C. § 551 (1994) (requires cable television companies to annually notify subscribers about the use and disclosure of their personal information as well as prohibits cable television companies from collecting or disclosing subscribers' personal information for purposes unrelated to providing cable services without their permission); in 1986, the Electronic Communications Privacy Act, 18 U.S.C. § 2702 (1998) (prohibits the unauthorized recording and collection of the contents of telephone conversations, data transmissions and e-mail messages); in 1988, the Video Privacy Protection Act, 18 U.S.C. §

United States privacy protections did not meet the standards required by the Directive. After much negotiation, United States and European Union officials developed safe harbor principles to overcome the United States' perceived lack of adequate privacy protection legislation in July 2000.⁵⁹ Compliance with the safe harbor provisions is voluntary. A non-European Union company adhering to these safe harbor principles will be deemed to be in compliance with the Directive.

The safe harbor principles include:

- **Notice:** Clear and conspicuous notice available when an individual is first asked for personal information explaining what type of information will be collected, how it will be collected and used, and options for limiting its use and disclosure.
- **Choice:** Clear and conspicuous opt-out choice.
- **Onward Transfer:** Choice of whether and how a third party may use the personal information. When transferring information to a third party, the company must require that the third party provide at least the same level of privacy protection as the individual originally chose.

2710 (1996) (prohibits video stores from disclosing specific information about customers' video selections unless the customer opts-in to such disclosures); in 1994, the Driver's Privacy Protection Act, 18 U.S.C. § 2721 et seq. (2000) (requires states to get individuals permission prior to selling Department of Motor Vehicles records); and in 1996, the Telecommunications Act, 47 U.S.C. § 251 et seq. (1999) (prohibits telephone companies from selling call records without consent).

⁵⁹The Safe Harbor Principles are available at <<http://www.export.gov/safeharbor/shprinciplesfinal.htm>>.

- **Security:** Reasonable measures to protect personal information from loss, misuses, unauthorized access or disclosure, alteration, or destruction.
- **Data Integrity:** Personal information should be accurate, complete and current and only that which is relevant to the purposes for which it was gathered should be retained.
- **Access:** Individuals must have reasonable access to their own records and the ability to correct errors.
- **Enforcement:** Mechanisms to assure compliance with these principles, recourse for individuals, and consequences where not followed.

VIII. THE MARKETPLACE REALITY AND ITS RESPONSE UNDER CURRENT LAW

Marketing practices on the Internet, such as “spamming” and online profiling, are similar to those practices in more traditional forms of marketing. Both concern the collection, distribution and use of consumers’ personal information for a commercial purpose. In contrast to the current outcry for legislation governing the collection and use of personally identifiable information on the Internet, the same practices in traditional commercial media have been predominantly addressed by industry self-regulation.⁶⁰ However, privacy

⁶⁰Although telemarketers have a duty under the Telecommunications Act to treat customer lists as proprietary and confidential information, no similar legal duty is imposed on direct marketing. The Direct Marketing Association (“DMA”), however, has promulgated guidelines concerning the use, transfer and sale of consumers’ personal information that its members voluntarily agree to follow. These guidelines require that consumers be notified if such data might be sold or transferred for marketing purposes and be given an opportunity to opt-out of such disclosures. Furthermore, sensitive data for which consumers have a reasonable expectation of privacy is not to be disclosed. The DMA’s guidelines are available at <<http://www.the-dma.org/library/guidelines/index.shtml>>. In addition, the DMA maintains a centralized database of consumers who want their names removed from all direct marketing lists.

advocates and some legislators believe that due to the nature of the Internet, the occurrence of these well-established marketing practices on the Internet demands legislative intervention.

With the exception of COPPA, there is currently no law explicitly barring or otherwise regulating the collection of personal information on the Internet or the re-use or sale of such information. Despite numerous bills proposed in Congress,⁶¹ federal law has not yet recognized an inherent right to privacy on the Internet. Therefore, consumers complaining of electronic privacy invasions have based their claims on traditional common law tort principles, such as trespass and the unreasonable intrusion upon the seclusion of another, and unfair trade practices. Likewise, the Federal Trade Commission has applied existing federal laws to restrict the transmission of unwanted and invasive commercial e-mails and the use and collection of personal information on the Internet for marketing purposes.

The final section of this WORKING PAPER reviews federal and state actions that address privacy abuse. While it is not certain that every known case has been included in this discussion, those that have been included are a representative example of the cases that have been brought and the results that have been achieved.

⁶¹For example: Consumer Online Privacy and Disclosure Act, H.R. 5430, 106th Cong. §2 (2000), available at <<http://thomas.loc.gov/cgi-bin/bdquery/z?d106:h.r.05430>>; Privacy Commission Act, H.R. 4049, 106th Cong. § 2 (2000), available at <<http://thomas.loc.gov/cgi-bin/bdquery/z?d106:h.r.04049>>; Enhancement of Privacy and Public Safety in Cyberspace Act, S. 3083, 106th Cong. § 2 (2000), available at <<http://thomas.loc.gov/cgi-bin/bdquery/z?d106:s.03083>>; and Online Privacy Protection Act of 2000, H.R. 3560, 106th Cong. § 2 (2000), available at <<http://thomas.loc.gov/cgi-bin/bdquery/z?d106:h.r.03560>>.

There are two critical conclusions that one can draw in reviewing the cases. First, the extent of privacy abuse has been minimal and is certainly not enough to justify the hype promoted by consumer advocates and politicians. Second, regulators and consumers have adequate recourse under present law to address the abuses that have occurred. There is no logical justification for additional legislation that may, in fact, stifle the growth of the Internet and cut off consumers from a more efficient and cost effective marketplace.

A. Federal Regulatory Actions

1. *In the Matter of GeoCities.*⁶² In August 1998, the Federal Trade Commission brought an action against GeoCities, a popular “virtual community” Web site operator, for misrepresenting the purposes for which it was collecting personally identifiable information from children and adults. FTC alleged that GeoCities’ misrepresentations violated Section 5 of the Federal Trade Commission Act, which prohibits generally unfair or deceptive trade practices. Under the settlement agreement, GeoCities agreed to clearly and prominently post on its site a privacy notice informing users what information is collected, how it is used and how users can access and delete their information.

2. *In the Matter of Liberty Financial Companies, Inc.*⁶³ In May 1999, the FTC entered into an agreement with Liberty Financial Companies, Inc. to settle allegations that the corporation had engaged in unfair or deceptive practices online. According to the Commission, the corporation had falsely represented

⁶²FTC File No. 982-3015 (1998), available at <<http://www.ftc.gov/os/1998/9908/geo-ord.htm>>.

that personal information collected from children on its Web site, www.younginvestor.com, would be maintained anonymously and that participants would receive an e-mail newsletter and various prizes. Liberty Financial allegedly maintained personal information about the child and family finances in an identifiable manner. In the settlement, Liberty Financial agreed to cease making representations about how personal information would be maintained, post a privacy policy on its children's sites, and obtain verifiable parental consent before collecting personal information from children.

3. *Federal Trade Commission v. Toysmart.com*.⁶⁴ In July 2000, the Federal Trade Commission entered into a consent agreement with Toysmart.com, LLC and Toysmart.com, Inc. (collectively, "Toysmart"), a failed Internet retailer of children's toys. The FTC filed its first-ever COPPA complaint against Toysmart in a Massachusetts federal court. The complaint alleged that the company gathered confidential, personal information from children in violation of COPPA. In addition, the complaint sought injunctive and declaratory relief to prevent the sale of customer information collected on Toysmart's Web site. The complaint alleged that such a sale would be in violation of the Toysmart privacy policy and thus, violate Section 5 of the Federal Trade Commission Act.

Toysmart's privacy policy stated that personal information would never be shared with third parties, but in the midst of financial turmoil, Toysmart began auctioning its customer database. The agreement settled allegations that Toysmart misrepresented to consumers that personal information would never be shared with third parties. However, in August 2000, a federal bankruptcy

⁶³FTC File No. 982-3522 (1999), available at <http://www.ftc.gov/os/1999/9905/1btyord.htm>.

judge thwarted the Commission's plan by rejecting its settlement agreement with Toysmart. The court held that the corporation could sell its most valuable and controversial asset, a personal customer information list, as a separate asset to a prospective buyer.

4. *Investigation of DoubleClick, Inc.*⁶⁵ In February 2000, the Federal Trade Commission launched a routine investigation of DoubleClick, Inc., the largest online advertising company. The FTC is currently determining whether DoubleClick has engaged in unfair or deceptive trade practices in violation of Section 5 of the Federal Trade Commission Act. The allegations were based upon DoubleClick's plan to combine information it retrieved from its users through cookies with a direct marketing database from its acquired direct marketing company. As a result, DoubleClick suspended its business plans in March 2000. Two days after the FTC initiated its investigation, the Electronic Privacy Information Center ("EPIC") filed a *Complaint and Request for Injunction, Request for Investigation and for Other Relief* with the Commission alleging that DoubleClick's decision to personally identify their customer profiles constitutes "unfair and deceptive" business practices. DoubleClick has also been the named defendant in several state lawsuits.

5. *Federal Trade Commission v. Rennert et al.*⁶⁶ In July 2000, the FTC settled numerous charges brought against several online pharmacies. In addition to charges that the Web sites made deceptive claims about the pharmaceutical products and services, the complaint alleged that the sites misrepresented the measures used to protect customer information and used

⁶⁴FTC File No. 002-3274 (2000), available at <<http://www.ftc.gov/os/2000/07/toysmartconsent.htm>>.

⁶⁵Statement by Jodie Bernstein, Director, Bureau of Consumer Protection, Federal Trade Commission, available at <<http://www.ftc.gov/opa/2000/02/dblclickstajb.htm>>.

such information for purposes contrary to those stated. The settlement requires these online pharmacies to implement reasonable procedures to protect the security of customer information. Furthermore, the defendants are prohibited from “selling, renting, leasing, transferring or disclosing personal information that was collected from their customers without express authorization from the customer.”

6. *Federal Trade Commission v. ReverseAuction.com, Inc.*⁶⁷ In January 2000, the Federal Trade Commission entered into a consent agreement with ReverseAuction.com, Inc. (“ReverseAuction”) to settle charges that the online auction house had violated consumers’ privacy by harvesting their personal information from a competitor’s site and then sending deceptive spam to those consumers to solicit business. In particular, ReverseAuction allegedly registered with its competitor, eBay, agreed to comply with eBay’s privacy policy, and then violated the policy by gathering and using eBay users’ personally identifiable information for unauthorized purposes, including spam.

Under the consent agreement, ReverseAuction has agreed not to engage in such practices in the future. Furthermore, ReverseAuction must delete the personal information of consumers who declined registration with the company upon receiving its spam. ReverseAuction must also provide those consumers who affirmatively responded to the spam with notice of the FTC’s charges and provide consumers with the option of canceling their registration and having their personal information expunged. The notice must indicate that eBay neither authorized nor knew of ReverseAuction’s dissemination of spam.

⁶⁶Settlement available at <<http://www.ftc.gov/os/2000/07/logstipmort.htm>>.

7. *United States v. Hambrick.*⁶⁸ In July 1999, the federal government filed criminal charges against the defendant who had allegedly attempted to entice a minor to run away with him during conversations in an online chat-room. The defendant had registered his personal information with Mindspring, an Internet Service Provider (the "ISP"), under the alias "Blowuinva." Pursuant to a state subpoena requesting user records for that alias, the ISP turned over evidence incriminating the defendant. The defendant filed a motion to suppress this evidence, arguing that the subpoena was invalid since it was not signed by a judicial officer with the matter pending before them or a grand jury and thus, was invalid.⁶⁹ The defendant asserted that under the Electronic Communications Privacy Act ("ECPA"),⁷⁰ his privacy was violated when the ISP provided the government with his records pursuant to an invalid subpoena.

The court held that the ECPA does not provide an individual with "a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection."⁷¹ The court denied the motion, finding that despite the invalidity of the subpoena, the ISP relied on a facially valid subpoena and could be found only civilly liable under the ECPA for revealing subscriber information to the government without first requiring a warrant, court order, or subpoena.

⁶⁷FTC File No. 002-3046 (2000), available at <<http://ftc.gov/os/2000/01/reverseconsent.htm>>.

⁶⁸55 F. Supp. 2d 504 (W.D. Va. 1999).

⁶⁹*Hambrick*, 55 F. Supp. 2d at 507.

⁷⁰18 U.S.C. § 2701 et seq. (1996).

⁷¹*Id.* at 506.

8. *United States v. Kennedy*.⁷² In January 2000, the federal government filed criminal charges against the defendant for the alleged intentional receipt of online child pornography. The defendant subscribed to Road Runner, a provider of high speed Internet services over cable wires. The government had obtained its evidence based on a court order directing Road Runner to disclose the plaintiff's subscriber information. Without obtaining the defendant's prior consent, Road Runner complied with the order. The defendant filed a motion to suppress the evidence, arguing that Road Runner had violated the Cable Communications Policy Act ("CCPA")⁷³, which requires the service provider to notify the subscriber before divulging information to the government. By contrast, there is no such requirement on service providers under the ECPA.⁷⁴ The court denied the defendant's motion, finding that the ECPA was controlling authority. Although the court declined to determine whether CCPA had been violated, it noted that "[t]raditionally, Internet providers have considered themselves subject to the . . . Electronic Communications Privacy Act."⁷⁵

B. State Regulatory Actions

1. *InfoBeat Inc.*⁷⁶ In January 2000, the New York State Attorney General

⁷²81 F. Supp. 2d 1103 (D. Kan. 2000).

⁷³47 U.S.C. § 551(f) (1992).

⁷⁴18 U.S.C. § 2701 et seq. (1996).

⁷⁵*Kennedy*, 81 F. Supp. 2d at 1111. The court declined to determine whether the government had violated the CCPA reasoning that even if such a violation had occurred, it would not affect the admissibility of evidence. The CCPA only provides a civil remedy, not an exclusionary remedy, for a violation.

entered into a settlement with InfoBeat Inc., a subsidiary of Sony Music, to settle charges that the Internet e-mail service provider had violated its own privacy policy. Contrary to the explicit terms of its privacy policy, InfoBeat disclosed to certain third party advertisers the e-mail addresses of those subscribers who hit on certain banner advertisements embedded in its online newsletters. InfoBeat attributes the privacy breaches to a software glitch, which has since been corrected.

2. Notices of Intended Actions. In June 2000, the Michigan State Attorney General filed Notices of Intended Action against a number of online retailers including Ortho Biotech, Inc. d/b/a www.procrit.com;⁷⁷ Stockpoint, Inc. d/b/a stockpoint.com;⁷⁸ AmericasBaby.Com, Inc. d/b/a/ www.babyfurniture.com, www.babygear.com, and www.AmericasBaby.com;⁷⁹ Intimate Friends Network Webpower, Inc., www.iFriends.Net,⁸⁰ and Searle, Inc. d/b/a/ www.searlehealthnet.com, searle.com and www.arthritisconnection.com.⁸¹ The online retailers allegedly have allowed DoubleClick, Inc., whose advertisements are embedded on their Web sites, to

⁷⁶*Infobeat Settlement Resolves Website Privacy Violation*, Press Release, Office of New York State Attorney General Eliot Spitzer, Jan. 25, 2000, available at <http://www.oag.state.ny.us/press/2000/jan/jan25c_00.html>.

⁷⁷*In the Matter of Ortho Biotech, Inc.*, AG File No. 20006841 (2000), available at <http://ag.state.mi.us/AGWebSite/consumer_and_business_info/nia_612_1.pdf>.

⁷⁸*In the Matter of Stockpoint, Inc.*, AG File No. 20006918 (2000), available at <http://ag.state.mi.us/AGWebSite/consumer_and_business_info/nia_612_3.pdf>.

⁷⁹*In the Matter of AmericasBaby.com, Inc.*, AG File No. 20006919 (2000), available at <http://ag.state.mi.us/AGWebSite/consumer_and_business_info/nia_612_2.pdf>.

⁸⁰*In the Matter of Intimate Friends Network and WebPower, Inc.*, AG File No. 20006920 (2000), available at <http://ag.state.mi.us/AGWebSite/consumer_and_business_info/nia_612_4.pdf>.

place cookies and Web bugs on the hard drives of visitors to those sites without the visitors' knowledge, in violation of their common law and state statutory rights to privacy. A Notice of Intended Action was also filed against DoubleClick, Inc. d/b/a www.doubleclick.net, www.NetDeals.com and www.IAF.net for failing to disclose that it was placing cookies on users' hard drives without their knowledge or consent.⁸² Each company was given ten days to correct certain online practices or else the Attorney General would file lawsuits alleging violations of the Michigan Consumer Protection Act.⁸³

3. *State of Texas v. Living.com.*⁸⁴ In September 2000, the Texas Attorney General's office filed a lawsuit to enjoin Living.com, a failed online furniture company, from selling its customer information. Within the hour, Living.com agreed to destroy its customers' personal financial data and the parties settled. Under the agreement, Living.com is allowed to sell customers' names and e-mail addresses after giving the customers notice and an opportunity to "opt-out" of the proposed sale. The settlement is subject to approval by a federal bankruptcy court.

C. Suits by Consumers

1. *Liu v. DeFelice d/b/a Investigative Services Company.*⁸⁵ In July 1998, the plaintiff, a Massachusetts resident, filed an invasion of privacy complaint

⁸¹*In the Matter of Searle, Inc.*, AG File No. 20009353 (2000).

⁸²*In the Matter of DoubleClick, Inc.*, AG File No. 20002052 (2000), available at <http://ag.state.mi.us/AGWebSite/consumer_and_business_info/dbleclck.pdf>.

⁸³All of the companies which received these Notices of Action are currently involved in ongoing discussions with the Attorney General's office. No lawsuits have yet been filed.

alleging that the defendant, a private investigator residing in New York, who had accessed her confidential credit information online in violation of the Federal Credit Reporting Act (“FCRA”)⁸⁶ and various Massachusetts consumer protection statutes. The defendant made his online request for the plaintiff’s information from a terminal in New York. Although the court ruled only on the due process issue of personal jurisdiction and found in favor of the plaintiff, it noted in dicta that the defendant’s online actions, if true, constitute “a statutorily defined invasion of privacy offense” under the FCRA.⁸⁷

2. *Stewart v. Yahoo! Inc.*⁸⁸ In April 2000, a Texas resident filed a complaint alleging that Yahoo! Inc., an Internet search portal company, and its subsidiary, Broadcast.com Inc., placed cookies on her computer to track her online surfing behavior in violation of a Texas’ anti-stalking law. Broadcast.com’s privacy policy indicated that it used cookies to research users’ demographics, interests, and behaviors on its Web site. The court is currently considering whether to grant class certification status to the plaintiff.

3. *Supnick v. Amazon.com and Alexa Internet.*⁸⁹ In May 2000, the plaintiff sought class action certification in a suit filed against Amazon.com (“Amazon”), a book and music Internet retailer, and Alexa Internet (“Alexa”), an Internet browser software company. Amazon distributed Alexa’s software, which was designed to provide statistics and monitor the Web sites and related links visited by its users. The plaintiff alleges that the software enables Alexa

⁸⁴ <<http://www.living.com>>.

⁸⁵ 6 F. Supp. 2d 106 (D. Mass. 1998).

and Amazon to intercept and access users' personal information in violation of the ECPA, the Stored Wire and Electronic Communications and Transactional Records Access Act,⁹⁰ and the common law rights against trespass to property and invasion of property. The court only addressed the issue of class certification, which it granted to the plaintiff. This case is currently pending.⁹¹

4. *John Doe a/k/a Aquacool 2000 v. Yahoo! Inc.*⁹² In May 2000, a lawsuit was filed against Yahoo! in a California federal court alleging constitutional and contractual privacy violations of a user who posted criticisms of his employer on a message board using a pseudonym. Yahoo! revealed the user's identity to his employer, without informing him, upon receipt of a subpoena from the employer. The user was later fired. This case is currently pending.⁹³

5. *Steinbeck v. Corematics, Inc. et al.*⁹⁴ In July 2000, a California resident filed a class action lawsuit in the Superior Court of California against Corematics, Inc., Toys R Us, Inc., and ToysRUs.com, Inc. (collectively, the "Defendants"). The plaintiff alleges that the Defendants committed a variety of offenses in operating the Web sites www.toysrus.com and

⁸⁶15 U.S.C. § 1681 (1970).

⁸⁷*Liu*, 6 F. Supp. 2d at 108.

⁸⁸Case No. 0001045 (Dallas Cty. Dist. Ct., filed Feb. 9, 2000).

⁸⁹No. C00-0221P, 2000 U.S. Dist. LEXIS 7073 (W.D. Wash. May 19, 2000).

⁹⁰18 U.S.C. § 2701 (1996).

⁹¹As of November 2000, the court granted both parties' requests to extend discovery. Docket available at

www.babiesrus.com. In particular, the Defendants purportedly surreptitiously placed cookies and Web bugs on the hard drives of Web site visitors. The plaintiff claims that the Defendants' actions constitute invasion of privacy in violation of the state constitution, fraud and deceit in violation of the state civil code, and the common law tort of trespass.

6. *Class Action Suits against RealNetworks, Inc.* Class Action lawsuits were filed against Internet software company, RealNetworks, Inc. in California state court in November 1999⁹⁵ and the Northern District of Illinois in February 2000.⁹⁶ RealNetworks provides video and audio services on the Internet that can be accessed by downloading its free software. Both cases alleged RealNetworks was using the downloaded software to monitor users' online behavior in violation of its privacy policy. Both cases are currently pending. The Northern District of Illinois has, however, ruled that the arbitration clause in the terms of use posted on the site, which the user must accept to download the software, is enforceable.

7. *Class Action Suits against DoubleClick, Inc.*⁹⁷ In California and New York, numerous complaints were filed against DoubleClick, Inc., an Internet advertising company that tracks Internet user behavior to personalize its banner advertisements, alleging it was unlawfully obtaining and selling consumers' personal information (including name, phone number and e-mail address) by

<<http://www.marketspan.com/DocketDirect/MSFDock.asp?DType=0&Code=411167893894994900798893793794794900181999>>.

⁹²No. 2:00cv04993 (C.D. Cal., filed May 11, 2000), available at <http://www.epic.org/anonymity/aquacool_complaint.pdf>.

⁹³Upon Yahoo!'s request, the case was transferred to the Northern District of California. No. 5:00-cv-20677 (N.D. Cal., June 21, 2000). In July 2000, Yahoo! was granted an extension of time to respond to the Complaint. No Answer has yet been filed.

tracing consumers' online behavior using cookies without disclosure of such activity and combining the information with personal information from a direct marketing database. These suits were consolidated in the Southern District of New York and are currently pending.

CONCLUSION

The evidence discussed above leads one to several conclusions about Internet privacy:

- The concerns over privacy intrusions by marketers are based on limited anecdotal evidence. Public policy should not be established on such anecdotal evidence.
- The limited number of improper intrusions that have occurred are being adequately addressed by existing legislation and individual consumer suits.
- The Internet is in its early stages of growth and should be nurtured, not hampered, by new laws or regulations.
- Industry self-regulation is advancing and addressing the concerns of consumers in innovative ways, much of which goes beyond the limits currently existing in the off-line marketing community. Legislation or new regulations will only slow this process down.
- The business community is developing software that gives consumers control over what personal information is or is not used by marketers. Such software will empower the consumer with more choice than any regulation can accomplish.
- Government regulation of the Internet is severely limited by the global nature of the medium, i.e., regulation is local, and use is global. Local regulation cannot adequately address global behavior.

All of this dictates restraint by legislators and regulators. Aggressive behavior will only serve to stunt the growth of the Internet, hurt many entre-

preneurs and small businesses who most benefit from the efficiencies offered by the Internet, and prevent targeted and cost effective benefits to consumers unprecedented in the off-line marketing world.

⁹⁴Case No. SCVSS 69202 (Cal. Super. Ct. July 28, 2000).

⁹⁵*McDonald v. RealNetworks, Inc.*, Docket No. 816666 (Orange County Super. Ct., filed Nov. 4, 1999).

⁹⁶*Lieschke v. RealNetworks, Inc.*, Nos. 99-C-7274 & 99-C-7380, 2000 U.S. Dist. LEXIS 7073 (N.D. Ill. Feb. 11, 2000).

⁹⁷*In Re DoubleClick, Inc. Privacy Litigation*, Docket No. 1352, 2000 U.S. Dist. LEXIS 11148 (J.P.M.L. July 31, 2000).