SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Canada-United States Law Journal

Volume 25 | Issue

Article 40

January 1999

Consumer Protection and Antitrust Enforcement at the Speed of Light: The FTC Meets the Internet

John Graubert

Jill Coleman

CONSUMER PROTECTION AND ANTITRUST ENFORCEMENT AT THE SPEED OF LIGHT: THE FTC MEETS THE INTERNET

John Graubert[*]
Jill Coleman[**]

I. INTRODUCTION

Rapid and significant advances in computer and communications technology have significantly transformed the global economic environment in which consumers and businesses operate – sometimes seemingly overnight. Regulators at the Federal Trade Commission (FTC) are faced with the continual challenge of applying their analytical and enforcement tools to new technological advances, so that the use of such technology is consistent with the goals of consumer protection and healthy competition.

One of the most significant consequences of this technological evolution over the past few years has been the dramatic growth of the Internet. The rapid rise of the Internet, and in particular the World Wide Web, as a global medium for communication and electronic commerce has profoundly altered our concepts of time, distance, and privacy.[1] The Internet has dramatically increased the speed and ease with which data can be obtained, analyzed, exchanged, and transmitted. Further, the Internet has expanded the ability to

---

[*] Mr. Graubert is Deputy General Counsel of the Federal Trade Commission. The views expressed in this Article are those of the authors and do not necessarily represent the views of the Federal Trade Commission or any individual Commissioner. The authors gratefully acknowledge the assistance of Debra Valentine, Lisa Rosenthal, Paul Luehr, and Martha Landesberg.

[**] Ms. Coleman is an attorney in the Office of the General Counsel.

[1] One recent survey of the total worldwide online population estimated that more than 159 million adults over the age of sixteen are using the Internet. *See* Nua Internet Surveys, Mar. 1999, (visited June 15, 1999) <http://www.nua.ie/surveys/how_many_online/index.html>. In the United States alone, 79.4 million adults, or 38% of the population aged 16 and over, were estimated to be online in January of 1999, and this number is growing at an explosive rate each year. According to one estimate, by the year 2000, the number of U.S. online adult users is projected to reach 100 million. *See* Intelliquest, *100 Million Americans Can't Be Wrong* (visited June 15, 1999) <http://intelliquest.com>. Further, although worldwide access to personal computers is still limited, in the United States today 50.3% of households reportedly own their own personal computer. *Over Half of U.S. Households Now Own PCs*, SAN JOSE MERCURY NEWS, May 19, 1999, at 1C. The number of Canadians over the age of 18 with Internet access at the end of 1998 was estimated to be 13.5 million. *See id.*

conduct transactions and engage in electronic commerce across national boundaries. At the same time, the Internet has permitted businesses to collect and use vast amounts of personally identifying and demographic information about consumers and their preferences, resulting in significant new concerns about potential losses of privacy, particularly the privacy of children. The innovations created by the Internet will continue and become more significant as computer and network technologies mature, as more daily economic activities migrate to the Internet, and as consumers and businesses develop greater confidence in their ability to communicate and conduct business safely and reliably in cyberspace.

From the FTC's perspective, however, the growth of the Internet has not, for the most part, required adoption of a wholly new legal framework for consumers and competition. The existing consumer protection and antitrust laws the FTC enforces have thus far proven to be as applicable to the online environment as they are to other markets. One area that has presented unique consumer concerns, however, is Internet privacy. As discussed below, there are mounting concerns about the protection of the online privacy of consumers, and there is much discussion of what the role of the government should be in this area.

The FTC is uniquely positioned to address these issues and other issues associated with the Internet. The agency has an extremely broad legislative mandate under the Federal Trade Commission Act: to protect consumers from unfair methods of competition and unfair or deceptive acts and practices across a wide range of business sectors.[2] The FTC also enforces some forty additional statutes as well as thirty separate rules governing specific industries and practices, such as telemarketing,[3] the use of 1-900 numbers,[4] and most recently, the protection of children's privacy online.[5] A wide range of commercial activities on the Internet fall squarely within the scope of the FTC's existing statutory and regulatory mandate. Accordingly, since the emergence of the Internet as a marketing medium in the mid-1990s, the FTC has been concerned with the ways that businesses may use the Internet to deceive and defraud consumers and potentially harm competition, and has been actively attacking unlawful conduct associated with this medium.

---

[2] *See* Federal Trade Commission Act, § 5(a), 15 U.S.C. § 45(a). *See generally* N. W. Averitt & R. H. Lande, *Consumer Sovereignty: A Unified Theory of Antitrust and Consumer Protection Law,* 65 ANTITRUST LAW J. 713 (1997) (discussing relationship of antitrust and consumer protection and the role of the FTC in enforcing both types of laws).

[3] *See* FTC Telemarketing Sales Rule, 16 C.F.R. § 310 (1999).

[4] *See* FTC Trade Regulation Rule Pursuant to the Telephone Disclosure and Dispute Resolution Act of 1992 [initial case] (900-Number Rule), 16 C.F.R. § 308 (1999).

[5] *See* FTC Children's Online Privacy Protection Rule, 64 Fed. Reg. 22,750 (1999) (to be codified at 16 C.F.R. § 312) (proposed Apr. 27, 1999).

The FTC faces several challenges in applying this regulatory and statutory authority to the Internet. How do we ensure that competition on the Internet, and between Internet and traditional retailers, is free and vigorous, so that consumers get the best quality products at competitive prices? How do we ensure that consumers are protected from deception and other abuses online, so that they can obtain accurate information that equips them to choose from among the products and services offered? Finally, how do we accomplish these goals in a manner that does not stifle the innovative potential this medium holds for legitimate businesses to reach more consumers with better products and services?

As discussed below, on the consumer protection front, the FTC has been active in defending against fraud on the Internet through its efforts to promote self-regulation and, as necessary, through law enforcement actions. In addition, the FTC has also played a significant role in helping to advance the online privacy interests of consumers by assessing the extent to which the personal information of online users is gathered and used by businesses, and encouraging industry self-regulation (but holding Internet merchants to their word when they promulgate privacy policies).

On the competition side, the Internet presents issues relating to the growth and operation of the system, such as control of standard-setting processes and communication facilities, as well as the traditional antitrust issues that may arise when parties do business in any market. Indeed, in one group boycott case, the FTC took action with respect to conduct that it alleged would have been plainly unlawful whether or not the Internet was involved. Such a boycott is still unlawful even though elements of the drama shift to cyberspace.[6]

In short, there is no exemption from the laws governing competition and consumer protection for the Internet, and those laws have been enforced vigorously by the FTC since the rise of the Internet as a marketing and communication medium. In the remainder of this Article, we briefly describe some of the experiences of the FTC with the application of those laws to cyberspace, as well as some of the additional concerns agencies like the FTC might have in this area as the Internet continues to develop.

II. COMPETITION AND THE INTERNET

It is true that the Internet has remarkable capabilities for bringing more people together with respect to a broad range of products and services. Consumers have ready access to more information and suppliers than ever be-

[6] *See* Fair Allocation System, Inc.: Analysis to Aid Public Comment, 63 Fed. Reg. 43,182, 43,183 (1998) [hereinafter Fair Allocation System].

fore. The Internet may be an extremely efficient marketplace in many ways, but it is still a marketplace and the traditional rules of antitrust are being applied in that marketplace.[7] The Internet shares some of the characteristics of its predecessors like catalog and mail order operations. Accordingly, many of the issues encountered on the Internet will be familiar ones for regulators and industry.

As always, to determine whether antitrust issues are present, regulators must take a close look at the facts of every case and try to understand the workings of the markets involved, including Internet markets. The need to learn about particular markets is not a new problem or task for regulators, but the Internet will undoubtedly present some new and interesting scenarios to consider.[8] It may well be that specific technical aspects and other characteristics of the Internet may affect market definition issues and market power and entry barrier analysis in a specific case. As is the case in other high-tech markets, some Internet markets may experience rapid innovation and "leapfrogging" technologies that undercut market power, while others are more prone to entrenchment and exclusionary conduct. Industry observers have noted, for example, that sellers on the Internet can add new lines of products relatively quickly, and they can also re-define the nature of shopping services using new technology.[9] These developments may pose interesting questions about the markets in which sellers are operating and who their competitors are.

Virtually any antitrust scenario can arise in cyberspace. For purposes of this discussion, we will look at two general categories of issues or potential issues: those relating to the structure and operation of the Internet itself, and the rules governing transactions on the Internet.

---

[7] For specific examples of the application of antitrust law to the Internet, see R. Steuer, *Retailing on the Internet*, 12 ANTITRUST 50 (Summer 1998).

[8] In high-tech markets generally, the competitive arena is frequently in the areas of innovation and development of future products and services, not just current conditions. The FTC has paid increasing attention to innovation markets. *See* In the Matter of Glaxo plc, 119 F.T.C. 815 (June 14, 1995) (development of migraine drugs); Hoechst AG, No. C-3629 (Dec. 5, 1995); Ciby-Geigy/Sandoz, 123 F.T.C. 842 (Mar. 24, 1997) (gene therapy research). *See generally* DOJ/FTC Antitrust Guidelines for the Licensing of Intellectual Property § 3.2.3 (Apr. 6, 1995).

[9] *See* J.W. Gurley, *How the Net is Changing Competition*, FORTUNE, Mar. 15, 1999, at 168.

A. The Structure of the Internet

1. Standard-Setting

The operation of the Internet depends on clear, strict compatibility, connectivity, and communications standards. Some have argued, accordingly, that a high degree of standardization is inevitable and beneficial in this market and that antitrust authorities should take a generally hands-off approach to standard-setting in this area.[10] Even such commentators, however, acknowledge that, under certain circumstances, single-firm conduct could co-opt the standard-setting process and raise antitrust concerns.[11]

One initial question to ask is, who is setting the standards? For example, for the last several years, the U.S. government (primarily through the Department of Commerce) has been in the process of privatizing control over, and introducing competition into, the domain name registration system – the address-standardization system that is a crucial underpinning of universal access to the Internet. Among other concerns, government authorities envisioned that the new, independent corporation established to manage the system, the Internet Corporation for Assigned Names and Numbers (ICANN), would operate under well-established standard-setting organization principles "that ensure transparency, equity and fair play,"[12] and reduce the risk that the organization could be dominated by any particular commercial interest.[13]

Recently, ICANN announced the selection of the first five companies to participate on a test basis in a new, competitive Shared Registry system.[14] Although this group of five may soon be joined by additional potential service providers, concerns have already been expressed that the significant existing customer base of one of the initial selectees could complicate the task of smaller registrants trying to provide effective competition.[15] As the Commerce Department has said, however, "antitrust law will provide accountability to and protection for the international Internet community" if market

---

[10] *See* M. A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 CONN. L. REV. 1041, 1042-43 (1996).

[11] *See id.* at 1065, 1074-78, 1086-89.

[12] Management of Internet Names and Addresses, 63 Fed. Reg. 31,741, 31,747 (1998) (Doc. Statement of Policy).

[13] *See id. See generally* David Balto & Fred Horne, *The New Wild West Can Use a Sheriff*, LEGAL TIMES, Nov. 2, 1998, at S36.

[14] *See* ICANN, ICANN Names Competitive Domain-Name Registrars, Press Release, Apr. 19, 1999 (visited July 7, 1999) <http://www.icann.org/icann-pr21apr99.htm>.

[15] *See* Karen Kaplan, *AOL, 4 Others Win Right to Register Internet Names*, L.A. TIMES, Apr. 22, 1999, at C1.

abuses occur in the domain name registration system.[16] Although an antitrust suit against Network Solutions, Inc., which has been handling domain name registration tasks under contract with the Department of Commerce and the National Science Foundation, was recently dismissed because the court found NSI's relationship with the government entitled the company to immunity,[17] future independent, private participants in the domain registration system may not be the beneficiaries of such immunity.

In a related context, in 1996 the FTC reached a consent agreement with Dell Computer Corporation in a case of attempted "capture" of a standardization process. During the development of a standard for the VL-bus, used for the transfer of instructions between a CPU and peripherals, the Video Electronics Standards Association (VESA), which was coordinating the standardization process, asked its members (including Dell) whether they had any patents or other intellectual property claims that might conflict with the proposed standard. Dell certified to VESA that it had no such claims, but later, after the standard was adopted, asserted that it did in fact own a patent that it claimed covered the standard. In effect, had Dell succeeded with this strategy, it would have enlisted the aid of its competitors in agreeing to an industry standard and then asserted unilateral control over that standard. The consent order prohibited Dell under these circumstances from enforcing its patent.[18] This was not strictly an Internet case, and indeed the VL-bus standard applies primarily to 486-based computers and is, therefore, in declining use. The matter is nevertheless important, not only because of its relevance to any attempt to co-opt a standard-setting process but, in particular, because the Internet Engineering Task Force, a standard-setting organization, has historically required the same agreement by participants not to assert intellectual property ownership of Internet standards.[19]

2. Monopolization of facilities

Despite the broadly decentralized nature of the Internet, problems of bottlenecks and monopolization can still arise. For example, in the MCI/WorldCom merger, the combined firm would have controlled over fifty

---

[16] *See supra* note 12, at 31,747.

[17] *See* PGMedia, Inc. v. Network Solutions, Inc., 1999-1 Trade Cas. (CCH) ¶ 72,503 (S.D.N.Y. Mar. 16, 1999). *See also* Thomas v. Network Solutions, Inc., 1999 U.S. App. LEXIS 9065 at *26-28 (D.C.Cir. May 14, 1999) (dismissing "essential facilities" claim against Network Solutions because plaintiff domain name registrants were not competitors of NSI).

[18] *See* FTC, For Your Information, News Release, June 17, 1996 (visited June 24, 1999) <http://www.ftc.gov/opa/1996/9606/dell2.htm>.

[19] *See* Lemley, *supra* note 10, at 1086-87.

percent of Internet backbone transmission facilities.[20] The Federal Communications Commission (FCC) decided that entry into this market was difficult enough that any anticompetitive conduct could not be readily cured by new entry. The FCC concluded that the significant post-merger share would have given the combined firm the incentive and ability to dictate terms to smaller backbone providers, and perhaps other Internet players, and potentially increase costs or discriminate against smaller rivals. The FCC, therefore, conditioned its approval of the transaction on divestiture of the Internet assets to Cable and Wireless.[21]

B. Conduct on the Internet

1. Price-fixing

Antitrust enforcers have frequently faced the difficult task of determining when public statements followed by parallel pricing constitute or reflect illegal price fixing, and when they are legitimate competitive responses.[22] The Internet, of course, simply makes all communications (lawful or unlawful) easier and faster. The task of the enforcement authorities is still the same – to look at the evidence and decide each case on its facts. In 1994, for example, the Department of Justice (DOJ) accepted consent agreements with several major airlines concerning what the Department alleged was a sophisticated system for reaching agreement on prices using the industry's computerized fare dissemination system.[23] The airlines transmitted vast quantities of data to this system, some of which was either not accessible to or unusable by the travel agents who were the ostensible beneficiaries of the system.[24] The airlines, however, had the capability and interest to analyze the data, and DOJ alleged that the airlines were using the system to propose, negotiate, and enter into complex agreements about fares and routes.[25] The consent order permits the airlines to promulgate legitimate fare and route information for the

---

[20] *See In re* Application of WorldCom, Inc. & MCI Communications Corp., Order FCC 98-225, 1998 WL 611053 (Sept. 14, 1998).

[21] *See id.*; Balto & Horne, *supra* note 13.

[22] *See* J. Baker, *Identifying Horizontal Price Fixing in the Electronic Marketplace*, 65 ANTITRUST L. J. 41 (1996).

[23] *See* United States v. Airline Tariff Publishing Co., 1994-2 Trade Cas. (CCH) ¶ 70, 687 (D.D.C. Aug. 10, 1994).

[24] These contained so-called "footnote designators" which provided additional information about when certain fares were proposed to go into effect.

[25] *See id. See also* Proposed Final Judgement and Competitive Impact Statement, 59 Fed. Reg. 15,225, 15,229-32 (1994).

benefit of customers, but bans the conduct that was believed to have simply facilitated improper price coordination.[26]

2. Boycotts

In August 1998, the FTC accepted a consent order from a group of Chrysler dealers in the Pacific Northwest who had allegedly attempted to force Chrysler to limit its supply of cars to a Kellogg, Idaho dealer who was selling cars over the Internet. The dealer group threatened to withhold warranty service and sales of particular car models unless Chrysler limited the allocation of cars to the Internet seller to an amount representing only the dealer's local sales.[27] Notably, Chrysler resisted these pressures and praised the efforts of the Internet seller, thereby highlighting that the scheme was purely a horizontal one and undercutting any possible free-rider defense.[28] The case shows how the Internet created a business opportunity, which in turn prompted a straightforward anti-competitive reaction by rivals, and then the application of traditional tools by enforcers. In fact, this case was in many ways an updated version of *United States v. General Motors*,[29] in which the Supreme Court held that a dealer cartel in Los Angeles aimed at preventing other dealers from selling through discount brokers was a *per se* illegal group boycott.[30]

3. Predatory Pricing

Allegations of predatory pricing often present intriguing analytical issues, and the economics of doing business on the Internet may add some new wrinkles in this area. Predatory pricing, in general, requires two things: initial sales below marginal cost (or an average variable cost surrogate) and the possibility of subsequent recoupment of foregone profits through supra-competitive price increases.[31] As to the first prong of the test, although the strategy of *giving* products away on the Internet is widespread, this may or may not be an indication of initial sales below marginal cost. First of all, the marginal costs of distributing additional copies of software on the Internet may be extremely small. In addition, a company may be generating other revenue, such as advertising revenue, from the distribution of its products

---

[26] *See* 59 Fed. Reg. at 15,232-33.

[27] *See* Fair Allocation System, *supra* note 6, at 43,182.

[28] *See id.*

[29] 384 U.S. 127 (1966).

[30] *See id.* at 147.

[31] *See* F.M. SHERER & D. ROSS, INDUSTRIAL MARKET STRUCTURE AND ECONOMIC PERFORMANCE 472-79 (3rd ed. 1990).

that may have to be taken into consideration.[32] The second prong, recoupment, may also present conceptual as well as practical difficulties. If entry is relatively easy, as it often is on the Internet, new entrants would be expected to undercut any attempt to raise prices.

This does not mean, however, that the possibility of predatory pricing in Internet markets should be dismissed. Once again, antitrust enforcers will have to examine the facts of each case closely. For example, we noted above that standardization plays a significant role in the operation of the Internet. If a single firm was able to dominate a standard, or otherwise benefit from significant network effects, standardization could well create entry barriers.[33] Such entry barriers could then make recoupment feasible.

III. PROTECTING CONSUMERS ON THE INTERNET

The consumer protection effort by the FTC in Internet matters is a mixture of enforcement actions and encouragement of the private sector to regulate itself. In this section, we will review (a) enforcement actions the FTC has taken against fraud and deception on the Web, (b) Internet privacy issues, and (c) the application of the FTC's rules and guides to cyberspace and global electronic commerce issues.

A. Fraud and Deception on the Web

1. Law Enforcement Actions

One of the FTC's main methods for eliminating unfair and deceptive practices on the Internet is to monitor Web site operators and take legal actions against those who are believed to be using this medium unlawfully. Relying on its broad enforcement authority under Section 5 of the FTC Act[34] and other statutes, the Commission has brought more than sixty-five cyberfraud cases, involving over 170 defendants, since 1994. Interestingly, the FTC does not frequently encounter particularly complicated, high-tech schemes on the Internet. Rather, garden variety frauds such as prize promotions, deceptive offers of business opportunities, credit repair scams, and "get-rich-quick" schemes have moved rapidly and easily to the Web, with serious consequences for consumers.[35] Just as it does for legitimate firms, the

---

[32] *See* Gurley, *supra* note 9.

[33] *See* Lemley, *supra* note 10, at 1074-75.

[34] *See* 15 U.S.C. § 45 (a).

[35] *See, e.g.*, FTC, Internet Mall Promoters Settle FTC Charges Earnings Claims For Internet-Based Businesses Were False, News Release, Apr. 15, 1999 (visited June 22, 1999) <http://www.ftc.gov/opa/1999/9904/imall1.htm> (stating that an Internet site and company

Internet virtually eliminates any entry barriers to scam artists. With almost no up-front costs – and using no more than a computer, modem, and a telephone line – an unscrupulous firm can hold a deceptive online auction, tout a pyramid scheme, or advertise products or services that turn out to be either worthless or nonexistent. What is new and different about Internet fraud, however, is its global reach. Internet frauds can potentially victimize millions of consumers literally around the world. Importantly, the FTC's online activities have focused not only on preventing Internet frauds, but also on providing remedies for injured consumers and deterring future law violators. Thus, the FTC assists legitimate online businesses to conduct transactions on the Web because, once consumers have been cheated online, they may forsake doing business on the Internet forever, even with the most reputable firms.

One traditional scam that has blossomed on the Internet is the pyramid investment scheme. Pyramid schemes claim to provide easy riches to consumers who are willing to recruit downstream participants or forward money to the original promoter. However, economists estimate that about ninety-five percent or more of participants in pyramid schemes lose their money.[36] The FTC has initiated several law enforcement actions in federal court against Internet pyramid marketers, often in cooperation with other federal, state, and local law enforcement agencies, to attack this growing problem.[37] The FTC has also worked with other law enforcement authorities – both domestic and foreign – to inform Web site operators worldwide that they may be in violation of the law and to prevent consumers from being injured by these schemes.[38]

---

principals agreed to pay $4 million, post a $500,000 bond before doing future business, and were barred from violating the FTC Franchise Rule to settle allegations they made false earnings claims for Internet-based businesses in violation of the Franchise Rule).

[36] FTC, FTC to Junk E-mailers: No Scamming While You're Spamming, News Release, Feb. 5, 1998 <http://www.ftc.gov/opa/1998/9802/junk.htm>.

[37] *See* FTC v. Fortuna Alliance, L.L.C., et. al., Civ. No. C96-799M (W.D. Wash., filed May 23, 1996); FTC v. JewelWay International, Inc., CV97-383 TUC JMR (D.Ariz., filed June 24, 1997); FTC v. 5 Star Auto Club, Inc. et al., No. 99-Civ-1693 (S.D.N.Y., filed Mar. 8, 1999).

[38] The FTC has held 16 different "surf days" in which Commission staff, often along with other domestic and foreign law enforcement officials, conduct synchronized searches of the Internet. Once the enforcers identify certain types of potential scams such as pyramids, false miracle cure claims, and deceptive spam, they send electronic messages to the Web sites' proprietors, newsgroups, and e-mailers warning them that their content may be unlawful. *See, e.g.*,. FTC, Get Rick Quick Schemes, Illegal Pyramid Schemes Caught in an International Law Enforcement Web, News Release, Nov. 17, 1997 (visited June 28, 1999) <http://www.ftc.gov/opa/1997/9711/intlsurf.htm>.

Another familiar consumer problem that has emerged on the Web is the proliferation of unsolicited commercial e-mail (UCE) or "spam." Aside from the nuisance factor that UCE messages create for Internet users and service providers, the messages themselves often contain false or misleading claims. In one case, the FTC discovered a defendant using spam to promote allegedly fraudulent credit repair services.[39] In another matter, the FTC took action against a spam e-mailer who solicited consumers with spam that contained allegedly false and misleading income claims for a business opportunity that purportedly resold advertising space on Internet news sites.[40] Another fraud that is not unique to the Web but has proliferated there, is the practice of on-line "cramming." As it pertains to the Internet, cramming involves billing consumers' credit or debit cards or telephone bills for unordered or fictitious Internet services.[41]

A few Web marketers have been more creative in taking advantage of the Internet's potential for high-tech deception. For example, in the *Audiotex Connection* case, the FTC brought a federal court action against a company that "hijacked" the modems of consumers who visited the company's adult entertainment Web sites.[42] The defendants accomplished this by directing visitors to their sites to download special software that disconnected these unsuspecting users from their own Internet service providers and reconnected them, via an international phone number, to an overseas site supposedly in Moldova but actually terminating in Canada. Consumers would stay unwittingly connected to the international call, accruing expensive long distance phone charges, until they shut their computers down entirely, not simply until they logged off defendants' Web site. The case was eventually settled, and defendants agreed to provide consumer redress that should ultimately exceed two million dollars.[43] Cutting-edge Web scams such as this one pose new and unpredictable dangers for consumers online.

2. Promoting Self-Regulation

While the FTC has been vigorously pursuing scam artists on the Internet through its law enforcement authority, the Commission has also played a

---

[39] *See* FTC v. Dixie Cooley, No. CIV-98-0373-PHX-RGS (D.Ariz., filed Mar. 4, 1998).

[40] *See* FTC v. Internet Business Broadcasting, Inc. et al., No. WMN-98-495 DMP (D.Md., filed Feb. 19, 1998).

[41] *See* FTC v. J.K. Publications, Inc. et al., No. CV-99-00044 ABC (AJWx) (C.D. Cal., filed Jan. 5, 1999).

[42] *See* FTC v. Audiotex Connection Inc., CV-97-0726 DRH (E.D.N.Y, filed Feb. 13, 1997). *See also* In the Matter of Beylen Telecom, Ltd., No. C-3782 (Jan. 23, 1998) (rendering the final consent order in a companion FTC case).

[43] *See* FTC v. Audiotex Connection, Inc., *supra* note 42.

significant role in encouraging voluntary self-regulation of commercial Internet practices. Self-regulation, when successful, typically provides a more prompt, flexible, and effective means for ensuring lawful behavior than does government legislation or regulation. This is often true whether self-regulation takes the form of private sector guidelines or cooperative public and private initiatives. The Commission recognizes that self-regulation can be preferable to government regulation in particular economic sectors, such as the Internet, because the dynamic high-tech environment calls out for rapid, innovative, and adaptive solutions. Thus, one of the Commission's chief tasks has been to help foster a climate in which Internet self-regulation is both possible and meaningful. The FTC has worked with industry to assist in its efforts to extend existing self-regulatory initiatives to the Web and to develop new mechanisms for protecting consumers online. If industry does not take satisfactory steps, however, the FTC has said it is prepared to recommend legislative solutions or undertake regulatory initiatives. Of course, concerted private behavior involving the Internet has the potential to raise possible antitrust concerns and impede competition. But the FTC will welcome self-regulation that is consistent with the antitrust laws and does not pose an obstacle to competition.[44]

B. Maintaining Consumers' Internet Privacy

In addition to focusing on unfairness and deception in cyberspace, the FTC has been at the forefront of the Internet privacy debate. Through the Internet, businesses have been able to gather significant amounts of information about consumers' identities, interests, and activities, often without the consumers' knowledge or consent. Even when consumers do consent to provide information about themselves when visiting a Web site, they rarely receive any assurance from the operators of that site that their personal identifiable information will be used only for the purposes for which it was provided or that the information will not be shared with others. In a survey of online privacy conducted last year, the FTC found that the vast majority of commercial Web sites – roughly eighty-five percent – collect personal in-

[44] The Commission has also tackled fraud and deception on the Web through a broad range of educational efforts to inform Internet users of the benefits and dangers of online commercial activities. To date, these efforts have included publishing numerous electronic consumer and business guides and brochures, creating informational Web sites, and sponsoring online forums. *See generally* FTC Web site at <http://www.ftc.gov>.

formation from consumers, but only a small fraction of these inform users of their information protection practices.[45]

The FTC has held several hearings and public workshops and has issued studies and reports that examine issues related to online privacy protection.[46] The Commission's central goals in examining online privacy issues are to understand the privacy concerns associated with expanding Internet use, promote a dialogue among consumers, the private sector, government, and other interested parties on this subject, and encourage the expeditious development of effective self-regulation in this area. The FTC's extensive work in this area so far has revealed that privacy and security protection rank among the most significant concerns consumers have about using the Internet and Web. Indeed, many consumers would rather not access Web sites without knowing that their personal information will be kept private. Until Web site operators adopt meaningful privacy protections for consumers, it is likely that many users will remain reluctant to use the Internet, let alone conduct electronic commerce. As a result, unless privacy issues are resolved sufficiently, the electronic marketplace may be unable to reach its full potential.

1. The Special Problem of Children's Online Privacy

Children constitute a rapidly growing segment of the online population. Taking advantage of this trend, many commercial Web sites are collecting a wide variety of detailed personal information from and about children by means of registration pages, user surveys, online contests, and applications.[47]

---

[45] *See* Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998) (visited June 28, 1999) <http://www.ftc.gov/reports/privacy3/toc.htm> [hereinafter *Privacy Online*].

[46] The FTC held its first public workshop on Internet privacy in April 1995. This workshop was followed by a series of hearings held in October and November 1995, examining the implications of globalization and technology on the FTC's missions, including online privacy issues. *See* FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech Global Marketplace* (May 1996) (visited June 28, 1999) <http://www.ftc.gov/opp/global/report/gc_vl.pdf>. The FTC held another online privacy workshop in June 1996. *See* FTC Bureau of Consumer Protection Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure (Dec. 1996) (visited June 28, 1999) <http://www.ftc.gov/reports/privacy/privacy1.htm>. In June 1997, the FTC held another public workshop focusing on privacy issues relating to spam, children's online privacy, and individual reference services. Finally, the FTC's *Privacy Online Report*, released in June 1998, involved an extensive survey of the privacy practices of 1,400 Web sites and examined the Internet industry's self -regulatory privacy efforts to date. *See Privacy Online*, *supra* note 44.

[47] The FTC found that eighty-nine percent of surveyed Web sites collected personal information from children, but only twenty-four percent posted privacy policies, and one percent obtained parental permission before collecting or disclosing children's information. *See Privacy Online*, *supra* note 44.

This information is often collected without notice to parents or opportunity for parental control. The FTC has devoted significant attention to the online collection of children's personal information by helping to identify the potential risks that current business data collection practices pose for children's privacy and safety. To address concerns about children's online privacy, Congress recently enacted the Children's Online Privacy Protection Act of 1998, which directs the FTC to issue regulations implementing the Act's specific privacy protection requirements.[48] Among other things, this legislation requires Web site operators or online services aimed at children to provide notice of their personal information collection and use practices and to obtain "verifiable parental consent" prior to collecting, using, or disclosing personal information gathered from children age twelve and under. Additionally, Web site operators must, upon request, provide parents with an account of the personal information that has been collected from their child, as well as an opportunity to terminate the Web site's future use or maintenance of such information. Children's participation in online games or contests cannot be conditioned on their providing more information than is "reasonably necessary" to permit such participation. Further, Web site operators must implement procedures to protect the security and confidentiality of the data collected online from children.[49] Significantly, the legislation also creates incentives for industry self-regulation, including providing safe harbors for industry groups or others who follow FTC-approved self-regulatory privacy guidelines.[50] The FTC recently proposed its regulations implementing this legislation.[51]

With respect to the privacy concerns of adults, and consistent with the FTC's approach to the Internet generally, the Commission has encouraged private sector-led solutions. Self-regulation of online privacy issues would permit firms to reach a consensus on appropriate privacy policies, experiment with different approaches, and implement the best strategies. However, if firms fail to develop and implement effective privacy protections for the Internet voluntarily, the Commission in the past has stated that additional legislation may be required.[52]

The FTC recently exercised its law enforcement authority in this area by challenging as deceptive the privacy practices of a Web site sponsored by

---

[48] *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6502 (1998).

[49] *See id.*

[50] *See id.* § 6503.

[51] *See* FTC Children's Online Privacy Protection Rule, *supra* note 5.

[52] *See Consumer Privacy on the World Wide Web*, FTC Statement Before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce (July 21, 1998) (visited June 28, 1999) <http://www/ftc/gov/os/1998/9807/privac98.htm>.

GeoCities. GeoCities – one of the most popular sites on the Web – allegedly misrepresented the purposes for which it collects personal identifying information from adults and children.[53] The company agreed to a settlement with the FTC that prohibits it from making such representations in the future and requires the firm to post on its sites a clear and prominent privacy notice regarding GeoCities' privacy policy. The order further provides safe harbors regarding the location and content of its privacy notice, the collection of information from children, and the procedure for obtaining "express parental consent" to collect personal information about children. Finally, the order imposes other specific disclosure provisions on GeoCities to correct previous practices and prevent future harm. The Commission's action in this matter demonstrates the agency's willingness to exert its enforcement power against those who compromise the privacy of Internet users by making false and misleading statements regarding their actual privacy practices.

2. Privacy's Global Dimension

Because the Internet is global in nature, the issue of privacy protection has an international dimension. Long before the advent of the Internet and the ensuing debate over Internet privacy, countries had developed their own national privacy regimes applicable to data collection and retention procedures. It is not surprising that the United States has relied primarily on a self-regulatory approach to protect the personal, identifiable data of its citizens. Against this backdrop of self-regulation, however, the United States implemented a number of legal privacy protections aimed at correcting specific abuses in industries by sector.[54] With respect to Internet privacy, the United States recently affirmed its commitment to effective self-regulation combined with appropriate sector-specific legislation.[55]

In contrast, the countries of the European Union have traditionally taken a different approach to privacy protection that entails comprehensive privacy legislation which is applicable to all sectors of the economy. The approach by the European Union to the privacy of personal data is best reflected in its all-encompassing 1995 Directive on Data Protection,[56] which was implemented last fall by the fifteen E.U. Member States. One of the most significant aspects of the E.U. Directive is the prohibition on the transfer of personal data to non-Member States that fail to provide an "adequate" level of

---

[53] *See* In the Matter of GeoCities, No. C-3850 (Feb. 5, 1999).

[54] *See, e.g., Privacy Online, supra* note 44.

[55] *See* U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE: FIRST ANNUAL REPORT, Nov. 1998 (visited June 28, 1999) <http://www.doc.gov/ecommerce/E-comm.pdf>.

[56] *See* Directive on the Protection with Regard to the Processing of the Personal Data and on the Free Movement of Such Data, No. 95/46/EC, Oct. 1995, 1995 O.J. (L 281) 31.

privacy protection. To maintain the free and uninterrupted flow of information between Europe and the United States following implementation of the E.U. Directive, it has been necessary to coordinate these disparate national approaches to privacy protection. Considerable efforts are now underway between the European Commission and the U.S. Department of Commerce to develop a set of privacy principles to serve as a safe harbor for U.S. companies seeking to comply with the E.U. Directive.[57]

While government involvement and self-regulation programs may be necessary in the near term to address the most urgent privacy concerns, such as children's online privacy protection, and to prevent serious disruption in the transfer of data between the trans-Atlantic countries, the most effective way to protect the privacy of online users may ultimately come from the high-tech marketplace itself. As always, natural market forces are likely to bring about the development of technologies for which there is a demand.[58] In the case of Internet privacy, several technologies potentially capable of protecting the online privacy of consumers are evidently already on the market or under development. Technology-based privacy solutions may eventually provide consumers with the confidence and security that they need to conduct business on the Internet on a global scale.

C. Cyberlaw Issues Still to Be Resolved

Although the FTC believes that the substantive legal tools presently available to the Commission provide a sufficient legal framework for protecting consumers from unfair and deceptive acts and practices on the Internet, the Commission is also examining how its specific consumer protection rules and guides should be applied to new electronic media forms, such as the Internet.[59] The FTC recognizes that, given the unique aspects of the

---

[57] Both sides are examining various proposals. The Department of Commerce has proposed creating "safe harbor" principles for U.S. companies who are involved in transferring personally identifiable data from the E.U. to the United States. Under this proposal, companies that adhere voluntarily to specified privacy principles would be presumed to provide "adequate" privacy protection as required by the E.U. Directive as long as they also embodied accepted U.S. privacy principles. See Safe Harbor Letter from Amb. David Aaron (Apr. 19, 1999) and other related materials available from the U.S. Department of Commerce, International Trade Administration Web site for more information. Department of Commerce, International Trade Administration (visited June 22, 1999) <http://www.ita.doc.gov>.

[58] *See* John Markoff, *Novell to Offer Data-Privacy Technology for Internet*, N.Y. TIMES, Mar. 22, 1999, at C1; Leslie Miller & E. Weise, *Keeping "Pry" Out of the Privacy Debate*, USA TODAY, Mar. 31, 1999, at D4.

[59] Some applications of FTC rules and guides to the Internet are straightforward. For example, the FTC's Mail and Telephone Order Rule applies to merchandise orders using the "telephone," – a term that is defined broadly in the Rule to include orders placed by fax or

Internet, further agency guidance may be required to ensure that businesses understand how to comply with rules and guides in their online advertising and that Internet users understand the protections they are afforded by these rules and guides as they surf the Web. To examine these issues, in May 1998, the FTC issued a notice seeking public comment on questions such as:

1) The extent to which several of the FTC's consumer protection rules and guides apply to new electronic media forms, including e-mail, CD-ROMs, and the Internet.

2) How certain terms appearing in consumer protection rules and guides that specify how representations should be made or disseminated – terms such as "writing," "printing," and "direct mail" among others – should be interpreted when such claims are made on electronic media.

3) How required or recommended disclosures should be made in electronic media.[60]

This last issue in particular poses some especially challenging issues. Many FTC consumer protection rules and business guides require or recommend that disclosures be made clearly and conspicuously.[61] In evaluating whether disclosures appearing in traditional media meet this standard, the Commission considers the net impression the advertisement creates. Disclosures are clear and conspicuous – and thus deemed to be communicated effectively – when they are noticeable, readable or audible, and understandable to the intended audience.[62] Because of the nature of the Internet, however, it may be more difficult to determine what information consumers will see when they access a Web site, and thus whether necessary disclosures on such sites are clear and conspicuous. Indeed, what consumers will see on a Web site is likely to vary depending on the point or Web page at which they access the Web site, how many pages they "hyperlink" through when reviewing the site, and how much of the page containing the disclosure is displayed

---

modem. *See* FTC Mail and Telephone Order Merchandise Rule, 16 C.F.R. § 435 (1999). The application of the Internet to terms appearing in other FTC rules and guides, however, may not be as clear-cut.

[60] *See* Interpretation of Rules and Guides for Electronic Media, 63 Fed. Reg. 24,996, 24,996-97 (request for comment) (1998).

[61] *See, e.g.*, Guides for Select Leather and Imitation Leather Products, 16 C.F.R. § 24; Guides for the Use of Environmental Marketing Claims, 16 C.F.R. § 260 (1998).

[62] *See* FTC Policy Statement on Deception, Oct. 1983 (visited June 28, 1999) <http://www.ftc.gov/bcp/policystmt/ad-decept.htm>.

by consumers' Web browsers without requiring additional scrolling. Each of these factors may impede the ability of consumers to view necessary disclosures appearing in Internet advertising.[63] One possible approach to this issue is to make required Internet disclosures "unavoidable" – in other words, consumers must be capable of viewing the disclosure without having to take affirmative steps such as scrolling or hyper-linking to another location.[64] The FTC held a workshop in May 1999[65] which provided interested parties with an opportunity to discuss clear and conspicuous disclosures in Internet advertising, as well as other issues regarding the applicability of certain FTC consumer protecting rules and guides in electronic media forms.[66]

The FTC also considered the international aspects of consumer protection on the Internet in another public workshop held in June 1999.[67] The Internet has contributed significantly to the creation of a borderless, global marketplace. The number of consumers purchasing goods and services and entering into contracts with foreign businesses is expected to grow tremendously. The globalization of electronic commerce has generated complex legal questions about how individual nations can best protect their citizens who are engaged in electronic commerce with foreign businesses. Among the issues that the FTC explored in its workshop, entitled "U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace," were the adequacy of currently applicable legal protections for U.S. consumers engaged in electronic commerce with foreign businesses, issues of jurisdiction and choice of law, availability and collection of consumer restitution or damages, as well as the challenging issues presented by differing standards of consumer protection (and differing views of what conduct is acceptable) in different parts of the world.[68] The workshop goal was to bring governments, industry, and con-

---

[63] *See supra* note 60, at 25,002.

[64] *See id.* at 25,002-03.

[65] *See* Announcement of Date of Public Workshop on the Interpretation of Rules and Guidelines for Electronic Media, Procedure for Requesting to Participate, and Request for Submission of Advertisements, 64 Fed. Reg. 14,156 (1999).

[66] The Commission is also committed to reviewing certain other consumer protection standards as part of its ongoing regulatory review program to determine, on a case-by-case basis, whether rules and guides should be modified to meet the special demands of the Internet and other new media forms. *See supra* note 60, at 24,998-99.

[67] *See* U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace, 63 Fed. Reg. 69,289 (1998); 64 Fed. Reg. 5,062 (1999) (announcing dates of workshop and extending deadline for public comment).

[68] Also on the international front, the FTC heads the U.S. delegation to the Consumer Policy Committee for the Organization for Economic Cooperation and Development (OECD). This Committee is currently working with other nations to develop international guidelines for consumer protection in electronic commerce. Additionally, the FTC has participated in several international initiatives to facilitate international consumer protection including, among others,

sumers together to encourage development of a global electronic marketplace that ensures safety, transparency, and legal certainty.

IV. CONCLUSION

As the Internet has been a fertile ground for business, it has also created interesting and challenging issues for the FTC. Thus far, however, the Commission's existing statutory authority to protect consumers and promote vigorous competition has largely proven to be effective and adaptable in meeting the new challenges of the online marketplace. The FTC will continue to apply those tools, making adjustments where necessary, as that marketplace continues to evolve.

---

the U.S.-Canada Telemarketing Task Force, the Mexico-U.S.-Canada Health Fraud Task Force, and International Marketing Supervision Network. Through these internationally coordinated activities, the FTC has been able to participate in establishing a dialogue between participating nations, identify areas of common interest, create a framework for cooperation, and begin to develop modalities for dealing with the jurisdictional and conflict of law issues that the Internet and the rise of electronic commerce pose.