

Protecting the Digital Consumer: The Limits of Cyberspace Utopianism

JOHN ROTHCHILD*

I. INTRODUCTION	895
II. NATURE OF ONLINE COMMERCIAL ACTIVITIES	899
<i>A. World Wide Web</i>	900
<i>B. Newsgroups</i>	901
<i>C. Electronic Mail</i>	902
<i>D. Chat Sessions</i>	903
III. VARIETIES OF ONLINE DECEPTIVE MARKETING PRACTICES	903
<i>A. Fraudulent Online Conduct</i>	904
<i>B. Misleading Online Conduct</i>	910
IV. SPECIAL CHARACTERISTICS OF THE ONLINE MEDIUM	911
<i>A. Increased Volume of Cross-Border Transactions</i>	912
1. Extraterritorial Assertion of Jurisdiction	912
a. Jurisdiction to Prescribe	913
b. Jurisdiction to Adjudicate	914
c. Location and Foreseeability in the Online Context	916
d. Summary: Jurisdiction over Online Conduct	916
2. Establishment of Jurisdiction	917

*Victor Kramer Fellow, University of Chicago Law School. A.B., Princeton University, 1979; J.D., University of Pennsylvania Law School, 1986. In 1997-98, I chaired a project of the Organisation for Economic Co-operation and Development ("OECD") that developed guidelines for consumer protection in electronic commerce. This Article builds on the work done in that project, and I wish to acknowledge the helpful comments I received from the project participants. The views expressed in this Article are my own, and not necessarily those of the OECD or any of the project participants.

3. Choice of Law	
918	
4. Enforcement of Judgments	
919	
5. Evasion of Law Enforcement Through Cross-Border Targeting	
921	
6. Difficulty in Obtaining Pre-Judgment Freezes of Assets Located Outside the Forum Country	
922	
7. International Comity	
923	
8. Restrictions on International Information-Sharing Among Law Enforcement Agencies	
923	
9. Impediments to Efforts by Consumers to Protect Themselves	
925	
<i>B. Ease of Evading Detection: Portability of Fraudulent Operations, and Disguising of Identity</i>	
926	
<i>C. New Entrepreneurs</i>	
929	
<i>D. Geographic Indeterminacy</i>	
930	
1. Limitations Imposed by Technology	
930	
2. Implications for Online Sellers	
933	
3. Home-Country Control	
937	
4. Opting Out	
939	
<i>E. Unclear Regulatory Environment</i>	
940	
<i>F. Summary: Barriers to the Development of Electronic Commerce Raised by the Special Characteristics of Online Communications</i>	
942	
V. ROLE OF GOVERNMENT IN CONTROLLING DECEPTIVE MARKETING PRACTICES IN ELECTRONIC COMMERCE	
942	
<i>A. Market Forces and Government Regulation</i>	
943	
<i>B. The Need for Government Intervention to Control Deceptive Conduct in Electronic Commerce</i>	
952	
<i>C. Four Dogmas of Cyberspace Utopianism: The Argument</i>	

1999]

*PROTECTING THE DIGITAL CONSUMER**Against Government Regulation of Electronic Commerce*

953

1. “Cyberspace Is a Self-Contained Jurisdiction,
over Which Territorially Based Sovereigns
Have No Legitimate Authority.”

953

2. “Attempts by Territorially Based Sovereigns to Exert Control
over Online Transactions Will Inevitably Prove Futile.”

954

3. “If One Government May Apply Its Laws Extraterritorially,
So May All Others, Resulting in a Clash of Jurisdictions
and a Requirement to Comply with All Nations’ Laws
Simultaneously.”

955

4. “Online Conduct Can Be Effectively Regulated by Those
Who Engage in It.”

955

*D. The Dogmas Dissected: Cyberspace Utopianism Has
No Clothes*

955

1. The Special Characteristics of Online Communications
Do Not Undermine the Legitimacy of Territorially Based
Jurisdiction

956

a. Online Communications, Though Universally Accessible,
Have Locally Differentiated Impact

957

b. Cost and Speed Advantages of Online Communications
Create Only Practical Issues

957

c. Virtual Addressing Does Not Undermine Territorial
Sovereignty

958

d. Physical Location of Online Interlocutors Is Not
Unknowable

958

e. The Relevant Factor Is the Location of the *Communicators*,
Not the Location of the *Communication*

960

2. The Argument from Futility Refutes Only One, Particularly
Poor, Enforcement Approach

960

3. The Problem of Overlapping Jurisdiction Can Be Addressed
Through Approaches Less Drastic Than Abdication

961

4. Deceptive Marketing Practices Are Not Likely To Be
Adequately Controlled by Market Forces Alone

962

5. Summary	968
VI. LETTING ONLINE COMMERCE GROW	968
<i>A. Improving the Transparency of the Legal Framework, and Adapting It to the Online Environment</i>	969
1. General Rule of Parity	969
2. Reasoning from Analogy with Other Means of Communication	970
3. Clarification and Updating of Regulatory Regimes	971
4. Educating Online Entrepreneurs	971
5. Negotiating an International Baseline Consumer Protection Regime	972
6. Protecting Online Privacy	972
<i>B. Enhancing the Effectiveness of Market-Based Solutions to the Problem of Online Deceptive Marketing Practices</i>	973
1. Facilitating Consumer Sovereignty	973
2. Industry Self-Regulation	974
3. Adapting Existing Alternative Dispute Resolution Mechanisms	976
4. Developing New Alternative Dispute Resolution Mechanisms	976
<i>C. Restraint in Extraterritorial Assertions of Jurisdiction</i>	978
1. Limiting What Is Deemed to Constitute Foreseeable Extraterritorial Effects	978
2. Focus on Location of People, Not of Computers	981
<i>D. International Cooperation Among Law Enforcement Authorities</i>	983
1. Mechanisms to Improve International Cooperation	983
2. Positive Comity	985

1999]

PROTECTING THE DIGITAL CONSUMER

3. Recognition of Foreign Judgments

986

4. Removing Obstacles to Cross-Border Investigations

986

VII. CONCLUSION

988

I. INTRODUCTION

Business-to-consumer commerce conducted via online means of communication,¹ though at present relatively modest in volume, is expected to grow exponentially over the next few years. According to one report, consumer purchases made over the Internet will rise from \$289 million in 1996 to \$26 billion in 2001.² With an estimated 100 million users online in 1998,³ and with a technology and cost structure that make it easy and inexpensive to place a message where it can be seen by all of those users,⁴ the Internet presents an irresistible lure and heady prospects for profit to marketers who are trying to get their message before a large audience.⁵ The blossoming of a true global marketplace for consumers, in which the Internet serves as the primary medium of communication, likewise holds potentially substantial benefits for consumers, making available a wider range of goods and services at a lower cost, thanks to an expansion of the effective sphere of competition, and allowing consumers the convenience of shopping from their own homes.⁶

¹For purposes of this Article, “online communications” refers to communications by means of data interchange across computer networks. This includes communications occurring via open networks, such as the Internet, as well as proprietary online services, such as America Online, CompuServe, Microsoft Network, and Prodigy. “Online commerce” and “electronic commerce” refer to commercial transactions in which online communications play a significant role.

²See BILL BURNHAM, *THE ELECTRONIC COMMERCE REPORT* 238 (1997). These figures are for purchases by U.S. households that are paid for via the Internet. *See id.* Other estimates of the annual volume of Internet retailing within the next few years range from \$7 billion to \$115 billion. *See* DEPARTMENT OF COMMERCE, *THE EMERGING DIGITAL ECONOMY* 38 (1998). A much larger volume of electronic commerce—\$202 billion in the year 2001—will consist of business-to-business transactions. *See* BURNHAM, *supra*, at 239. Some of the business entities involved in these transactions, in view of their small size and limited sophistication, may be regarded as akin to individual consumers in terms of their ability to protect themselves from deceptive marketing practices.

Measurements of the volume of electronic commerce vary widely, reflecting corresponding variations in the definition of what constitutes electronic commerce. *See Measuring Electronic Commerce*, at 6, 25, OECD Doc. OCDE/GD(97)185.

³*See* DEPARTMENT OF COMMERCE, *supra* note 2, at 7. The number of Internet users may rise to one billion by 2005, *see id.*, or even by the year 2000, *see* Nicholas Negroponte, *The Third Shall Be First*, *WIRED*, Jan. 1998, at 96, 96.

⁴*See infra* text accompanying notes 143-45.

⁵The amount spent on Internet advertising rose from \$50 million in 1995 to \$2 billion in 1998. *See* Ashley Dunn, *Ad Blockers Challenge Web Pitchmen*, *L.A. TIMES*, Mar. 2, 1999, at A1.

⁶*See* AUSTRALIAN COMPETITION & CONSUMER COMM’N, *THE GLOBAL ENFORCEMENT CHALLENGE* 5-6 (1997).

1999]

PROTECTING THE DIGITAL CONSUMER

Business-to-consumer online commerce will increasingly involve international transactions, in which the purchaser and vendor are located in different countries. This new form of international commerce is to be distinguished from the more familiar paradigm of international trade. In the older paradigm, a consumer purchases foreign-made goods from a vendor located in the consumer's own country. It is not the consumer who enters into an international transaction, but rather the vendor—or if not the vendor, another entity in the vendor's chain of supply. In the newer paradigm, disintermediation occurs, and the consumer purchases goods directly from a vendor located in another country.⁷

The change is a significant one from the standpoint of consumer protection policy. In the older paradigm of international trade, legislation and other rules of conduct designed to protect consumers from deceptive marketing practices apply with their full force, since the relevant transaction is a domestic one between the consumer and a domestic vendor. But when a consumer deals directly with a foreign vendor, the controls on deceptive marketing practices lose much of their efficacy: attempts to enforce the laws of the consumer's jurisdiction face both legal and practical roadblocks, and self-regulatory mechanisms may be unavailable.⁸

The special characteristics of the online medium also raise novel issues for sellers and other crucial participants in online commerce, including Internet service providers, presence providers, advertising agencies, proprietors of online malls, and Web site designers. Due to the inherently international nature of online communications, online sellers face the unhappy prospect that a multiplicity of jurisdictions will take more than a passing interest in their activities. Other communications technologies make it relatively simple to target commercial solicitations to a particular geographic area. When sellers make use of the various modes of online communication, such targeting ranges from the difficult to the impossible. This geographic indeterminacy raises severe and intractable issues of jurisdiction and choice of law, interfering with the ability of online sellers to structure their operations on grounds of legal predictability.⁹ Online sellers must also endure commercial uncertainty in the form of regulatory opacity. It is in many cases unclear how existing regulatory regimes governing trade practices apply to online commerce.

⁷The expansion of international online commerce is an aspect of a longer-term transformation of the global economy, which has seen a steady enlargement of the geographic scope of the market that is effectively available to consumers. In a set of hearings conducted in late 1995, the Federal Trade Commission ("FTC") examined this trend toward globalization of commerce, finding it characterized by great increases in the volume of international trade, cross-border investment, and transnational corporate business structures. FEDERAL TRADE COMM'N STAFF, *ANTICIPATING THE 21ST CENTURY: COMPETITION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE* 1-10 (1996). The OECD has also taken note of this trend. *See Revised Recommendation of the Council Concerning Co-operation Between Member Countries on Anticompetitive Practices Affecting International Trade*, OECD Doc. C(95)130 final [hereinafter *Revised Recommendation*] (noting "continued growth in internationalization of business activities"), available at <<http://www.oecd.org/daf/clp/rec8com.htm>>.

⁸*See* AUSTRALIAN COMPETITION & CONSUMER COMM'N, *supra* note 6, at 2.

⁹"Without an enforceable set of rules to permit commercial predictability, certainty, and consumer confidence, the 'global market' will never achieve its potential." Shirley F. Sarna,

The growth in online commerce will inevitably be accompanied by a rise in deceptive marketing practices¹⁰ directed at consumers. As much as ten percent of online commerce may involve consumer fraud.¹¹ This suggests that annual consumer losses from online deceptive marketing practices may amount to several billion dollars within a few years.¹² With this much money at stake, governments

Advertising on the Internet: An Opportunity for Abuse?, 11 ST. JOHN'S J. LEGAL COMMENT. 683, 689 (1996); see also *Illegal and Harmful Content on the Internet*, COM(96)487 final at 4-5 (“[L]egal and regulatory certainty is the *conditio sine qua non* to foster investments, guarantee the development of a competitive Internet services sector, and ensure the growth of a wider Internet-based economy in Europe.”).

Merchants may also themselves be the victims of online fraud. When a credit card thief makes unauthorized use of a consumer's credit card number, and the sale is made at a distance without signature verification, the consumer is typically liable for no more than \$50, while the merchant may be responsible for the full amount of the loss. See Saul Hansell, *Internet Merchants Try to Fight Fraud in Software Purchases*, N.Y. TIMES, Nov. 17, 1997, at D1.

¹⁰As used in this Article, “deceptive marketing practices” includes both fraudulent and negligent misrepresentations. According to one definition, a misrepresentation is fraudulent if the maker “knows or believes that the matter is not as he represents it to be,” “does not have the confidence in the accuracy of his representation that he states or implies,” or “knows that he does not have the basis for his representation that he states or implies.” RESTATEMENT (SECOND) OF TORTS § 526 (1965). A misrepresentation is negligent if the maker “fails to exercise reasonable care or competence in obtaining or communicating the information.” *Id.* § 552.

¹¹Up to 10% of all U.S.-based telemarketing is fraudulent. Annual losses from fraudulent telemarketing in the United States have been estimated at up to \$40 billion. See Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101(3) (1994) (“Consumers and others are estimated to lose \$40 billion a year in telemarketing fraud.”); COMMITTEE ON GOV'T OPERATIONS, THE SCOURGE OF TELEMARKETING FRAUD: WHAT CAN BE DONE AGAINST IT?, H.R. REP. NO. 102-421, at 7 (1991). Revenues from U.S.-based telemarketing amount to roughly \$400 billion annually. See Ann Marie Arcadi, Note, *What About the Lucky Leprechaun?: An Argument Against “The Telephone Consumer Protection Act of 1991,”* 1991 COLUM. BUS. L. REV. 417, 417; Patrick E. Michela, “*You May Have Already Won . . .*”: *Telemarketing Fraud and the Need for a Federal Legislative Solution*, 21 PEPP. L. REV. 553, 554 n.14 (1994).

Online commerce possesses several of the characteristics of telemarketing that facilitate fraud: the participants in an electronic commerce transaction may be located in different jurisdictions, and sellers need not maintain any fixed location. See H.R. REP. NO. 103-20, at 2 (1993), *reprinted in* 1994 U.S.C.C.A.N. 1626.

¹²No hard figures on the volume of consumer losses to online deceptive marketing practices are yet available. One consumer complaint intake service in the United States reports that complaints about online fraud rose sixfold from 1997 to 1998. See Sara Nathan, *Internet Fraud*, USA TODAY, Feb. 24, 1999, at 1B.

The evidence from law enforcement actions that have been brought against deceptive conduct with an online component indicates that consumer losses are already quite substantial. See *FTC v. Audiotex Connection, Inc.*, No. CV-97-0726 (E.D.N.Y. filed Feb. 13, 1997) (modem hijacking; \$2.7 million); *FTC v. Cano*, No. 97-7947-CAS-(AJWx) (C.D. Cal. filed Oct. 29, 1997) (guaranteed offshore credit cards; \$3-4 million); *FTC v. JewelWay Int'l, Inc.*, No. CV-97-383 TUC JMR (D. Ariz. filed June 24, 1997) (pyramid scheme; losses in excess of \$150 million); *FTC v. Fortuna Alliance, L.L.C.*, No. C96-799M (W.D. Wash. filed May 22, 1996) (pyramid scheme; \$7-11 million); *SEC v. Huttoe*, Litigation Release No. 15,185, 63 S.E.C. Docket (CCH) 1011 (D.D.C. Dec. 12, 1996) (market

1999]

PROTECTING THE DIGITAL CONSUMER

are well advised to give serious consideration to methods of protecting consumers from deceptive marketing practices.¹³

Sellers have an equally significant interest in the development of mechanisms to control online deceptive marketing practices. If deceptive trade practices are allowed to rage uncontrolled through the online medium, consumers will regard it as an unsafe place to venture, and electronic commerce will never attain its full potential.¹⁴ A sobering lesson may be derived from the audiotext or “pay-per-call” industry.¹⁵ In the 1980’s, as the industry grew and prospered, fraudulent activities were allowed to proliferate. As a result of consumer complaints and negative publicity, “[p]ay-per-call, which had grown quickly to a billion-dollar industry, lost \$400 million in one year.”¹⁶ Electronic commerce is currently at a critical stage of development. If the online medium gains a reputation as a haven for swindlers, a great deal of time and effort will be required to restore its image to the point where consumers will consider it safe enough to spend their money online.

This Article explores the obstacles to the growth of business-to-consumer electronic commerce that result from online deceptive marketing practices, from the standpoints of both consumers and online sellers. On the supply side, it proposes an approach to jurisdiction, choice of law, and related issues that would promote legal and regulatory transparency for sellers. On the demand side, it proposes a strategy of co-regulation that governments and nongovernmental organizations should follow in order to control online deceptive marketing practices.

manipulation; \$12 million). For a discussion of the FTC’s recent actions against online fraud, see FEDERAL TRADE COMM’N, *FIGHTING CONSUMER FRAUD* (1998).

¹³Electronic commerce implicates consumer protection concerns beyond deceptive marketing practices. For example, online communications raise issues relating to privacy, marketing directed to children, obscenity, hate speech, stalking, theft of information, and injury from defective products. Although these topics are beyond the scope of this Article, many of the proposals offered in this Article—for example, those addressing personal jurisdiction, and international cooperation of law enforcement agencies—are applicable to some of these issues as well.

¹⁴In one survey, 75% of respondents said that unknown reliability of online businesses was a key factor in their decision whether to engage in online commerce. *E-Commerce Survey: Business Reliability Ranks Near Transaction Security in Public Trust in Online Purchasing*, REP. ELEC. COMM., Feb. 10, 1998, at 3.

¹⁵“Audiotext” refers to audio information and entertainment services that are transmitted by telephone. A consumer who accesses the service incurs a charge, on either a per-minute or per-call basis, which is typically reflected on the consumer’s telephone bill, and the provider of the service receives a portion of those charges.

¹⁶FEDERAL TRADE COMM’N STAFF, *ANTICIPATING THE 21ST CENTURY: CONSUMER PROTECTION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE 17* (1996).

In so doing, this Article rejects two widely discussed views as to the proper role of the government in protecting consumers from online deceptive marketing practices: first, the view that governments have no legitimate role to play in this area; and second, the view that the existing trade practices regulatory regime can be applied unmodified to online commercial transactions. Advocates of the former position view cyberspace as a utopian realm radically disconnected from other forms of discourse, where ordinary rules do not apply. In so characterizing the online medium, they fail to observe the many characteristics that the online medium shares with other means of communication at a distance, such as the telephone and broadcast media. Holders of the latter view overlook the respects in which online communications differ from all other extant communications media. These differences call for a fundamental rethinking of the consumer protection strategies that governments have applied to transactions conducted via other communications media.

This Article begins with a brief overview of the modes of online communication that are of greatest relevance to commercial transactions, and continues with a description of the varieties of online deceptive marketing practices that are presently at large. It proceeds with a delineation of the novel aspects of online communications, demonstrating that regulatory strategies for controlling online deceptive marketing practices must be adapted to account for these aspects. The Article then examines, and rejects, the notion that governments have no legitimate role to play in regulating online commercial conduct. It concludes with a recommended set of strategies for governments and private entities.

II. NATURE OF ONLINE COMMERCIAL ACTIVITIES

The online medium offers several different facilities through which commercial activities may be conducted. Given the variety of these forms of communication, the online medium may be more properly viewed as a collection of several different media, united by their common use of computer-to-computer communications at a distance. The forms of online communication that are most relevant to electronic commerce are the World Wide Web, newsgroups, electronic mail, and chat sessions. A consumer who obtains access to the Internet via a commercial Internet service provider typically may make use of all of these forms of communication.

A. *World Wide Web*

1999]

PROTECTING THE DIGITAL CONSUMER

The World Wide Web (“Web”) is a collection of electronic documents, organized into Web sites residing on computers throughout the world that are linked to the Internet.¹⁷ Each Web page can link to any other such document in such a way that users may navigate from one document to another very easily and without regard to the physical location of the computer on which any document is stored. A Web page may contain textual, graphical, and multimedia material. Web pages are viewed by means of a software application called a Web browser, which receives data transmitted from the computer on which a Web page resides and displays it on the recipient’s computer. A Web page may contain hyperlinks that point to other Web pages located on any computer in the world that is set up as a Web server. With most modern browser software, the user actuates a hyperlink by clicking on it with the mouse pointer. Upon doing so, the page that the user was viewing is replaced more-or-less instantaneously by the page to which the hyperlink points.

Hundreds of thousands of businesses have established their own Web sites.¹⁸ These sites may be simple or elaborate, and may allow more or less interactivity to the user. The simplest form of a commercial Web site is a page that presents the user with the company’s name, some description of the products or services it offers, and a means of locating or communicating with the company through offline means.¹⁹ Rather than being limited to static text or graphics, a Web site may be enhanced with animated graphics, audio, and video. In addition to the initial or “home” page, a site may include any number of additional pages linked to each other in various ways.

More elaborate Web sites may add interactive features. The simplest such feature is a link that, when clicked on, allows the user to send an e-mail message to the site owner by simply typing in a message and clicking a “Send” button. Other types of links allow users to download documents with textual, graphical, or multimedia content from a Web site to their own computer. Some sites include interactive games, designed to entice the viewer to spend more time absorbing marketing messages. Sites often ask visitors to “register” by providing personal information, which the site owner may use to target marketing messages more accurately or to generate income by making the information available to other businesses.

The most advanced commercial sites allow users to purchase products online. Among the best known and most successful of these are sites owned by Dell Computers, which as of July 1998 was generating revenues of \$5 million per day selling computers on the Web;²⁰ Auto-by-Tel, which in November 1997 was

¹⁷See *ACLU v. Reno*, 929 F. Supp. 824, 836-38 (E.D. Pa. 1996), *aff’d*, 521 U.S. 844 (1997).

¹⁸As of April 15, 1999, Yahoo’s “Business and Economy/Companies” category contained 434,145 listings. *Yahoo Business and Economy* (visited Apr. 15, 1999) <http://www.yahoo.com/Business_and_Economy/>.

¹⁹Some courts have characterized this type of Web site as a “passive” site, and have identified other types of sites as “interactive” and “integral.” See *Weber v. Jolly Hotels*, 977 F. Supp. 327, 333 (D.N.J. 1997); *Agar Corp. v. Multi-Fluid, Inc.*, No. 95-5105, 1997 U.S. Dist. LEXIS 17121 (S.D. Tex. June 25, 1997); *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

²⁰See Michael Krantz, *Click Till You Drop*, TIME, July 20, 1998, at 34, 38.

realizing \$500 million in monthly automobile sales from its Web site; and Amazon.com.²¹

In addition to maintaining its own Web site, a company may publicize its site through advertisements placed on other Web sites. These generally take the form of rectangular banners with graphical content that is meant to be eye-catching. The banner is a link to the advertiser's own site, which the user may view simply by clicking on the banner.

B. Newsgroups

A newsgroup is a sort of electronic bulletin board containing postings that online visitors may read and respond to.²² Readily available newsreader software makes it easy to read messages that others have posted, and to compose and transmit one's own messages. Anyone with access to a newsgroup may view and respond to messages posted in it.²³ The responses are themselves available to all, and may invite further response. A series of postings on a particular topic, known as a "thread," resembles a conversation among any number of participants with the dialogue frozen and available for all to see. Newsgroup postings typically are deleted within a few days to a few weeks after they are posted (depending on how active the newsgroup is), in order to allow space on the host server for new postings.

Some newsgroups are Internet-based, while others are established by proprietary online services. Internet newsgroups, collectively referred to as the "Usenet," are maintained in a decentralized fashion on servers connected to the Internet that are located around the world. No single entity controls them. They are generally accessible by anyone who has an Internet connection that includes a newsgroup feed. Usenet newsgroups are arranged hierarchically by subject matter. Each newsgroup has a name, which also constitutes its "address" or means of accessing it, denoting the subject matter that it is designed to address. Popular top-level designations include "rec" (for recreation), "comp" (for computers), and "alt" (for alternative). The full name of a newsgroup may indicate a very specific subject matter—for example, *alt.books.isaac-asimov* or *rec.bicycles.racing*.

Other newsgroups are created and maintained by proprietary online services, such as America Online and CompuServe. These newsgroups, which may be referred to as "forums" or "discussion groups," are generally accessible only by members of the online service that hosts them.

Some newsgroups are created as forums for discussions of a commercial nature. For example, about two dozen Usenet newsgroups have names beginning with the designation "alt.business," such as *alt.business.home* and *alt.business.import-export*. But commercial postings are not limited to newsgroups that are designed to

²¹See DEPARTMENT OF COMMERCE, *supra* note 2, at 2.

²²See generally ED KROL, THE WHOLE INTERNET USER'S GUIDE & CATALOG 151-85 (2d ed. 1994).

²³Users generally cannot delete messages posted by others. However, it is possible to do so if one possesses the requisite skills. See Adam Gaffin & Ellen Messmer, *Censors Hit Cyber-Speech*, NETWORK WORLD, Oct. 31, 1994, at 1 (Top News Section) (describing the use of "cancelbots" to delete newsgroup messages), available in LEXIS, News Library, Papers File.

1999]

PROTECTING THE DIGITAL CONSUMER

receive them. In the past few years, it has become a common practice for vendors to post commercial messages in newsgroups regardless of their intended subject matter. This technique, known as off-topic posting, cross-posting, or "spamming," first gained wide notice in 1994 when it was employed by two immigration lawyers who posted messages advertising their services in over 5000 newsgroups.²⁴ Newsgroup spamming is viewed as highly offensive by people who access a newsgroup in order to find material on a particular topic, and instead must wade through screen after screen of commercial postings that are of no interest.

C. Electronic Mail

Electronic mail consists of messages, generally textual, that are transmitted over a computer network from a sender to one or more recipients.²⁵ Internet e-mail uses a virtual addressing scheme, in which a user's e-mail address is unrelated to her geographic location. Like those who communicate via Web pages, newsgroup postings, and chat sessions, the sender of an e-mail message creates or selects the content of the communication. Unlike those other forms of online communication, however, the sender of an e-mail message also determines the recipient of the communication, since an e-mail message is transmitted from point to point, rather than being made available for viewing by all comers.

Electronic mail may also serve as a one-to-many mode of communication, by using an Internet mailing list.²⁶ An Internet mailing list is a means of distributing e-mail messages easily to a preselected set of e-mail addresses, which may number from a handful up to thousands or millions. To use a mailing list, a member sends an e-mail message to an address defined by the list owner, whereupon the message is distributed automatically to all other members of the list. Some lists are "open," meaning that any e-mail user can join, thereby becoming a recipient of all messages posted to the list and obtaining the capability of posting messages to the list. Other lists are "closed": the person who maintains such a list performs a gatekeeper function, determining who will be allowed to participate. Mailing lists may also be either "moderated" or "unmoderated." With the latter, any message posted to the list is automatically distributed to all participants. With the former, the list owner screens incoming messages and decides which of them to pass along to the list participants.

Because members of an Internet mailing list generally do not know who the other members are, and cannot control the membership, they do not know who will receive the messages they post to the list. In this respect, Internet mailing lists resemble the more public forms of online communication: Web pages, newsgroup postings, and chat sessions.

Another way of turning e-mail into a one-to-many form of communication is through use of bulk e-mail software. Typically used to send unsolicited commercial messages, bulk e-mail software allows a user to distribute messages to a large number of recipients, drawn from a list that the sender compiles, rents, or purchases. Bulk e-mail differs from Internet mailing lists in that mailing list

²⁴See *infra* text accompanying note 65.

²⁵See *KROL*, *supra* note 22, at 101-37.

²⁶See *ACLU v. Reno*, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

members receive messages directed to the list only if they subscribe to it, whereas recipients of bulk e-mail generally have not made any such election. Senders of bulk e-mail typically have no information about those to whom they direct their messages, other than their e-mail addresses.

D. Chat Sessions

A chat session is a communications medium in which two or more participants can exchange textual messages in real time, regardless of their geographic location.²⁷ Multi-party chats may occur via the Internet, using a facility known as "Internet Relay Chat," or in a setting provided by a proprietary online service. The participants in a chat session are generally identified only by pseudonyms. A participant types in a message, which is then displayed almost instantaneously on the monitors of all other participants. Chat sessions sometimes have a designated subject matter, from which participants may freely diverge. Participants may enter and exit the chat session at will. Typically, in a multi-party chat, participants are unaware of the identities or geographic locations of the other participants.²⁸

Real-time textual exchange via the Internet may also occur on a point-to-point basis, through use of a server-based program called "talk" or various client-side programs, such as ICQ. In this sort of chat, the participants are known to each other.

III. VARIETIES OF ONLINE DECEPTIVE MARKETING PRACTICES

The varieties of deceptive marketing practices that are conducted via the Internet generally parallel what is found on the pre-Internet communications media.²⁹ However, the online medium is particularly conducive to particular types of fraud—for example, chain letters and other pyramid schemes, which are quickly propagated through bulk e-mail and pattern Web sites.

²⁷ See PAUL GILSTER, *THE INTERNET NAVIGATOR* 428 (2d ed. 1994).

²⁸ For a discussion of the nature and culture of real-time chat, see HOWARD RHEINGOLD, *THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER* 176-88 (HarperPerennial 1994) (1993).

²⁹ For a discussion of the varieties of Internet-based fraud, see DANIEL J. BARRETT, *BANDITS ON THE INFORMATION SUPERHIGHWAY* 47-122 (1996).

1999]

PROTECTING THE DIGITAL CONSUMER

Deceptive marketing practices that make use of the online medium typically involve other communications media as well. A solicitation carried on the Internet—by e-mail, on a Web site, or in a newsgroup or chat session—often refers the reader to a source of additional information about the offering. This may be a telephone number that accesses a recorded sales pitch, an automatic fax-back service, or a live salesperson. Payment is usually requested via check or money order sent through postal mail. However, it is possible for a fraudulent transaction to be conducted entirely online. This can occur if the solicitation is self-contained within a Web site or an e-mail message or newsgroup posting, and payment is made either through an online mechanism (e-cash) or by transmitting a credit card or bank account number online.

A. Fraudulent Online Conduct

Some of the most common types of online fraud include:

Pyramid schemes. Pyramid and multi-level marketing schemes have proliferated widely on the Internet.³⁰ Typically, the promoters of such schemes collect payment from consumers for the right to recruit new participants, and to collect commissions for doing so. Nearly all of the participants in these schemes lose money.³¹ Sometimes these are operated as Ponzi schemes, in which fees paid by participants lower in the pyramid are used to simulate earnings that are paid to earlier investors, thereby increasing the verisimilitude of the scheme. Operation of these schemes on a large scale can have devastating results, as occurred in Albania when a large proportion of the population lost most or all of their savings in several massive pyramid investment schemes.³² Enforcement authorities have brought several law enforcement actions against perpetrators of Internet-based pyramid schemes.³³

³⁰Pyramid schemes were the most prevalent form of online fraud in 1996, but dropped to fourth place in 1997 and seventh place in 1998. See Internet Fraud Watch, *Internet Fraud Statistics* (visited Apr. 14, 1999) <<http://www.fraud.org/internet/intstat.htm>>. On one day in December 1996, FTC investigators and other law enforcement agencies conducted an “Internet Pyramid Surf Day,” combing the Internet for examples of deceptive pyramid schemes. The search located over 500 Web sites and newsgroup postings offering such schemes. See *Pros Take on the Cons*, DALLAS MORNING NEWS, Dec. 13, 1996, at 12D.

³¹Losses resulting from these schemes can be enormous. In one case, the FTC halted an Internet-based pyramid scheme in which more than 150,000 consumers lost more than \$150 million. See *Pyramid Operators Settle with FTC*, ARIZ. REPUBLIC, Nov. 19, 1997, at E3.

³²See Tracy Wilkinson, *Pyramid Scheme Fever Scorches Albanian Society*, L.A. TIMES, Feb. 3, 1997, at A1.

³³The FTC has brought such actions in *FTC v. Cano*, No. 97-7947-CAS-(AJWx) (C.D. Cal. filed Oct. 29, 1997); *FTC v. JewelWay Int’l, Inc.*, No. CV97-383 TUC JMR (D. Ariz. filed June 24, 1997); and *FTC v. Fortuna Alliance, L.L.C.*, No. C96-799M (W.D. Wash. filed May 23, 1996). See *Prepared Statement of the Federal Trade Commission on “Internet Fraud” Before the Subcommittee on Investigations of the Governmental Affairs Committee, United States Senate (Feb. 10, 1998)* (visited Mar. 17, 1999) <<http://www.ftc.gov/os/1998/9802/internet.test.htm>> [hereinafter *FTC Prepared Statement*]. The Australian Competition and Consumer Commission obtained an order against Destiny Telecom International Inc., based on allegations it operated a pyramid scheme propagated in part through a Web site. See *Australian Competition & Consumer Comm’n v. Destiny Telecom Int’l Inc.*, No. BC9704570, 1997 AUST FEDCT LEXIS 758

Chain letters. Chain letters, which are a type of pyramid scheme, promise recipients that they will make a fortune if they follow simple instructions, which typically involve sending small sums of money (five dollars or less) to each of four or five listed individuals, inserting one's own name in place of the top name on the list, and propagating the scheme by forwarding the letter to others.³⁴ The online medium is ideally suited to this kind of scheme, as it eliminates the greatest expense required of participants: postage to transmit the solicitation to others. Using the techniques of bulk e-mail and newsgroup postings, chain letters can be forwarded to thousands or millions of potential new participants at virtually zero marginal cost. This sort of scheme is resistant to law enforcement action, given the ubiquity of chain letters on the Internet and the fact that most of the perpetrators are also victims of the scheme.³⁵

Bogus business opportunities. Internet communications are used to promote business opportunities that fall short of the claims made for them. Many of these are nothing more than disguised pyramid schemes.³⁶ Authorities have brought enforcement actions against online marketers who touted business opportunities involving credit repair services,³⁷ work-at-home schemes,³⁸ locating people who are owed money by a government agency,³⁹ franchises,⁴⁰ defrauding the postal system,⁴¹ and online shopping programs.⁴²

(FCA Sept. 17, 1997). The New York Attorney General settled cases with the proprietors of 12 online pyramid sites. See *Vacco's Crackdown Nets 'Net Schemers*, N.Y. POST, Mar. 12, 1998, at 42.

³⁴A version of a chain letter which circulated widely on the Internet in 1997 begins with the announcement: "GUARANTEED \$50,000 IN 90 DAYS." It urges recipients to send five dollars to each of four people on a list, ordering a "report" from each of them. The letter states that because this scheme involves the selling of a product or service, it complies with U.S. law—a view that the U.S. Postal Service does not share. See U.S. Postal Inspection Serv., *Chain Letters* (visited Mar. 17, 1999) <<http://www.usps.gov/websites/depart/inspect/chainlet.htm>> ("Do not be fooled if the chain letter is used to sell inexpensive reports on credit, mail order sales, mailing lists, or other topics. The primary purpose is to take your money, not to sell information. 'Selling' a product does not ensure legality."). This sort of scheme is "the classic pyramid." BARRETT, *supra* note 29, at 51.

³⁵In a nontraditional law enforcement effort, the FTC and the U.S. Postal Inspection Service sent warning letters to more than 1000 people whose names were found on bulk e-mail solicitations that appeared to be fraudulent. Some 80% of these solicitations were chain letters. See Leslie Miller, *Senders of Junk E-mail Warned*, USA TODAY, Feb. 6, 1998, at D1.

³⁶See BARRETT, *supra* note 29, at 51-53 (discussing mailing list sales, advertising by fax, stuffing envelopes, shareware sales, sales of printed reports, T-shirt sales, and other schemes).

³⁷See Bryan Coryat, 121 F.T.C. 784, 795 (1996) (credit repair agency business opportunity).

³⁸See Timothy R. Bean, 121 F.T.C. 772, 781 (1996) (publishing and printing); Robert Serviss, 121 F.T.C. 820, 831 (1996) (sales of business reports).

³⁹See Sherman G. Smith, 121 F.T.C. 807, 817 (1996) (locating people owed refunds on their mortgage insurance).

⁴⁰See *FTC v. Chappie* (Infinity Multimedia), No. 96-6671-CIV-Gonzalez (S.D. Fla. filed June 24, 1996) (CD-ROM display racks).

⁴¹See Complaint, *Minnesota v. Dean* (Minn. Dist. Ct. filed July 18, 1995) (on file with author) (selling information on obtaining first-class mail services for two cents).

1999]

PROTECTING THE DIGITAL CONSUMER

In an effort to identify fraudulent business opportunities offered on the Web, the International Marketing Supervision Network conducted an “International Internet Sweep Day” in November 1997. In that action, law enforcement authorities from twenty-four countries searched the Web for “get-rich-quick” schemes and other money-making opportunities that appeared of dubious legitimacy. As part of the effort, participating law enforcement agencies sent hundreds of e-mail messages to proprietors of these sites, warning them of the requirement that they conform with applicable laws.⁴³

Credit repair schemes. Fraudulent credit repair schemes involve claims that the seller can remove, or can instruct the consumer how to remove, accurate, non-obsolete negative information from the consumer’s credit report.⁴⁴

“Miracle” health and diet products. Several cases have been brought against promoters of purported cures for AIDS and other diseases,⁴⁵ and mood-enhancing herbal products.⁴⁶ The U.S. Food and Drug Administration has warned consumers not to purchase home abortion kits or female self-sterilization kits that are offered via the Internet, as they pose significant health risks.⁴⁷

Items paid for, but never delivered. An Internet-based scam may be as simple as accepting payment for goods or services, and then failing to deliver as promised.⁴⁸

Investment and securities scams. One common type of Internet-based securities scam is the offer and sale of phoney or overvalued investments. “Ranging from traditional securities like stocks and bonds, to more esoteric investment

⁴²See *FTC v. Intellicom Servs., Inc.*, No. 97-4572 TJH (Mx) (C.D. Cal. filed June 23, 1997) (investment in a “virtual shopping mall”); see also *Field of Schemes—List of Defendants in FTC Cases* (visited Apr. 14, 1999)

<<http://www.ftc.gov/opa/1997/9707/field2.htm>>.

⁴³See J. Scott Orr, *U.S. to Net Surfers: Beware of Scams*, STAR-LEDGER (Newark, N.J.), Nov. 18, 1997, at 30.

⁴⁴See *FTC v. Cooley*, No. CIV-98-0373-PHX-RGS (D. Ariz. filed Mar. 4, 1998); *FTC v. Consumer Credit Advocates, P.C.*, No. 96 Civ. 1990 (S.D.N.Y. filed Mar. 19, 1996); *FTC v. Corzine*, No. CIV-S-94-1446 (E.D. Cal. filed Nov. 21, 1994); Lyle R. Larson, 121 F.T.C. 851, 857 (1996); Rick A. Rahim, 121 F.T.C. 842, 847 (1996); Martha Clark, 121 F.T.C. 799, 804 (1996); see also *FTC Cases in “Operation Eraser”* (visited Mar. 24, 1999) <<http://www.ftc.gov/opa/1998/9803/erascase.htm>>; *FTC Prepared Statement*, *supra* note 33.

⁴⁵See *Massachusetts v. Phillips*, No. 96-00661 (Norfolk Superior Ct., temporary restraining order Apr. 25, 1996) (herbs and battery-powered device as cure for AIDS); *Minnesota v. McClendon*, No. CO-95-7224 (Ramsey County, Minn. Dist. Ct., filed Aug. 22, 1995) (germanium sesquioxide as cure for AIDS and other diseases); Complaint, *Illinois v. Viva America Mktg., Inc.* (Sangaman County, Ill. Cir. Ct.) (on file with author) (germanium sesquioxide to lower cholesterol, reduce arthritic joint pain, and treat AIDS and cancer).

⁴⁶See *Global World Media Corp.*, FTC Docket No. C-3772 (Oct. 9, 1997) (ephedrine product), available in WESTLAW, FATR Library, FTC Database.

⁴⁷See Margaret Mannix, *Have I Got a Deal for You!*, U.S. NEWS & WORLD REP., Oct. 27, 1997, at 59-60.

⁴⁸See *FTC v. Brandzel*, No. Civ. 96C 1440 (N.D. Ill. filed Mar. 13, 1996) (computer memory chips paid for but not delivered); *FTC v. Hare*, No. 98-8194 CIV (S.D. Fla. filed Mar. 30, 1998) (failure to deliver goods bought at online auction); Kathy Kristof, *Watch Your Wallet While Surfing the Net as Reports of Fraud Triple from 1996*, DETROIT NEWS, Oct. 2, 1997, at B1 (after accepting deposit and not delivering the goods, company informed consumer that it had scammed him).

opportunities involving anything from eel farms, cattle breeding, and oil and gas drilling to cyber-casinos, multi-level marketing programs, and portable nuclear reactors, securities hawked over the Internet come in a huge variety of shapes and sizes.”⁴⁹ Another technique is the dissemination of false information in order to manipulate the price of a security. Such disinformation may be spread through newsgroup postings, in chat sessions, or via online newsletters. Typically the perpetrator engages in what is known as “pump and dump”: false information is used to pump up the price of a stock through the creation of spurious demand, whereupon the perpetrator dumps his holdings on unwitting buyers at an enormous profit.⁵⁰ Other types of online misconduct relating to securities include: offerings of unregistered securities and illegal off-exchange futures; dispensing fraudulent investment advice; broker-dealer misconduct; conflicts of interest by promoters and investment managers;⁵¹ and failure to comply with registration and disclosure requirements.⁵² Businesses posing as online banks are also becoming more prevalent.⁵³

Gambling. Several states have taken action against online gambling sites. The state of Missouri sued a Delaware corporation, which maintained its principal place of business in Pennsylvania, based on a gambling Web site established by the company’s wholly owned subsidiary in Grenada. The court issued an order forbidding the company to market its gambling services to residents of Missouri,⁵⁴ disagreeing with the defendant’s views as to whether the court had jurisdiction.⁵⁵ The company violated the court’s order, and the company and its president were

⁴⁹Joseph J. Cella III & John Reed Stark, *SEC Enforcement and the Internet: Meeting the Challenge of the Next Millennium*, 52 BUS. LAW. 815, 821 (1997); see also *id.* at 837-42 (discussing enforcement actions involving investment scams).

⁵⁰See *id.* at 825-28, 842-43 (detailing process of “pump and dump” and describing enforcement action against a pump-and-dump scheme yielding illegal profits of more than \$10 million).

⁵¹See TECHNICAL COMM. OF THE INT’L ORG. OF SEC. COMM’NS, REPORT ON ENFORCEMENT ISSUES RAISED BY THE INCREASING USE OF ELECTRONIC NETWORKS IN THE SECURITIES AND FUTURES FIELD 5-6 (Sept. 1997).

⁵²See Steven Jay Marks, [1994-1996 Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 26,791 (C.F.T.C. Sept. 3, 1996); J. Spencer Brown, [1994-1996 Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 26,790 (C.F.T.C. Sept. 3, 1996).

⁵³See Tom Lowry, *Bogus Cyberbanks Pose Increasing Threat*, USA TODAY, Apr. 6, 1998, at B1; Peter Pae, *In a Spreading Net, a Federal Lookout for Sharks*, WASH. POST, June 9, 1998, at F1.

⁵⁴See *Nixon v. Interactive Gaming & Communications Corp.*, No. CV97-7808 (Jackson County, Mo. Cir. Ct., injunction entered May 22, 1997). Missouri also sued an Idaho Indian tribe and associated companies based on their maintenance of an Internet gambling site that was made available to residents of Missouri. See *Missouri Attorney General Obtains Order Blocking Indian Tribe’s Online Gambling*, 3 Electronic Commerce & L. Rep. (BNA) 191 (Feb. 11, 1998) (citing *Missouri v. UniStar Entertainment*, No. CV-198-7CC (Jackson County, Mo. Cir. Ct., temporary restraining order issued Jan. 29, 1998)).

⁵⁵A representative of Interactive Gaming & Communications Corp. opined, “What we’re doing is not illegal. It boils down to the fact that the United States forgets it doesn’t have jurisdiction over the world. We’re fully licensed in Grenada.” Vira Mamchur Schwartz, *Place Your Bets, Break the Law*, INTERNET WORLD, Feb. 1997, at 16, 16.

1999]

PROTECTING THE DIGITAL CONSUMER

subsequently indicted by a state grand jury.⁵⁶ The state of Minnesota brought a similar action against a Nevada corporation.⁵⁷

Internet-based gambling has drawn the attention of the U.S. Congress, which has considered legislation banning the practice.⁵⁸

Spoofing. Spoofing involves using online communications to impersonate another person or entity.⁵⁹ Several characteristics of the online medium make it easy to engage in this practice: the addressing scheme is virtual; domain names are handed out without any verification of the identity of the domain owner; communications are at a distance; and technical aspects of the Internet make it easy to forge identifying information that appears in e-mails. A swindler could use this technique by setting up a Web site with a domain name that suggests a well-known company but is different from the domain actually owned by the company, offering on the site a product that the actual company might sell, and then receiving payment from unsuspecting consumers.⁶⁰ In one variation of this scheme, swindlers set up a phony Web page for "Loyola State University," and offered bachelor's, master's, and doctoral degrees for fees ranging from \$1995 to \$2795.⁶¹ Although there are several universities in the United States containing the name "Loyola," there is no "Loyola State University."

Swindlers may also send e-mail solicitations purporting to come from somebody else. In one case, a scammer sent an e-mail message, in bulk, purporting to be from a representative of America Online, asking the recipients to help the company update its records by providing information such as name, address, social security number, mother's maiden name, and credit card number. Likewise, hackers may commandeer an online user's identity and use it to commit nefarious acts.⁶²

Scams that are unique to the Internet. Most of the fraudulent online activities that have been observed to date are simply transpositions of scams that have long been practiced using other means of communication. Some of these scams are particularly at home online: for example, pyramid schemes may be disseminated through pattern Web sites, and spoofing is more easily accomplished online than through other media. In addition, there is a new class of scams that are possible only in the online context. An example of this is a case in which swindlers

⁵⁶See Doug Abrahms, *Missouri Fights Internet Gambling in Court*, WASH. TIMES, Aug. 6, 1997, at B7.

⁵⁷See *Minnesota v. Granite Gate Resorts, Inc.*, No. C6-95-007227, 1996 WL 767431 (Minn. Dist. Ct. Dec. 11, 1996), *aff'd*, 568 N.W.2d 715 (Minn. Ct. App. 1997), *aff'd*, 576 N.W.2d 747 (Minn. 1998).

⁵⁸See Alan K. Ota, *The Virtual Casino*, CONG. Q., Jan. 23, 1999, at 192; Mark Grossman, *Net Casinos Have High Legal Stakes*, LEGAL TIMES, Oct. 6, 1997, at 23, 28.

⁵⁹See John Burgess, *Untangling Pirate-Rigged Web Sites*, WASH. POST, Mar. 18, 1996, at 17 (Washington Business Section).

⁶⁰For example, a swindler could register the domain name "sony_corp.com", set up a Web site at <www.sony_corp.com> with content indicating that the site is owned by the well-known consumer electronics corporation, and offer bogus Sony-brand electronic products for sale. Sony Corp.'s actual site is located at <www.sony.com>, and the "sony_corp.com" domain is at this writing unregistered.

⁶¹See Mannix, *supra* note 47, at 59.

⁶²See Jared Sandberg, *Hackers Prey on AOL Users with Array of Dirty Tricks*, WALL ST. J., Jan. 5, 1998, at B1 (describing a variety of hacker techniques, including "phishing," "carding," "instant message bombing," "e-mail bombing," and "tossing").

advertised the availability of adult-oriented images through their Web site. Users were told they could access the images free of charge if they first downloaded viewer software. Once downloaded, this software turned off the sound on the user's modem, hung up the connection to the user's Internet service provider, and dialed a telephone number in Moldova which reconnected the user to the Internet. Users only learned they had been scammed when they received a telephone bill containing a hefty charge for the international call to Moldova—which might have lasted for hours, as the software maintained the overseas telephone connection even after the user signed off the Internet. The swindlers received a portion of the long distance charges.⁶³ Other types of “Trojan horse” programs—such as “one that records your name and password as you log on to an electronic account and then passes them along to someone else—who might be able to read your E-mail, draw on your checking account, or gain access to some other private domain”—may be on the horizon.⁶⁴

Spamming. Spamming refers to the sending of bulk unsolicited commercial e-mail, and making commercially oriented off-topic newsgroup postings. The first widely noted use of this marketing technique occurred in 1994, when a law firm in Phoenix, Arizona posted an advertisement in thousands of Usenet newsgroups, offering their services as immigration lawyers. The originators of this spam, Laurence Canter and Martha Siegel, became instantly famous and widely reviled throughout the community of Internet users for what was viewed as a serious breach of Internet etiquette.⁶⁵

While the techniques of bulk commercial e-mail and newsgroup postings are not inherently deceptive,⁶⁶ they are to a significant extent employed as a delivery

⁶³See *FTC v. Audiotex Connection, Inc.*, No. CV-97-0726 (E.D.N.Y. filed Feb. 13, 1997).

⁶⁴Marshall Jon Fisher, *Moldovascam.com: A Complicated Case of Electronic and Telephone Fraud Suggests Just How Vulnerable Internet Users May Be*, ATLANTIC MONTHLY, Sept. 1997, at 19, 19.

⁶⁵See Dee Pridden, *How Will Consumers Be Protected on the Information Superhighway?*, 32 LAND & WATER L. REV. 237, 239-40 (1997); Mary Furlong & Stefan B. Lipson, *Trekking the Internet*, SATURDAY EVENING POST, May-June 1997, at 54, 55. Canter and Siegel cemented their unpopularity in the online world by publishing a book advising would-be online entrepreneurs to exploit the commercial possibilities of the Internet through techniques similar to those that catapulted the authors to fame. See LAURENCE A. CANTER & MARTHA S. SIEGEL, *HOW TO MAKE A FORTUNE ON THE INFORMATION SUPERHIGHWAY* (1994).

⁶⁶The sending of unsolicited commercial e-mail, though not inherently deceptive under trade practices laws, may constitute an actionable violation of private rights. Thus, Internet service providers have filed actions against senders of bulk e-mail alleging violations of the Lanham Act, 15 U.S.C.A. § 1051 (West 1997 & Supp. 1999), Computer Fraud and Abuse Act, 18 U.S.C.A. § 1001 (West 1976 & Supp. 1999), state computer crimes statutes, and common law trespass to chattels. See *America Online, Inc. v. IMS*, No. 98-0011-A (E.D. Va. filed Jan. 6, 1998); *America Online, Inc. v. LCGM, Inc.*, No. 98-102-A (E.D. Va. filed Jan. 22, 1998); *Bigfoot Partners, L.P. v. Cyber Promotions, Inc.*, 97 Civ. 7397 (S.D.N.Y. filed Oct. 6, 1997); *America Online, Inc. v. Over the Air Equipment, Inc.*, No. 97-1547-A (E.D. Va. filed Oct. 2, 1997); *Concentric Network Corp. v. Wallace*, No. C-96 20829-RMW(EAI) (N.D. Cal. injunction entered Nov. 5, 1996). The sender of bulk e-mail who used a forged header pointing to a domain owned by an innocent third party was sued by the domain owner and the Internet service provider that hosted the domain. The complaint was based on common law nuisance, trespass, conversion, and negligence, as well as a state

1999]

PROTECTING THE DIGITAL CONSUMER

mechanism for fraudulent solicitations. One sampling of unsolicited e-mail found that nearly one-third consisted of solicitations for multi-level marketing, make-money-fast, and work-at-home schemes⁶⁷—types of solicitations that experience teaches are likely to be fraudulent.⁶⁸ Unsolicited e-mail relating to investments tops the list of complaints received by the U.S. Securities and Exchange Commission Division of Enforcement.⁶⁹ It is also the number one complaint that America Online, the world's largest online service, receives from its e-mail subscribers.⁷⁰

B. Misleading Online Conduct

Enumerating the varieties of *misleading* online conduct is more difficult than setting forth the range of *fraudulent* conduct. While nearly all jurisdictions are in agreement as to the basic definition of fraud, the definition of misleading conduct varies from one legal system to another. What is considered misleading under one system is a standard marketing practice in another. It is in the realm of misleading conduct that the problem of geographic indeterminacy becomes most acute, as a seller undertaking a marketing practice that is legal where the seller is located may find that it is illegal in some jurisdictions where the marketing message is received.

A European Commission Green Paper catalogues the variations among the misleading marketing practices laws of the fifteen European Union ("EU") member countries.⁷¹ The rules governing the use of comparative advertising vary

computer crimes statute. *See* Parker v. C.N. Enters., No. 97-06273 (Travis County, Tex. Dist. Ct., injunction entered Nov. 10, 1997).

⁶⁷*See* Ram Avrahami, Comments Submitted to Public Record in FTC Public Workshop on Consumer Information Privacy (Apr. 15, 1997), *available at* <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/avraham.htm>>.

⁶⁸The volume of unsolicited commercial e-mail ("UCE")—and therefore the volume of fraudulent UCE—is very high. UCE may amount to 10% of all e-mail, and one large Internet service provider finds that at times up to 50% of the e-mail traffic it carries is UCE. *See* John Markoff, *Internet Is Expanding Arms Race with Junk E-Mail*, N.Y. TIMES, Mar. 17, 1998, at D1. According to one report, 40% of all Usenet traffic consists of UCE, and another 40% is made up of "cancel" messages sent by anti-spammers. *See* Janet Kornblum, *Antispammers Going on "Strike,"* CNET NEWS.COM (Apr. 3, 1998) <<http://www.news.com/News/Item/0,4,20713,00.html>>.

⁶⁹*See* Cella & Stark, *supra* note 49, at 832.

⁷⁰*See* Patricia Riedman, *Juno Sues Over Falsified Addresses*, ADVERTISING AGE, Dec. 1, 1997, at 68; FTC Public Workshop on Consumer Information Privacy (June 12, 1997), transcript at 51 (testimony of Jill Lesser), *available at* <<http://www.ftc.gov/bcp/privacy/wkshp97/volume3.pdf>>.

⁷¹*See* Green Paper on Commercial Communications in the Internal Market, COM(96)192 final. They include the following:

Misleading advertising: United Kingdom bans advertising by barristers; French Bar Associations forbid advertising by individuals, but not by the profession as a whole; Germany limits discounting to three percent; other EU countries allow price advertising, as long as it is not misleading or anti-competitive; Scandinavian countries encourage price advertising; there are detailed and inconsistent regulations on trading stamps and discounts in Greece, Portugal, Spain, and Italy; there is an effective ban on "three for the price of two" promotions in Germany and Denmark. *See id.* at 21-22.

greatly from one country to another,⁷² as do the rules concerning direct advertising, television and radio advertising, prize competitions, price advertising, advertising directed at children, and use of trademarks and copyrights.⁷³ Internet marketers may wish to make use of any or all of these marketing practices. The problem of geographic indeterminacy makes it a hazardous undertaking to engage in any of them.

IV. SPECIAL CHARACTERISTICS OF THE ONLINE MEDIUM

Promotional gifts: Germany strictly limits them; Belgium bans tie-in offers, but Netherlands allows them with restrictions; Denmark allows promotions that are of low value, and gifts that are closely associated with the product purchased; other EU countries have fewer restrictions, but there are some very specific requirements: for example, promotions in Italy must be approved by the Ministry of Finance. *See id.* at 23.

Prize promotions: Lotteries are banned in Denmark, Belgium, and Finland; lotteries require state permits in Netherlands and Italy; France and Germany ban games requiring purchase to participate; there are various restrictions on the types and value of prizes. *See id.* at 23-24.

Sponsorship restrictions: Types of sponsorship that are banned in some countries are completely unregulated in others. *See id.* at 24-25.

Commercial communications directed at children: Sweden bans advertising and sponsorship of programs aimed at children under age 12; Greece bans television advertising of toys to children between 7:00 a.m. and 10:00 p.m. *See id.* at 26.

Commercial communications for food products: Some countries extend labeling requirements to advertising, others do not; in advertising confectionery products, some countries require including an image of a toothbrush, which requires a different TV advertisement for such countries. *See id.* at 27.

Advertising of pharmaceuticals: Some countries ban advertising of over-the-counter ("OTC") drugs on audio-visual media; others require pre-notification for such advertising; some prohibit sales promotions for OTC drugs; lists of prescription drugs vary from country to country, so sellers can only do pan-European advertising of drugs that are OTC in all countries. *See id.* at 27-28.

Advertising of financial services: Disclosure requirements vary widely. *See id.* at 28.

⁷²*See* Jenna D. Beller, *The Law of Comparative Advertising in the United States and Around the World: A Practical Guide for U.S. Lawyers and Their Clients*, 29 INT'L LAW. 917, 925-43 (1995); Alexander Gigante, *Ice Patch on the Information Superhighway: Foreign Liability for Domestically Created Content*, 14 CARDOZO ARTS & ENT. L.J. 523, 536-41 (1996) (contrasting comparative advertising law of the United States and Italy). The European Commission has enacted a directive that provides baseline rules governing comparative advertising within the EU. *See* Directive 97/55/EC of the European Parliament and of the Council of 6 October 1997 Amending Directive 84/450/EEC Concerning Misleading Advertising So As To Include Comparative Advertising, 1997 O.J. (L 290) 18, corrected at 1998 O.J. (L 194) 54. EU member countries must implement that directive by April 23, 2000. *See id.*

⁷³*See* ADVERTISING LAW IN EUROPE AND NORTH AMERICA (James R. Maxeiner & Peter Schotthöfer eds., 1992). Ironically, many of the legal restrictions on marketing practices that exist in European countries, and that now interfere with the ability of businesses to follow a unitary marketing strategy, had their origins as measures designed to benefit businesses by limiting competition. *See* J. Bergevin, *Sales Promotions—The Reasons Underlying Restrictions in Europe*, COM. COMM., Jan. 1998, at 1, 2 & n.4.

1999]

PROTECTING THE DIGITAL CONSUMER

In some respects, the problem of deceptive marketing practices on the Internet is nothing new. “The swindles over the Internet are no different from the confidence games of the past; the only difference is the medium.”⁷⁴ However, certain characteristics of the online medium give rise to special difficulties in controlling deceptive marketing practices that are absent, or are present only to an attenuated degree, with marketing methods that use other communications media. These same characteristics give rise to legal uncertainty for online sellers, making it difficult for them to structure their online activities so as to be consistent with trade practices laws. These characteristics fall into five categories.

⁷⁴Cella & Stark, *supra* note 49, at 835.

First, because the cost of making a communication over the Internet and the delivery time of a communication are independent of the geographic separation of the parties to the communication, the development of electronic commerce will result in a substantial increase in transactions involving a seller in one country and a buyer in another. *Second*, the nature of the medium enables the perpetrator of an online scam to evade law enforcement efforts by moving the operation relatively quickly and easily from one jurisdiction to another, and by disguising his identity. *Third*, because the costs of promoting a commercial activity via the Internet are relatively modest, the Internet opens the doors to an enormous flood of new entrepreneurs, some of whom will engage in illegal conduct. *Fourth*, in most cases it is impossible for the sender of a communication to identify the geographic location of the recipient of the communication, or to limit the availability of a communication to a geographic or political subdivision of the online community. *Fifth*, it is often unclear how the existing regulatory structure applies to the online medium.

A. Increased Volume of Cross-Border Transactions

Because the cost of making a communication over the Internet is independent of the geographic separation of the parties to the communication, and because there is no significant time delay in receipt of an online communication regardless of the distance the message travels, the development of electronic commerce is likely to result in a substantial increase in transactions involving a seller in one country and a buyer in another.⁷⁵ Cross-border commercial transactions raise difficulties for both consumers and sellers that are absent in the domestic context.

1. Extraterritorial Assertion of Jurisdiction

⁷⁵See [AUSTRALIAN] FEDERAL BUREAU OF CONSUMER AFFAIRS, UNTANGLING THE WEB: ELECTRONIC COMMERCE AND THE CONSUMER 20 (1997) (“[T]he proportion of consumer transactions involving a foreign supplier is likely to increase significantly.”).

In most cases, however, international transactions remain constrained by the cost of international parcel delivery. According to a study by the OECD’s Committee on Consumer Policy, the cost of delivering a parcel across an international border is two to four times the cost of a delivery of roughly the same distance within a domestic market. See *International Parcel Delivery*, at 10, OECD Doc. OCDE/GD(97)151, available at <http://www.oecd.org/dsti/sti/it/consumer/prod/e_97-151.htm>; *The Once and Future Mall*, ECONOMIST, Nov. 1, 1997, at 68.

Delivery costs become irrelevant in the case of “digital goods,” such as data, software, or digitized music, which may be delivered via the Internet over the same path through which the order was received. The volume of software delivered digitally in the United States is presently less than one percent of the total, but “most analysts believe that a large amount of software will eventually be distributed electronically.” Lisa Bransten, *On-Line Larceny Prompts Venture to Develop Lucrative New Business*, WALL ST. J., Aug. 4, 1997, at A11.

1999]

PROTECTING THE DIGITAL CONSUMER

The frontierless nature of online communications will increasingly give rise to commercial disputes in which the disputants, and the instruments through which they communicate, are located in several different jurisdictions. In many such situations, application of the existing rules will not raise any difficult jurisdictional issues. “When cyberspace is simply a medium of direct communication between people—much like the telephone, mail, or fax—we should expect that the legal issues will not be materially different from issues in ‘real’ space.”⁷⁶ The same is true when the parties to a dispute arising from online communications are located within a single jurisdiction. However, in other contexts the special characteristics of online communications raise issues that are crucial from the standpoint of determining which legislatures may prescribe rules applicable to particular transactions and which courts may assert jurisdiction over the parties to a dispute.

Two aspects of jurisdiction require consideration: jurisdiction to prescribe and jurisdiction to adjudicate.⁷⁷

a. Jurisdiction to Prescribe

Jurisdiction to prescribe may be defined as “the authority of a state to make its law applicable to persons or activities.”⁷⁸ Traditionally, a state had jurisdiction to prescribe concerning conduct taking place within its territory and with respect to its nationals located abroad. That formalistic approach has increasingly given way to

conceptions better adapted to the complexities of contemporary international intercourse. . . . Territoriality and nationality remain the principal bases of jurisdiction to prescribe, but in determining their meaning rigid concepts have been replaced by broader criteria embracing principles of reasonableness and fairness to accommodate overlapping or conflicting interests of states, and affected private interests.⁷⁹

As these criteria are applied in the *Restatement (Third) of the Foreign Relations Law of the United States*, a state has jurisdiction to prescribe with respect to “conduct outside its territory that has or is intended to have substantial effect within its territory,”⁸⁰ subject to the limitation that such exercise of jurisdiction must not be “unreasonable.”⁸¹ The reasonableness of a particular exercise of jurisdiction is gauged by reference to a variety of factors,⁸² most of which raise no

⁷⁶I. Trotter Hardy, *The Proper Legal Regime for “Cyberspace,”* 55 U. PITT. L. REV. 993, 1000 (1994).

⁷⁷A third aspect of jurisdiction, jurisdiction to enforce, concerns the authority of a state “to induce or compel compliance or to punish noncompliance with its laws or regulations.” RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 401(c) (1987) [hereinafter RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW]. See discussion of enforcement of judgments *infra* text accompanying notes 106-09.

⁷⁸RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW, *supra* note 77, § 401 introductory note; *see id.* § 401(a).

⁷⁹*Id.* § 402 introductory note; *see also* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 298 (3d ed. 1979).

⁸⁰RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW, *supra* note 77, § 402(1)(c).

⁸¹*Id.* § 403.

⁸²*See id.*

especially novel difficulties when applied to online conduct.⁸³ One of the factors—“the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory”⁸⁴—invokes the criteria of *location* and *foreseeability*, which, as discussed below, may be of uncertain application in the online context.

b. Jurisdiction to Adjudicate

Jurisdiction to adjudicate, commonly also referred to as jurisdiction *in personam* or personal jurisdiction, refers to “the authority of a state to subject particular persons or things to its judicial process.”⁸⁵ Jurisdiction to prescribe and jurisdiction to adjudicate “are often interdependent” but, because they serve different purposes, “balancing the competing interests in the different contexts can lead to different results.”⁸⁶

The factors relevant to resolving an issue of *in personam* jurisdiction that are peculiarly problematic in the online context are, as with jurisdiction to prescribe, *location* and *foreseeability*. The *location* of a person engaging in conduct giving rise to a dispute is crucial as a threshold matter, since it determines whether an assertion of jurisdiction is extraterritorial: if the person is deemed to be located within the forum state, assertion of jurisdiction under the territoriality principle is uncontroversial.

As with jurisdiction to prescribe, the exercise of *in personam* jurisdiction is proper under the Restatement approach only if “reasonable.” To be reasonable, exercise of jurisdiction must be based on the existence of adequate “links” between the conduct sought to be regulated and the regulating state. Several of the

⁸³For example, these factors include: connections between the regulating state and the person responsible for the regulated activity or those the regulation is designed to protect; the importance of the regulation to the regulating state and to other states; impact of the regulation on justified expectations; importance of the regulation to the international system; consistency of the regulation with international traditions; and the likelihood of conflict with another state. *See id.* § 403(2).

⁸⁴*Id.* § 403(2)(a). The federal antitrust statutes incorporate a nearly identical formulation, authorizing jurisdiction over foreign trade or commerce that has “a direct, substantial, and reasonably foreseeable effect” on commerce. Sherman Act, 15 U.S.C. § 6a (1994); Federal Trade Commission Act, 15 U.S.C. § 45(a)(3) (1994).

European Community (“EC”) law has equivocated in its adherence to the “effects test.” *See C.S. KERSE, E.C. ANTITRUST PROCEDURE 285-90* (3d ed. 1994). The corresponding jurisdictional doctrine under EC law, known as the “implementation test,” holds that the existence of jurisdiction depends not on “the place where the [allegedly anticompetitive] agreement, decision or concerted practiced was formed,” but rather “the place where it is implemented.” *Joined Cases 89, 104, 114, 116, 117, 125-29/85, A. Ahlström Osakeyhtiö v. Commission (“Wood Pulp”), 1988 E.C.R. 5193, 4 Common Mkt. Rep. (CCH) ¶ 14,491, at 18,612* (Sept. 27, 1988). In practice, the “implementation test” yields very nearly the same results as the U.S. “effects test.” *See UNITED STATES DEP’T OF JUSTICE AND THE FED. TRADE COMM’N, ANTITRUST ENFORCEMENT GUIDELINES FOR INTERNATIONAL OPERATIONS 12 n.51* (1995). “The merger laws of the European Union, Canada, Germany, France, Australia, and the Czech and Slovak Republics, among others, take a similar approach.” *Id.*

⁸⁵RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW, *supra* note 77, § 401 introductory note; *see id.* § 401(b).

⁸⁶*Id.* § 401 introductory note.

1999]

PROTECTING THE DIGITAL CONSUMER

applicable factors depend on factors of location and foreseeability: (1) whether the person or thing over which jurisdiction is asserted is “present in the territory of the state”; (2) whether the person “carries on business” or “activity” in the state; (3) whether an activity occurring outside the state had “a substantial, direct, and foreseeable effect within the state”; and (4) whether a thing is “owned, possessed, or used in the state.”⁸⁷

The location of conduct is a decisive factor under several provisions of the Brussels Convention, which allows a person to be sued outside the state of his domicile (1) “in matters relating to a contract, in the courts for *the place of performance of the obligation in question*”; and (2) “in matters relating to tort, delict or quasi-delict, in the courts for *the place where the harmful event occurred*.”⁸⁸ The Convention also allows a consumer to bring a breach-of-contract action in a forum other than the one in which the defendant is domiciled if “in the State of the consumer’s domicile the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising.”⁸⁹ The location of defendant’s conduct is also decisive under many state “long-arm” statutes, which allow assertion of jurisdiction over a person located outside the forum state if the person transacted business or caused harm within the state.⁹⁰

The analysis of *in personam* jurisdiction under constitutional due process requirements depends in part on the foreseeability that the defendant’s conduct will have consequences in the forum state.⁹¹ Foreseeability of consequences in the forum state is also a necessary ingredient of the due process requirement that jurisdiction be based on “some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of its laws.”⁹²

⁸⁷*Id.* § 421(2). The other reasonableness factors—domicile, residence, and nationality of a person; state pursuant to whose laws a corporation is organized or a vehicle is registered; and consent to exercise of jurisdiction—raise no special issues in the online context.

⁸⁸Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, Sept. 27, 1968, art. 5(1), (3), 1990 O.J. (C 189) 1, 69 (consolidated) (each emphasis added) [hereinafter Brussels Convention].

⁸⁹*Id.* art. 13(3)(a), at 71.

⁹⁰For example, long-arm statutes provide for jurisdiction over claims arising from “the causing of any injury within this state,” UTAH CODE ANN. § 78-27-24(3) (1995); breach of contract “by failing to perform acts required by the contract to be performed in this state,” FLA. STAT. ANN. § 48.193(1)(g) (West 1997); and “[t]he transaction of any business within this State,” 735 ILL. COMP. STAT. ANN. 5/2-209(1) (West 1992).

⁹¹*See* World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 295-97 (1980) (noting that the factors in due process analysis include whether “the defendant’s conduct and connection with the forum State are such that he should reasonably anticipate being haled into court there”).

⁹²Hanson v. Denckla, 357 U.S. 235, 253 (1958); *see also* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985) (“This ‘purposeful availment’ requirement ensures that a defendant will not be haled into a jurisdiction solely as a result of ‘random,’ ‘fortuitous,’ or ‘attenuated’ contacts, or of the ‘unilateral activity of another party or a third person,’” but rather only “where the contacts proximately result from actions by the defendant *himself*.”) (citation omitted) (emphasis in original).

c. Location and Foreseeability in the Online
Context

The novel aspects of online communication confound application of these criteria. First, it may not be clear where to “locate” certain types of online conduct. For example: (1) Is a business considered to have a location where the server hosting the files constituting its Web site is located? (2) In the case of a contract for the supply of a digital good, does performance take place (a) where the seller of the good is located at the time he transmits it, (b) where the computer holding the good is located at the time the seller causes it to be transmitted, (c) where the computer from which the purchaser downloads his e-mail is located, (d) where the computer to which the purchaser downloads his e-mail is located, or (e) where the purchaser is located at the time he downloads or reads his e-mail? (3) In the case of tortious conduct consisting of an online communication, does the harmful event occur in a location associated with the sender or in one associated with the recipient? (4) If a seller invites a transaction via a Web site or a newsgroup posting, is that invitation located in the state where the consumer views it? (5) Does the maintenance of a Web site or posting of a newsgroup message constitute “doing business” in every jurisdiction where such communications are received?

The Justices of the Supreme Court have split over whether the “purposeful availment” requirement may be met merely by placing a product into the stream of commerce with the knowledge that it would be carried into the forum state. *See Asahi Metal Indus. Co. v. Superior Court*, 480 U.S. 102 (1987).

1999]

PROTECTING THE DIGITAL CONSUMER

Second, with certain types of online communication it is unclear whether effects in a given jurisdiction are “foreseeable.” Thus, if a person makes a commercial communication via a Web site or newsgroup posting, is it foreseeable that the communication will have effects in every jurisdiction in which such communications may be received? If a person sends a message via bulk e-mail, an Internet mailing list, or in a chat session, is it foreseeable that the message will have effects in every jurisdiction in which a recipient of the message is located? When sending an e-mail message to a single recipient, are effects foreseeable wherever the recipient happens to be located when he accesses the message? Is the analysis different if the communication is made in a language that is understood almost exclusively by residents of a particular country, or if the maker of the communication advertises in a jurisdiction using other, specifically targeted media as well?

d. Summary: Jurisdiction over Online Conduct

Jurisdictional issues, which are rarely simple to resolve, are particularly intractable in the online context. The nature of online communications creates difficulties in applying standard notions of location and foreseeability, which are critical in a variety of formulations of jurisdictional rules. Any approach to jurisdictional issues in the online context must grapple with defining where online events and those who participate in them are deemed to be located, and under what circumstances an online communication, which may be received in locations beyond the sender’s ability to control, will be deemed to have foreseeable effects in a given jurisdiction.⁹³

2. Establishment of Jurisdiction

The fact that a court may have authority to *assert* jurisdiction over a defendant located outside the forum state does not necessarily imply that the plaintiff will be able to *establish* jurisdiction in practice. A court cannot exert jurisdiction over a defendant until the defendant is served with process. Serving a defendant located within the territory of another sovereign “can be a difficult and uncertain undertaking.”⁹⁴ These difficulties are reduced, but not eliminated, when the two

⁹³ An alternative enforcement paradigm, which avoids the extraterritorial assertion of jurisdiction, involves the institution of an enforcement action, by a regulatory authority of the country in which the victim resides, in the courts of the country where the perpetrator is located. There are several difficulties with this approach: the court in which the action is instituted may not accord standing to a foreign regulatory authority, and the conduct forming the basis of the action may not constitute a violation of the law of the forum country. The European Commission has proposed a directive to address some of these difficulties. See Proposal for a European Parliament and Council Directive on Injunctions for the Protection of Consumers’ Interests, COM(95)712 final [hereinafter Proposal for European Injunctions]. The EC’s approach has been criticized as inadequate to the task, due to the limited scope of its applicability. See Michael Bogdan, Injunctions for the Protection of Cross-Border Consumer Interests: Comments on a Proposed E.C. Directive from a Nordic Viewpoint (unpublished manuscript, on file with author).

⁹⁴ GARY B. BORN & DAVID WESTIN, INTERNATIONAL CIVIL LITIGATION IN UNITED STATES COURTS 120 (1990).

jurisdictions are signatory to a treaty on service of process, such as the Hague Service Convention⁹⁵ or the Inter-American Convention on Letters Rogatory.⁹⁶

3. Choice of Law

A court with jurisdiction to adjudicate a particular controversy will not necessarily apply the law of the state in which it is located. If the parties are located in the forum jurisdiction, and all of the operative facts occurred there, a court will apply the *lex fori*. However, where the controversy has “a significant relationship to more than one state,”⁹⁷ the court must resort to choice-of-law principles in order to determine which jurisdiction’s laws it will apply to resolve the controversy.

Choice-of-law issues are notoriously difficult to resolve even in relatively simple contexts.⁹⁸ The complexities of transnational commercial activities conducted via the Internet may give rise to particularly thorny choice-of-law questions. Due to the nature of online communications, an online transaction may routinely involve several jurisdictions. For example, a person in State *A* may make a communication through a Web site hosted on a computer located in State *B*, that is received by a person in State *C* who obtains access to the Internet through a server located in State *D* (which is owned and operated by a company headquartered in State *E*), and that results in a transaction involving the shipment of physical goods or downloading of digital goods from a source located in State *F*.

Among states of the United States, the two most popular approaches to resolving choice-of-law issues are *lex loci delicti* and “most significant relationship.”⁹⁹

⁹⁵Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, Nov. 15, 1965, 20 U.S.T. 362, 658 U.N.T.S. 163, *reprinted following* FED. R. CIV. P. 4 (1992).

⁹⁶Inter-American Convention on Letters Rogatory, Jan. 30, 1975, S. TREATY DOC. NO. 98-27, 14 I.L.M. 339 (entered into force Aug. 27, 1988). In spite of the difficulties, lawsuits enforcing trade practices laws against defendants located outside the jurisdiction are possible. *See* FTC v. Win USA Servs., Inc., No. C98-1614-Z (W.D. Wash. filed Nov. 7, 1998) (action by FTC against Canadian defendants); FTC v. 9013-0980 Quebec Inc., No. 1:96CV-1567, 1996 U.S. Dist. LEXIS 18897 (N.D. Ohio Aug. 13, 1996) (same); FTC v. Ideal Credit Referral Servs. Ltd., No. C96-0874R (W.D. Wa. filed June 5, 1996) (same); Australian Competition & Consumer Comm’n v. Destiny Telecom Int’l Inc., No. BC9704570, 1997 AUST FEDCT LEXIS 758 (FCA Sept. 17, 1997) (action by Australian Competition & Consumer Commission against U.S. defendant). The California Department of Corporations issued an order against a “British company that was selling investments in a time machine. The company claims that it will either develop a machine itself or be so well known that a traveler from the future will go back in time and provide the company with the technology to develop the time machine.” California Dep’t of Corps., *Internet Investments Ordered to Stop Selling (June 10, 1998)* (visited Apr. 18, 1999) <<http://www.corp.ca.gov/pressrel/nr9811.htm>>.

⁹⁷RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 1 (1971).

⁹⁸“[O]ne federal judge I know maintains that his most effective technique to encourage settlement in unruly diversity cases is to suggest that the parties brief the choice of law issues.” Seth F. Kreimer, *The Source of Law in Civil Rights Actions: Some Old Light on Section 1988*, 133 U. PA. L. REV. 601, 601 (1985).

⁹⁹Richard H. Acker, *Choice-of-Law Questions in Cyberfraud*, 1996 U. CHI. LEGAL F. 437, 447, 457. Thirteen states follow the rule of *lex loci delicti*, and twenty-two apply the “most

1999]

PROTECTING THE DIGITAL CONSUMER

Under the rule of *lex loci delicti*, the applicable law is the law of the place “where the last event necessary to make an actor liable for an alleged tort takes place.”¹⁰⁰ But this approach does not work well in the context of fraud, since “there is often no one clearly demonstrable place of injury and at times injury will have occurred in two or more states.”¹⁰¹

The “most significant relationship” approach involves a balancing test that is dependent on a number of factors. One standard exposition of the test that applies where the cause of action is based on fraud or misrepresentation takes cognizance of six factors: (1) the place where the plaintiff acted in reliance upon the defendant’s representations, (2) the place where the plaintiff received the representations, (3) the place where the defendant made the representations, (4) the residence and nationality of the parties, (5) the place where a tangible thing which is the subject of the transaction was situated, and (6) the place where the plaintiff was to render performance under the fraudulently induced contract.¹⁰²

Where the cause of action arises from contract, and the parties have not effectively selected the governing substantive law,¹⁰³ the relevant criteria in a choice-of-law analysis are (1) the place of contracting, (2) the place of negotiation of the contract, (3) the place of performance, (4) the location of the subject matter of the contract, and (5) the location of the parties.¹⁰⁴

The special characteristics of online communications create difficulties in the application of these criteria. For example, does a person “make” or “receive” an online communication (a) where the maker of the communication is located at the time he transmits it, (b) where the computer through which the maker of the communication connects to the network is located, (c) where the computer through which the recipient of the communication connects to the network is located, (d) where the computer from which the purchaser downloads his e-mail is located, or (e) where the recipient of the communication is located at the time he receives it? When performance consists of the delivery of a digital good, does performance occur at the sending end or the receiving end? Is the result different if the seller transmits the good by making it available for download from the seller’s Web site? What is the situs of contracting or negotiation of a contract that is arrived at through online communications?¹⁰⁵

significant relationship” test. *Id.* at 447, 457. In addition, five states follow the “choice-influencing considerations” approach, and three adhere to “governmental interest analysis.” *Id.* at 450-52.

¹⁰⁰RESTATEMENT (FIRST) OF CONFLICT OF LAWS § 377 (1934).

¹⁰¹RESTATEMENT (SECOND) OF CONFLICT OF LAWS ch. 7 introductory note (1971).

¹⁰²*See id.* § 148(2).

¹⁰³*See id.* §§ 186, 187. In the European context, the Rome Convention places significant limitations on the ability of the parties to a consumer transaction to select the governing law. *See* Convention on the Law Applicable to Contractual Obligations, June 19, 1980, art. 5, 1980 O.J. (L 266) 1. The U.N. Convention on the Law Applicable to the International Sale of Goods, the EU Data Protection Directive, and the laws of individual European Union member countries may also apply. *See* Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT’L LAW. 991, 993-1004 (1998).

¹⁰⁴*See* RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 188(2).

¹⁰⁵*See* Matthew R. Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT’L L. 75, 94 (1996) (“How are the relevant factors to be

The novel issues raised by choice-of-law analysis of online transactions will thus center around what is deemed to be the *location* of various persons and events. As is the case with jurisdiction, the location of online events and the persons who bring them about can be difficult to assess.

4. Enforcement of Judgments

Once jurisdiction is established and a judgment rendered, there remains the difficulty of enforcing the judgment against a defendant located outside the forum state. In the absence of a treaty, it will ordinarily not be possible to enforce the injunctive provisions of an order vindicating a public right—such as a prohibition against further violations of a law designed to protect the public from deceptive marketing practices—in the courts of a different sovereign.¹⁰⁶ If the defendant has identifiable assets within the territory of the forum state, enforcement of a money judgment may be feasible. However, in cases involving fraud, typically no such assets are found. If mutual recognition of judgments exists between the forum state and the state where the defendant is located, it may be possible in theory to execute a money judgment against assets located in the latter territory.¹⁰⁷ However, in cases involving fraud the assets will likely be dissipated by the time enforcement of the foreign judgment is obtained.

considered in transnational cyberspace? More importantly, how are contacts such as the place of injury, place of conduct causing injury, and nationality determined in the networked world?”).

¹⁰⁶See Proposal for European Injunctions, *supra* note 93, at 6. The rationale for this rule of public international law is that a

state that pursues . . . public claims outside the confines of its own territory is attempting to invoke its sovereign rights within the territory of the forum state. The institution of legal proceedings itself implies an assertion that the plaintiff state is *entitled* to prosecute its public rights in the forum state.

F.A. Mann, *The International Enforcement of Public Rights*, 19 N.Y.U. J. INT'L L. & POL. 603, 608 (1987) (emphasis in original). In the absence of the consent of the sovereign of the forum state, this assertion “involves the infringement of domestic jurisdiction or sovereignty.” *Id.*

¹⁰⁷The Brussels Convention provides for mutual recognition and enforcement of judgments rendered in contracting states. However, the signatories to the Brussels Convention, *supra* note 88, are limited to European countries. In 1996, the Hague Conference on Private International Law embarked on a four-year project to draft an international convention on jurisdiction and the recognition and enforcement of foreign judgments in civil and commercial matters. See Hague Conference on Private International Law, Final Act of the Eighteenth Session, Oct. 19, 1996, 35 I.L.M. 1391, 1405; CATHERINE KESSEDJIAN, SYNTHESIS OF THE WORK OF THE SPECIAL COMMISSION OF JUNE 1997 ON INTERNATIONAL JURISDICTION AND THE EFFECTS OF FOREIGN JUDGMENTS IN CIVIL AND COMMERCIAL MATTERS (Prel. Doc. No. 8, Nov. 1997) (report by Hague Conference Permanent Bureau concerning proposed convention).

In the absence of any international agreement, foreign judgments may be enforceable under the law of the forum state. For example, recent cases in Canada have established that under certain circumstances foreign judgments may be enforced in Canadian provincial courts. See *Morguard Investments Ltd. v. De Savoye* [1990] 3 S.C.R. 1077 (Can.) (establishing principle that provincial courts must recognize judgments of other provincial courts as long as rendering court had jurisdiction); *McMickle v. Van Straaten* [1992] 93 D.L.R. (4th) 74 (B.C.S.C.) (enforcing default judgment rendered by a California court);

1999]

PROTECTING THE DIGITAL CONSUMER

Enforcement of judgments by entering onto the territory of another sovereign raises issues of extraterritoriality. "The governing principle is that a state cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter."¹⁰⁸ Beyond this familiar limitation on extraterritorial enforcement, the online medium raises certain novel issues. For example, does a search of a computer database that is physically located in another state constitute "measures" on "the territory of another state," so as to require the consent of that state?¹⁰⁹

5. Evasion of Law Enforcement Through Cross-Border Targeting

A technique commonly employed by professional perpetrators of consumer fraud is to set up operations in one country, but to target only residents of other countries. They hope that by doing so they will slip under the radar of law enforcement authorities, as authorities in the country in which they are located will perceive little interest in expending resources to protect foreign consumers, and authorities in the country where the victims are located will face practical difficulties in taking action against a seller located outside the country. In some cases, the laws are inadequate to respond to this problem.¹¹⁰

Canada and the United States have a good deal of experience with this phenomenon in the context of telemarketing. A U.S.-Canada working group set up to study the problem of cross-border telemarketing fraud found that cross-border targeting raises several obstacles to effective law enforcement: the geographic dispersal of victims makes it difficult to identify the extent of a fraudulent telemarketing operation and hinders investigation by raising costs of travel and creating logistical difficulties; effective law enforcement action requires cooperation among two or more law enforcement agencies in different

Terry W. Milne & Terry I. Wuester, *Recognition of American Judgments in Canada: Recent Canadian Law Moves Toward a "Full Faith and Credit" Standard*, 74 MICH. B.J. 42 (1995). "United States courts have been customarily liberal in recognizing and enforcing foreign judgments." Ronald A. Brand, *Enforcement of Foreign Money-Judgments in the United States: In Search of Uniformity and International Acceptance*, 67 NOTRE DAME L. REV. 253, 256 (1991). At least 20 states of the United States recognize foreign judgments by virtue of their adoption of the Uniform Foreign Money-Judgments Recognition Act. See Alan J. Sorkowitz, *Enforcing Judgments Under the Uniform Foreign Money-Judgments Recognition Act*, PRAC. LAW., July 1991, at 57, 58. States may also recognize foreign judgments as a matter of comity. See Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 59 (1996).

¹⁰⁸BROWNLIE, *supra* note 79, at 306-07; see also RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW, *supra* note 77, § 432 cmt. b.

¹⁰⁹See Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117, 171-74 (1997).

¹¹⁰For example, enforcement authorities in the Canadian province of British Columbia brought an action against a company located in the province that was making deceptive solicitations to residents of the United States. The trial court dismissed the action, on the ground that the British Columbia deceptive trade practices law only applied to conduct that directly targeted residents of the province. The decision was, however, reversed on appeal. See *Director of Trade Practices v. Ideal Credit Referral Servs. Ltd.* [1997] 145 D.L.R. (4th) 20 (B.C. Ct. App.).

jurisdictions; the requirement that witnesses travel to a different jurisdiction may make it difficult to present evidence at trial; applying remedies such as terminating a telemarketer's telephone service becomes more complicated when two jurisdictions are involved; and the need to extradite defendants creates procedural hurdles and delays.¹¹¹

Online swindlers will find cross-border targeting to be a useful expedient, given the fact that in the online environment international communications are no more expensive than domestic ones. The geographic indeterminacy of most forms of online communications¹¹² makes targeting of solicitations more difficult than in other media, but if the transaction is consummated in part through postal mail the seller can achieve targeting by exercising discretion in entering transactions.

6. Difficulty in Obtaining Pre-Judgment Freezes of Assets Located Outside the Forum Country

Some national legal regimes allow enforcement actions aimed at stopping fraudulent conduct to be brought *ex parte*, in order to obtain a freeze of the defendant's assets pending resolution of the merits of the action. This prevents the law violator from dissipating or secreting her assets upon learning that a law enforcement action has been instituted against her.¹¹³

Obtaining a freeze of the assets of a defendant located in a foreign country is much more difficult. In certain countries belonging to the British Commonwealth, a procedure known as a *Mareva* injunction is available.¹¹⁴ "The *Mareva* injunction is an *ex parte*, interlocutory measure intended to freeze a defendant's assets prior to judgment in order to prevent the removal of those assets from the jurisdiction of the court."¹¹⁵ A request for a *Mareva* injunction is made in the course of litigation,

¹¹¹See UNITED STATES-CANADA COOPERATION AGAINST CROSS-BORDER TELEMARKETING FRAUD: REPORT OF THE UNITED STATES-CANADA WORKING GROUP TO PRESIDENT BILL CLINTON AND PRIME MINISTER JEAN CHRÉTIEN (1997) [hereinafter U.S.-CANADA TELEMARKETING REPORT].

¹¹²See *infra* text accompanying notes 146-90.

¹¹³The FTC makes extensive use of this procedure, with good results. In actions brought under § 13(b) of the Federal Trade Commission Act, 15 U.S.C. § 13(b) (1994), the FTC is authorized to seek a permanent injunction against violations of any provision of law that it enforces. In cases involving fraudulent conduct, where there is reason to believe that defendants will hide their assets if they have notice of a law enforcement proceeding, courts will issue an *ex parte* temporary restraining order, including a freeze on all of defendants' assets. See *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1031 (7th Cir. 1988); *FTC v. H.N. Singer, Inc.*, 668 F.2d 1107, 1113 (9th Cir. 1982); *FTC v. Southwest Sunsites, Inc.*, 665 F.2d 711, 718 (5th Cir. 1982).

¹¹⁴The name derives from the English case of *Mareva Compania Naviera S.A. v. International Bulkcarriers S.A.*, 2 Lloyd's Rep. 509 (C.A. 1975), in which the English Court of Appeal issued an injunction freezing the assets of a defendant prior to judgment. *Mareva* injunctions have been granted by courts in a number of countries, including Australia, New Zealand, Antigua, the Bahamas, Canada, Malaysia, Hong Kong, and Singapore.

¹¹⁵Peter S. O'Driscoll, *Performance Bonds, Bankers' Guarantees, and the Mareva Injunction*, 7 NW. J. INT'L L. & BUS. 380, 398 (1985).

1999]

PROTECTING THE DIGITAL CONSUMER

instituted in the jurisdiction where the defendant or his assets are located,¹¹⁶ charging the defendant with violations of the law of that jurisdiction. If granted, a *Mareva* injunction freezes the defendant's assets pending resolution of this underlying action in the defendant's jurisdiction. The *Mareva* action may be combined with a parallel action instituted in the courts of the country where the enforcement authority is located.

This can be a very effective means of gaining a favorable resolution of an enforcement action.¹¹⁷ However, this approach has its limitations: *Mareva* injunctions are not available in all countries;¹¹⁸ such an action is possible only if the defendant's assets in the foreign jurisdiction can be identified prior to institution of the proceeding; hiring foreign counsel to bring the *Mareva* action may be very expensive; the jurisdiction where the *Mareva* injunction is instituted may have bank secrecy laws that make it all but impossible to ascertain the extent of frozen funds; in cases where the *Mareva* action is unsuccessful, the plaintiff may be liable for substantial damages; and even where successful, this type of action does not prevent the defendant from resuming her violative behavior after arriving at a monetary settlement.

7. International Comity

When litigation in the courts of one country affects the significant interests of another country, the result can be conflict between two sovereigns. This sort of conflict has been most acute in connection with obtaining evidence that is located outside the country where the court sits. Aggressive efforts to obtain such evidence, particularly in cases involving enforcement of competition laws, have resulted in registration of diplomatic protests and the enactment of blocking statutes by many countries.¹¹⁹ Unduly aggressive enforcement action by government agencies in the context of cross-border online fraud risks giving rise to this sort of conflict, with detrimental effects on the efficacy of cross-border enforcement actions.

¹¹⁶*Mareva* injunctions have been held to be enforceable under the Brussels Convention, *supra* note 88, as well as the Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (Lugano Convention), Sept. 16, 1988, 1988 O.J. (L 319) 9. See Adrian U. Dorig, *The Finality of U.S. Judgments in Civil Matters as a Prerequisite for Recognition and Enforcement in Switzerland*, 32 TEX. INT'L L.J. 271, 281 n.65 (1997). Therefore, it may be possible to "forum shop" by obtaining a *Mareva* injunction in the courts of a country that is favorable towards its issuance, and enforcing it in another country where the defendant's assets are located.

¹¹⁷The FTC has used this approach in several cases with positive results. See *FTC v. Fortuna Alliance, L.L.C.*, No. C96-799M (W.D. Wash. filed May 23, 1996); *FTC v. On Line Communications, Inc.*, No. CV-S-96-55 LDG (RLH) (D. Nev. filed Jan. 23, 1996).

¹¹⁸Some countries offer similar procedural devices under another rubric. The *Mareva* injunction "is roughly equivalent to United States attachment procedures and the French *saisie conservatoire*." O'Driscoll, *supra* note 115, at 398. It is also comparable to seizure and preliminary injunctions under German law, and interim injunctions under Italian law. See Coleen C. Higgins, *Interim Measures in Transnational Maritime Arbitration*, 65 TUL. L. REV. 1519, 1523 n.12 (1991).

¹¹⁹See BORN & WESTIN, *supra* note 94, at 367-73.

8. Restrictions on International Information-Sharing Among Law Enforcement Agencies

National rules that restrict the ability of law enforcement agencies to share information with counterpart agencies in foreign countries are an additional impediment to cross-border enforcement against online deceptive trade practices. If an agency in Country *A* seeks to bring an enforcement action against a company in Country *B* that is making deceptive solicitations to residents of Country *A*, it could be aided enormously by information in the hands of enforcement authorities in Country *B*. For example, an enforcement authority in Country *B* may have received complaints about the company from its own citizens, or it may have conducted an investigation of the company for possible violations of its own laws. National laws protecting the confidentiality of information received or gathered by law enforcement authorities may make it difficult or impossible to share this sort of information across borders.¹²⁰ These national laws vary substantially from one country to another. Such confidentiality rules usually do not restrict the ability of enforcement authorities within a single national unit from sharing such information.

Bilateral mutual legal assistance treaties (“MLATs”) provide a formal means of overcoming certain restrictions on cross-border sharing of investigatory materials by law enforcement agencies.¹²¹ However, MLATs are not universally available, and do not cover all types of requests. In addition, their use entails certain costs. “Formal *MLAT* proceedings can consume valuable time and resources for those at both ends of the process. Offenders can sometimes delay proceedings or get information about the evidence being gathered against them by challenging *MLAT* requests.”¹²²

Other approaches to improving international information sharing among law enforcement agencies involve modification of domestic confidentiality laws,¹²³

¹²⁰*Cf.* Nina Hachigian, *Essential Mutual Assistance in International Antitrust Enforcement*, 29 INT’L LAW. 117 (1995) (arguing that countries should enter into agreements to share confidential information relating to the enforcement of competition laws).

¹²¹Examples of MLATs to which the United States is a party include: Treaty with Canada on Mutual Legal Assistance in Criminal Matters, Mar. 18, 1985, U.S.-Can., S. TREATY DOC. No. 100-14 (1988) (entered into force Jan. 24, 1990); and Treaty on Cooperation between the United States of America and the United Mexican States for Mutual Legal Assistance, Dec. 9, 1987, U.S.-Mex., S. TREATY DOC. No. 100-13 (1988) (entered into force May 3, 1991).

¹²²U.S.-CANADA TELEMARKETING REPORT, *supra* note 111, at 20 (emphasis in original).

¹²³To this end, Congress enacted the International Antitrust Enforcement Assistance Act of 1994 (IAEAA), Pub. L. No. 103-438, 108 Stat. 4597 (codified at 15 U.S.C. §§ 6201-6212 (1994)). The IAEAA authorizes U.S. competition enforcement agencies to enter into agreements with their counterparts in other countries allowing sharing of certain categories of information that would otherwise be held confidential. The first agreement that the United States has negotiated pursuant to the IAEAA is with Australia. *See* Request for Comments on Proposed Agreement Between the Government of the United States of America and the Government of Australia on Mutual Antitrust Enforcement Assistance, 62 Fed. Reg. 20,022 (1997).

1999]

PROTECTING THE DIGITAL CONSUMER

and establishment of databases of consumer complaints that may be accessed internationally.¹²⁴

¹²⁴For example, a coalition of law enforcement agencies in Canada operates a telemarketing complaint database called “phonebusters,” which centralizes complaints about telephone- and online-related deceptive marketing practices from consumers throughout Canada. phonebusters makes information from the database available to law enforcement authorities in the United States, which may prove useful in the case of deceptive practices that target consumers in both Canada and the United States. See Ontario Provincial Police, *Phonebusters* (visited Mar. 21, 1999) <www.gov.on.ca/phonebusters>. The Telemarketing Complaint System database, maintained by the FTC and the National Association of Attorneys General, is likewise available to Canadian law enforcement authorities through a law-enforcement-only Web site called “Consumer Sentinel.” See *Consumer Sentinel: Binational Telemarketing Network* (visited Apr. 17, 1999) <<http://www.ftc.gov/sentinel/index.html>>.

Even where there are no rules restricting the cross-border sharing of information that may assist law enforcement, there may be practical obstacles to effective information sharing. These obstacles include: lack of awareness among law enforcement officials of the types of information that may be available from their foreign counterparts; lack of access to the agency maintaining information that would be useful; and linguistic barriers. Competition authorities have entered into bilateral¹²⁵ and multilateral¹²⁶ agreements that seek to overcome some of these problems.

9. Impediments to Efforts by Consumers to Protect Themselves

The increasingly cross-border nature of electronic commerce also makes it more difficult for consumers to protect themselves from fraud. When the vendor is located outside the country of the consumer's residence, the consumer will not have the same access to sources of information about the vendor's business practices. For example, a consumer located in Japan may not be aware that offices of the Better Business Bureau located throughout the United States and Canada maintain information on complaints filed against companies located within their service area. Even if the consumer is aware of the availability of such information, he may be deterred by the cost of international telephone communications, the inconvenience of time zone differences, or lack of requisite linguistic skills.¹²⁷

Consumers in cross-border transactions also may not be entitled to protections offered by national regulatory regimes. For example, consumers within the United

¹²⁵The United States has entered into several such agreements. *See* Agreement Between the Government of the United States and the Government of the Federal Republic of Germany Relating to Mutual Cooperation Regarding Restrictive Business Practices, June 23, 1976, U.S.-F.R.G., 27 U.S.T. 1956, T.I.A.S. No. 8291, *reprinted in* 4 Trade Reg. Rep. (CCH) ¶ 13,501; Agreement Between the Government of the United States of America and the Government of Australia Relating to Cooperation on Antitrust Matters, June 29, 1982, U.S.-Austl., T.I.A.S. No. 10365, *reprinted in* 4 Trade Reg. Rep. (CCH) ¶ 13,502; Agreement Between the Government of the United States of America and the Government of Canada Regarding the Application of Their Competition and Deceptive Marketing Practices Laws, Aug. 3, 1995, U.S.-Can., 35 I.L.M. 309, *reprinted in* 4 Trade Reg. Rep. (CCH) ¶ 13,503 [hereinafter U.S.-Canada Agreement]. The United States and the European Commission also entered into such an agreement. *See* Agreement Between the Government of the United States of America and the Commission of the European Communities Regarding the Application of Their Competition Laws, Sept. 23, 1991, U.S.-EC, 1995 O.J. (L 95) 45, *corrected at* 1995 O.J. (L 131) 38, *reprinted in* 4 Trade Reg. Rep. (CCH) ¶ 13,504 [hereinafter U.S.-EC Agreement].

The U.S.-Canada agreement is notable as the sole example of a bilateral cooperation agreement involving the United States that specifically addresses cooperation between consumer protection law enforcement authorities. *See* U.S.-Canada Agreement, *supra*, art. VII.

¹²⁶*See* Revised Recommendation, *supra* note 7.

¹²⁷The Better Business Bureau has begun implementation of a Web-site certification program that may make it easier for consumers to obtain information about businesses located in the United States and Canada. *See* Don Oldenburg, *It's Official: BBBOnline*, WASH. POST, May 7, 1997, at D5; Better Bus. Bureau, *BBBOnline* (visited Apr. 14, 1999) <<http://www.bbbonline.org>>.

1999]

PROTECTING THE DIGITAL CONSUMER

States who make domestic purchases paying by credit card can take advantage of the U.S. chargeback regime¹²⁸ to void the purchase if they find themselves the victim of fraud or deception. But this protection may not be available in the context of cross-border purchases.¹²⁹

Finally, attempts by consumers to enforce their rights through private lawsuits naming foreign defendants are subject to all of the difficulties experienced by government agencies bringing law enforcement actions, and more. In particular, the costs of maintaining an action against a defendant located outside the jurisdiction are likely to deter all but the most seriously injured consumers from pursuing this option.¹³⁰

B. Ease of Evading Detection: Portability of Fraudulent Operations, and Disguising of Identity

A scam that is operated via the Internet requires very little infrastructure, all of it portable. “An Internet presence is ephemeral. The process of setting up shop or moving the base of operations can be relatively quick and cheap.”¹³¹ A very simple fraud might require no more than an e-mail account and an offshore answering machine. The swindler opens an e-mail account, and uses a simple and inexpensive technique to send out several million e-mail messages urging the recipient to call a certain telephone number for some important information. On calling the number, whose dialing pattern may not reveal that it accesses a telephone located overseas,¹³² the consumer receives a lengthy recorded message that is of no value. In the process, the consumer incurs a sizable long distance bill, the proceeds of which are shared between the owner of the phone number, who sent out the e-mail solicitations, and the telephone authority of the foreign jurisdiction. By the time enforcement authorities learn of the scam, the perpetrator has disappeared: the e-mail account is closed, and the foreign telephone number is disconnected. The perpetrator may then open new accounts and repeat the scam under another guise.

¹²⁸ See Truth in Lending Act, 15 U.S.C. § 1666 (1994); Regulation Z, 12 C.F.R. § 226.13 (1998).

¹²⁹ Likewise, in the United Kingdom, merchants have interpreted section 75 of the Consumer Credit Act of 1974, 22 & 23 Eliz. 2, § 75 (Eng.), which establishes a chargeback regime, as inapplicable to international transactions. U.K. credit card issuers have agreed to apply section 75’s protections in certain limited categories of international transactions. See *Consumer Redress in the Global Marketplace: Chargebacks*, at 70, OECD Doc. OCDE/GD(96)142, available at <http://www.oecd.org/dsti/sti/it/consumer/prod/e_96-142.htm>.

The OECD’s Committee on Consumer Policy has addressed the possibility of establishing an international chargeback regime that would overcome the domestic limitation of national legal regimes. See *id.*

¹³⁰ See Geanne Rosenberg, *Legal Uncertainty Clouds Status of Contracts on Internet*, N.Y. TIMES, July 7, 1997, at D3.

¹³¹ [AUSTRALIAN] FEDERAL BUREAU OF CONSUMER AFFAIRS, *supra* note 75, at 20.

¹³² Telephone numbers of Caribbean island nations may be dialed from the United States using the same dialing pattern that is used for domestic calls: “1” followed by a three-digit area code, followed by a seven-digit number.

Even if a swindler chooses to set up a relatively more permanent shop, in the form of a Web site, the operation remains fully portable. A Web site has its physical manifestation in the form of a computer that is connected to the Internet. It is accessed through a virtual addressing scheme that is completely divorced from geography. That is, a Web site's physical manifestation may be relocated to anyplace in the world with an Internet connection without affecting its virtual address. The owner of the Web site need not reside in geographic proximity to the server on which the domain is hosted. Moreover, the physical location of the computer housing a Web site is ordinarily completely unknown to those who access the site. This enables a swindler to evade regulatory authorities by shifting her operations to a different geographic jurisdiction, without affecting her location in cyberspace or the continuity of her operations.¹³³

The perpetrator of a scam may make use of a variety of techniques to disguise his identity in online communications. When sending an e-mail using standard mailreader software, it is a simple matter to insert whatever identity one wishes on the "From" line of the e-mail.¹³⁴ Specialized software allowing one to forge the header information contained in e-mails, so as to make it difficult or impossible to trace the e-mail to its sender, is widely available at a very modest cost. It is also possible to route e-mail messages through an anonymous remailer, which strips the e-mail of all identifying information before relaying it to its destination.¹³⁵

Senders of bulk commercial e-mail are especially creative in their use of techniques to disguise their identity. Some swindlers open "throwaway" e-mail accounts with service providers: the swindler opens an account using a false identity and invalid credit card number, the account is activated before the registration information is verified, and the swindler uses the account to send out a single bulk e-mailing and then abandons the account. Swindlers also send bulk e-mail using a valid account, but forge the identifying information contained in the e-mails, or relay the spam from a server identified with a different domain, to make it difficult to trace the e-mail back to its source.¹³⁶

¹³³See Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1112 (1996); Reid Kanaley, *Sorting Out Spam*, PHILADELPHIA INQUIRER, July 10, 1997, at F1 (noting that some Internet gambling sites have moved offshore, and senders of bulk e-mail could do the same).

¹³⁴The "From" line of an e-mail message typically simply reflects the information with which the sending mailreader is configured, leaving it completely within the sender's discretion how he wishes to be identified in the e-mail he sends.

¹³⁵See Barry Fraser, *Regulating the Net: Case Studies in California and Georgia Show How Not to Do It*, 9 LOY. CONSUMER L. REP. 230, 236 (1997).

¹³⁶See *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1019 (S.D. Ohio 1997); Roy Schwedelson, *E-Mail Needs Federal Involvement*, DM NEWS, Nov. 10, 1997, at 24, available in LEXIS, News Library, DMNEWS File. Senders of bulk commercial e-mail—even those who are pursuing entirely lawful activities—have a powerful incentive to disguise their identity. One who sends bulk e-mail displaying his actual e-mail address on the "From" line is liable to receive two distressing types of response. The first is "undeliverable" messages, which are automatically returned to the sender of an e-mail that cannot be delivered as addressed. Bulk e-mailers typically use very poor quality lists of addressees, with a high proportion of addresses that are invalid. See Peter H. Lewis, *Many Users of Commercial On-line Services Are Getting a Steady Diet of "Spam,"* N.Y. TIMES, Oct. 20, 1997, at D4. The resulting barrage of "undeliverable" messages would clog the in-

1999]

PROTECTING THE DIGITAL CONSUMER

It is also a simple matter to disguise one's identity when posting messages in newsgroups or communicating in chat sessions. Standard newsreader software allows one to post a Usenet message showing any "From" line one wishes. Chat session conversations are more often than not conducted through the use of "handles"—pseudonymous appellations that mask the speaker's true identity.¹³⁷

It is likewise trivially easy for the owner of a Web site to disguise her identity. The content of a Web site is entirely unverified, allowing the site owner to assume whatever identity she wishes. Furthermore, the registration mechanism that might provide a means of identifying the true owner of a Web site is wholly unreliable. Under the present World Wide Web domain name registration system, a person can obtain the use of a domain with a .com, .org, or .net extension simply by paying a small fee and providing certain identifying information to the registrar. But the domain name registrar does not perform any verification of the information supplied, and there is nothing to prevent a domain owner from submitting false information as to her identity.¹³⁸

box of a bulk e-mailer who used his actual e-mail address. The second undesirable type of response is large numbers of flames, or nasty e-mail responses, from irate recipients of unsolicited commercial e-mail. A high proportion of these recipients view unsolicited commercial e-mail as an intrusion at best, and many of them respond with a reply message, addressed to the address on the "From" line of the incoming e-mail, expressing their displeasure. By using a false "From" address, the bulk e-mailer makes these responses somebody else's problem. If the address inserted on the "From" line points to a valid domain, the owner of the domain or its online presence provider may be overwhelmed by the responses. Occurrences of this sort have led to lawsuits against bulk e-mailers. *See Parker v. C.N. Enters.*, No. 97-06273 (Travis County, Tex. Dist. Ct., injunction entered Nov. 10, 1997).

¹³⁷ *See Fraser, supra* note 135, at 236; Pridgen, *supra* note 65, at 244-45 ("[A]pparently some salespeople are hyping their products in on-line chat rooms or on bulletin boards, while pretending to be just regular consumers or even celebrities.").

¹³⁸ For example, at one point the registration for the domain name "martianconsulate.com" identified the administrative contact as "Head, Honcho," with a U.S. telephone number of 305-555-1212, which is (transparently) the number for directory assistance in south Florida.

The payment mechanism that is used in an online transaction may sometimes enable law enforcement officials to discover the location and identity of an online swindler. However, a careful swindler can interrupt the money trail by use of offshore accounts in countries with strict bank secrecy laws, setting up dummy corporations, requiring payment by cashier's check, and other means. The introduction of online digital cash payment mechanisms that embody strong forms of privacy protection may render payment mechanisms an even less useful method of detection.

The ease with which one may disguise one's ownership of a Web site is particularly insidious in combination with the relatively modest cost of creating a professional-looking Web site. A well-designed Web site conveys the impression that it must be associated with a substantial and reliable commercial establishment. It may in reality be only a thin facade disguising a scheme to defraud.

The difficulty that governments face in confronting the dangers to consumers that result from the fact that it is easy for online speakers to disguise their identity is compounded by the fact that in many contexts speakers have a legitimate interest in anonymity. "The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."¹ Anonymity also "provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent."² Maintaining anonymity in commercial transactions may be the only weapon available to consumers who want to prevent the aggregation of their transactional data into personal profiles.³ Based on such considerations, the Supreme Court has identified a First Amendment right to anonymity, at least in certain contexts.⁴

¹McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341-42 (1995).

²*Id.* at 342; *see also* Talley v. California, 362 U.S. 60, 64 (1960); ACLU v. Reno, 929 F. Supp. 824, 849 (E.D. Pa. 1996) ("Anonymity is important to Internet users who seek to access sensitive information . . ."), *aff'd*, 521 U.S. 844 (1997); Fraser, *supra* note 135, at 236; Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117 (1996).

³*See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 407-10 (1996); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 877 (1996).

⁴*See McIntyre*, 514 U.S. at 341-42 (identifying a First Amendment right to anonymity in the context of publishing political leaflets).

1999]

PROTECTING THE DIGITAL CONSUMER

C. New Entrepreneurs

Because the costs of promoting a commercial activity via the Internet are relatively modest, the Internet opens the doors to an enormous flood of new entrepreneurs—some of whom will be in the business of fraud. In the United States, Internet access may be obtained for \$20 a month. A domain name may be registered for \$70, and server space for hosting a Web site is available at \$30 a month. Setting up a simple Web site is easy to do. Lists of e-mail addresses to enable the sending of bulk commercial e-mail may be had at \$35 per million names, or less.⁵ The required computer equipment is available for less than \$1,000, and may be sited on one's dining room table. Add a post office box or a private mail receiving service and a new entrepreneur is in business.⁶

The absence of large obstacles to entry, though positive from the standpoint of competition, creates additional difficulties for law enforcement. It means that the number of potential law violators is greatly increased; that the newcomers are likely to be running smaller fraudulent operations, making it harder to deploy law enforcement resources effectively; and that these new entrepreneurs are more likely to be unsophisticated⁷ and unschooled in legal requirements applying to their activities and therefore are more likely to violate the laws unintentionally.

⁵See Doug Abrahms, *AOL Sues Junk E-mailers in Attempt to Stem Flood*, WASH. TIMES, Jan. 8, 1998, at B6.

⁶See Christopher Wolf & Scott Shorr, *Cybercops Are Cracking Down on Internet Fraud*, NAT'L L.J., Jan. 13, 1997, at B12 ("The cost of setting up shop on the Internet is plunging along with the cost of consumer access.").

⁷In one case, a participant in a chain-letter scheme perpetrated by bulk e-mail was found to be a 15-year-old boy. See *PC Talk Radio Show Archives* (visited Apr. 14, 1999) <<http://www.pcmike.com/radioarc.html>>.

*D. Geographic Indeterminacy*⁸

1. Limitations Imposed by Technology

In most cases it is difficult for the sender of an online communication to identify the geographic location of the recipients of the communication. The means of communicating via the Internet that are most likely to be employed in online commerce are: (1) sending e-mail—either one-to-one, in bulk to recipients who have requested it (via Internet mailing lists), or in bulk to recipients who have not requested it (unsolicited commercial e-mail); (2) maintaining a Web site; (3) posting messages in a newsgroup; and (4) making statements in a chat session.⁹ An e-mail address need not indicate the geographic location of either the person to whom it is assigned or the service provider that provides connectivity. Unlike a telephone number, an e-mail address contains no area code or country code. The sender of an e-mail message therefore will not necessarily know the location of the recipient of the message.¹⁰ The owner of a Web site may collect reams of data about a site visitor, including the browser used to access the site and every page viewed during the visit, but there is no automatic means of determining the geographic location of the visitor. One who posts a message in a newsgroup has no way of knowing who will access it. Lurkers in chat sessions are generally identified only by a handle.

⁸This section is based on the discussion in John Rothchild, *Making the Market Work: Enhancing Consumer Sovereignty Through the Telemarketing Sales Rule and the Distance Selling Directive*, 21 J. CONSUMER POL'Y 279, 298-300 (1998).

⁹See *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 166 (S.D.N.Y. 1997). For a discussion of the various means of communicating via the Internet, see Leif Swedlow, *Three Paradigms of Presence: A Solution for Personal Jurisdiction on the Internet*, 22 OKLA. CITY U.L. REV. 337, 347-54 (1997).

¹⁰Some e-mail addresses do contain what appears to be the equivalent of a telephone number's country code, in the form of a two-letter abbreviation indicating the country that registered the domain name. For example, an e-mail address at a domain registered in Canada might have the form "user_name@domain_name.ca". But this would not necessarily imply that the owner of the address, or the server hosting it, is located in Canada. A country's domain registrar is not forbidden from issuing a domain name to a non-resident, and the server need not be located in the country that issued the domain name. In fact, top-level domains issued by countries such as Turkmenistan (.tm), Tuvalu (.tv), and the Federated States of Micronesia (.fm) have become valuable commodities to businesses that hope to profit from association with the two-letter abbreviations (trademark, television, and FM radio), but have nothing to do with the issuing countries. See Andrew Raskin, *Buy This Domain*, WIRED, Sept. 1998, at 106, 108, 110.

A domain name may reference an institution whose geographic location is widely known or may be easily determined. For example, if one sends an e-mail to "user_name@uchicago.edu", one might reasonably assume that the recipient has some connection with the University of Chicago, which is widely known to be located in the state of Illinois. But a domain name may suggest a geographic location that is, intentionally or unintentionally, misleading. For example, the URL <www.chicago.com> points to a Web site maintained by a computer professional located in California. See Swedlow, *supra* note 147, at 392-93. Even when an e-mail address accurately points to the geographic location where the addressee resides, there is no guarantee that she will be located there when she

1999]

PROTECTING THE DIGITAL CONSUMER

It is also generally impossible or infeasible for the sender to limit the availability of a communication to a geographic, political, or other subset of the online community. "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community."¹¹ A World Wide Web site generally may be accessed from anywhere in the world. In theory, a site owner may limit access to persons in a particular geographic location through a registration system. To do so, the site owner must employ "out-of-band" communications to ascertain the geographic location (or other pertinent characteristics, such as age) of the would-be visitor. This might be done by requiring the visitor to register by submitting proof of his geographic location, in the form of a verifiable address or telephone number. This is, however, a cumbersome, expensive, and time-consuming procedure, and one that would deter most prospective site visitors. For that reason it is rarely employed, other than in very limited circumstances.¹² The characteristic mode of interaction with the World Wide Web involves browsing freely at whatever site a search engine or hypertext link takes one to—the software one uses to access the Web is even referred to as a "browser." An advertiser who required visitors to pre-register and disclose their location before being allowed access to the advertiser's Web site could expect not to be troubled by many visitors.¹³

receives the e-mail, as it is possible to log into one's access provider and receive one's e-mail from a remote location. *See* Burk, *supra* note 133, at 1113.

More commonly, an e-mail address gives no hint as to the location of its owner: The 15 million subscribers to America Online, for example, who may be located anywhere in the world, all have an e-mail address ending in "aol.com".

¹¹*Reno v. ACLU*, 521 U.S. 844, 853 (1997) (quoting *ACLU v. Reno*, 929 F. Supp. 824, 844 (E.D. Pa. 1996)); *see also* *Hasbro Inc. v. Clue Computing, Inc.*, 994 F. Supp. 34, 42 (D. Mass. 1997) ("[W]hile magazine publishers can affirmatively decide not to sell or distribute magazines in certain forums, this option of bypassing particular regions is not yet available to Web site providers.") (citing the Affidavit of Clue Computer owner, Eric Robison, ¶ 8(c)).

¹²One such circumstance involves adult-oriented materials. For example, the owner of a Web site operated from Italy, which distributes sexually explicit pictures, but is prohibited by court order from making the pictures available in the United States due to trademark rules, employs a password system under which "prospective users fax an 'order form' . . . along with a credit card number, and receive back a password and user ID via e-mail." *Playboy Enters., Inc. v. Chuckleberry Publ'g, Inc.*, 939 F. Supp. 1032, 1043 (S.D.N.Y. 1996). Likewise, the owner of a computer bulletin board system offering sexually explicit pictures to subscribers required prospective subscribers to submit an application form listing the applicant's address and telephone number. *See United States v. Thomas*, 74 F.3d 701, 705 (6th Cir. 1996).

¹³The owner of a Web site may well prefer that access to the site be limited to those living within a particular geographic area. For example, when the owner of a jazz club in Columbia, Missouri named "The Blue Note" decided to establish a Web site for the club, his intention was to reach people who lived close enough to the club to visit it in person as paying customers. Instead, he reached all the world, including the owners of a famous jazz club in New York City also called "The Blue Note." As a result of his going global, the owners of the New York club sued him for trademark infringement and unfair competition. The suit, brought in federal district court in New York, was dismissed for lack of jurisdiction. *See Bensusan Restaurant Corp. v. King*, 126 F.3d 25 (2d Cir. 1997).

Those who communicate by posting messages in newsgroups or chat sessions have no means of limiting access to geographic subgroups of the online community. The sender of an e-mail message has only the illusion of control over the geographic accessibility of her messages. Although she may direct a message to a person known to reside at a particular location, the recipient need not be at that location when she retrieves the message.¹⁴

¹⁴ Access to a Web site or newsgroup may be blocked at the recipient's end, by the recipient's Internet service provider. Efforts by governments to require service providers to block access to newsgroups or Web sites, or to enforce content restrictions generally, have been controversial.

Blocking access to Web sites. Perhaps the best known example of government efforts to enforce content restrictions on the Internet involves CompuServe which, until its acquisition by America Online, was the second-largest online service provider in the world. In December 1995, prosecutors in Bavaria, Germany notified CompuServe that they were investigating the distribution of pornography via the Internet. In response, CompuServe blocked access to over 200 newsgroups. The blocking affected all of CompuServe's 4.3 million subscribers throughout the world, as the technology did not exist to block access only by those in a specific geographic location. In February 1996, CompuServe restored access to all but five of the newsgroups, and made available user-side blocking software. See John Markoff, *On-Line Service Blocks Access to Topics Called Pornographic*, N.Y. TIMES, Dec. 29, 1995, at A1; Peter H. Lewis, *An On-line Service Halts Restriction on Sex Material*, N.Y. TIMES, Feb. 14, 1996, at A1. Authorities in Munich subsequently prosecuted the managing director of CompuServe's German operations, Felix Somm, based on CompuServe's failure to block access to objectionable material in newsgroups. See Edmund L. Andrews, *Germany's Efforts to Police Web Are Upsetting Business*, N.Y. TIMES, June 6, 1997, at A1. The court found Somm guilty as charged, and imposed a two-year suspended sentence. The conviction is on appeal. See Alan Cowell, *Head of German Web Sentenced for Pornography*, N.Y. TIMES, May 29, 1998, at A3.

In a less publicized incident, police in the United Kingdom pressured Internet service providers to block access to 133 newsgroups that were considered pornographic. See Alan Boyle, *Governments Take On the Net*, MSNBC (visited Feb. 26, 1997) <<http://www.msnbc.com>>. And China has blocked access to 100 Web sites, including ones containing English-language news and dissident publications. See Kathy Chen, *China Bars Access to as Many as 100 Internet Web Sites*, WALL ST. J., Sept. 5, 1996, at B5.

Forbidding links to objectionable content. German prosecutors brought charges against a German university student for maintaining a Web-page link to a site containing a left-wing newspaper called "Radikal." The newspaper contained material that was viewed as incitement to terrorism. The court dismissed the charges, finding that the link had been established before objectionable material was added to the Web site. See Edmund L. Andrews, *German Judge Dismisses Criminal Charge Over Internet Link*, N.Y. TIMES, July 1, 1997, at D7.

Registration requirements. China requires Internet subscribers to register with the police, and organizations with Internet-related businesses to provide information about their operations to the government. See Tom Korski, *China to Require Businesses Using Internet to Divulge Details of Operations*, 2 Electronic Commerce & L. Rep. (BNA) 583 (June 6, 1997). Singapore's Class Licence Scheme requires Singaporean Internet service providers and certain content providers to register with the government. See *The Singapore Broadcasting Authority Act (Chapter 297)* (visited Mar. 23, 1999) <<http://www.sba.gov.sg/work/sba/internet.nsf/pages/Doc21>>.

Controls on content. A French law, known as the Fillon Amendment, which threatened Internet service providers with penalties if they did not follow guidelines as to content established by a new council, was invalidated by the *Conseil Constitutionnel*. See Alan Boyle, *East vs. West? No, It's Nations vs. Net*, MSNBC, Oct. 2, 1996 (visited Feb. 26,

1999]

PROTECTING THE DIGITAL CONSUMER

2. Implications for Online Sellers

This lack of control over the sphere of dissemination of material that is made available on the Internet may create a serious compliance problem for online marketers. If material they post on the Internet is available to all without regard to geographic location, are online marketers subject to the marketing practices laws of every jurisdiction? If so, sellers may be confronted with an unpalatable choice among conforming their solicitations to the requirements of the most restrictive jurisdiction, risking being subjected to enforcement actions brought at any location in the world, or forgoing the online medium altogether. “[R]egulation in any one jurisdiction has the potential to control available Internet content world-wide.”¹⁵

1997) <<http://www.msnbc.com>>. Germany’s “multimedia law” allows Internet service providers to be held liable for content they transmit if “they have knowledge of such content and are technically able and can reasonably be expected to block the use of such content.” Informations-und-Kommunikationsdienste-Gesetz [Information and Communication Services Act] art. 1, § 5 (1997). Singapore’s Internet Code of Practice requires Singaporean Internet service providers to block access to defined categories of “prohibited material,” including “pornography, violence and incitement of racial or religious hatred.” Eileen Drage O’Reilly, *Singapore Broadcast Authority Issues Revised Internet Code of Practice*, 2 Electronic Commerce & L. Rep. (BNA) 1099, 1099 (Oct. 24, 1997). Vietnam prohibits “content that would ‘report false information, libel the prestige of organizations, insult national heroes and great men, or incite superstition or social evils.’” David Case, *Big Brother Is Alive and Well in Vietnam—And He Really Hates the Web*, WIRED, Nov. 1997, at 164, 175. China requires Internet service providers to remove material that is not in keeping with content restrictions set by the government, which include a prohibition against defamation of government agencies. See Angela Gregorits, *New Chinese Regulations Establish Scheme to Monitor, Criminalize Certain Internet Use*, 3 Electronic Commerce & L. Rep. (BNA) 36 (Jan. 14, 1998); Erik Eckholm, *China Cracks Down on Dissent in Cyberspace*, N.Y. TIMES, Dec. 31, 1997, at A3.

Efforts by regulatory authorities to control access to the Internet can result in backlash. Austrian Internet access providers took the entire country offline for two hours to protest a raid by law enforcement authorities on one provider based on allegations that it was allowing the transmission of child pornography. See Mark Ward, *Viennese Vice Squad Sparks Net Strike*, NEW SCIENTIST, Apr. 5, 1997, at 7, 7.

For a discussion of efforts by governments to control content on the Internet, see Viktor Mayer-Schönberger & Teree E. Foster, *A Regulatory Web: Free Speech and the Global Information Infrastructure*, in BORDERS IN CYBERSPACE 235 (Brian Kahin & Charles Nesson eds., 1997).

¹⁵Wolf & Shorr, *supra* note 144, at B12. The dilemma to marketers posed by the problem of geographic indeterminacy is not unique to the Internet. The same issue arises, usually in attenuated form, in other contexts. For example, international television broadcasts may contain commercial material that violates the law of some but not all of the countries in which the broadcast is received.

A similar phenomenon occurs by virtue of the federal legal system in the United States. Companies that advertise their products on network television or other nationwide media in the United States must comply with the trading practices laws of all 50 states, the District of Columbia, and the federal government. Even if they do not advertise, companies that use a single packaging for distribution of their product throughout the United States may find themselves in a similar bind. Ben & Jerry’s, an ice cream maker that is located in Vermont and distributes its product throughout the United States, ran into this problem when it wanted to state on its packaging that the milk from which its product is made contains no bovine growth hormone. Four states objected to the proposed labeling, with the result that the company was unable to use the labeling in any of the 46 states that did not so object,

Some regulatory authorities have taken the position that they may assert jurisdiction over anyone who makes information available to residents of their territorial jurisdiction via the Internet, regardless of the sender's physical location. The state of Minnesota forthrightly asserts this position on its Web site,¹⁶ and has acted upon it. The state brought an enforcement action against defendants located

since "it is not feasible for companies such as Ben & Jerry's to label their products differently for individual markets." Beth Berselli, *Settlement Reached in Hormone Labeling Case*, WASH. POST, Aug. 15, 1997, at A22.

The inability of marketers to limit the distribution of their commercial messages can lead to the converse of the "rogue nation" effect. Beer brewer Anheuser-Busch, one of the corporate sponsors of the 1998 World Cup, which was hosted by France, hoped to place advertising placards around the Stade de France, which would have made them visible to an expected cumulative television viewership of 37 billion people around the world. But French law prohibits all advertising of alcohol and tobacco products, meaning that the placards could not be placed on French soil. See Anne Swardson, *Battle over Bud Brewing for French-Hosted World Cup Soccer*, WASH. POST, Apr. 14, 1997, at A12. The result was a "highest common denominator" effect: viewers throughout the world, including those located in countries where the proposed advertising was legal, were denied the benefit of Anheuser-Busch's promotional messages, due to application of the law of the jurisdiction where the communication originated.

¹⁶The Web site states: "PERSONS OUTSIDE OF MINNESOTA WHO TRANSMIT INFORMATION VIA THE INTERNET KNOWING THAT INFORMATION WILL BE DISSEMINATED IN MINNESOTA ARE SUBJECT TO JURISDICTION IN MINNESOTA COURTS FOR VIOLATIONS OF STATE CRIMINAL AND CIVIL LAWS." Minnesota Attorney Gen., *Warning to All Internet Users and Providers* (visited Mar. 23, 1999)

<<http://www.ag.state.mn.us/home/consumer/consumernews/OnlineScams/memo.html>>.

This assertion seems not to accord with the view of a plurality of the Supreme Court in *Asahi Metal Industry Co. v. Superior Court*, 480 U.S. 102 (1987), according to which a defendant's knowledge that his product (in this case, information) will enter a state does not alone subject him to the jurisdiction of the courts of that state: there must in addition be "an action of the defendant purposefully directed toward the forum State." *Id.* at 112 (quoting *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985)).

The Texas Attorney General has also expressed an expansive view concerning jurisdiction over electronic bulletin board activities. See Bradley A. Slutsky, *Jurisdiction over Commerce on the Internet* (last modified June 6, 1997)

<<http://www.kslaw.com/menu/jurisdic.htm>>.

Other states and regulatory bodies have been more cautious about asserting jurisdiction generally over the Internet. The Attorney General of Florida has issued an advisory opinion expressing the view that although state law prohibits Florida residents from using the Internet to place bets with entities located outside the state, Internet technology makes enforcement of this law very difficult, and regulation of the Internet is better left to the federal government than a patchwork of individual states. Florida Attorney General, 95 Op. Att'y Gen. 70 (1995). In addition, securities regulators in the United States and United Kingdom have issued policy statements to the effect that they will abstain from asserting jurisdiction over securities offerings that are made available via the Internet, even though the offerings may be viewed by residents within their respective territorial jurisdictions, if certain conditions are met. See Statement of the Commission Regarding Use of Internet Web Sites to Offer Securities, Solicit Securities Transactions or Advertise Investment Services Offshore, Securities Act Release Nos. 33-7516, 34-39779, IA-1710, IC-23071 (Mar. 23, 1998), Int'l Series Release No. 1125, 63 Fed. Reg. 14,806 (1998) (to be codified at 17 C.F.R. pts. 231, 241, 271, 276) [hereinafter Statement of the Commission]; *U.K. Securities Regulator Clarifies Stance on Web Sites Operated by Foreign Funds*, 3 Electronic Commerce & L. Rep. (BNA) 730, 731 (June 3, 1998).

1999]

PROTECTING THE DIGITAL CONSUMER

outside Minnesota—an individual residing in Nevada, and a Nevada corporation—that operated a Web site offering online gambling, allegedly in violation of the state deceptive marketing practices law. The trial court held that it had personal jurisdiction over the defendants, and that determination was upheld on appeal.¹⁷

If enforcement authorities around the world followed the Minnesota approach, the result could be to confront online marketers with a tangle of regulations that vary from one jurisdiction to another. Within the member countries of the European Union alone—a relatively homogeneous grouping—there are substantial variations in the rules applying to marketing practices.¹⁸ In the world at large, the variations are considerably greater.

Legislatures have enacted laws regulating content on the Internet that purport to apply to all the world. The United States Congress enacted the Communications Decency Act of 1996, which imposes criminal penalties for the transmission of obscene or indecent material to minors.¹⁹ The state of California passed a law that regulates Internet marketers doing business with residents of the state.²⁰ Other states have passed laws purporting to regulate identification of the sender of an online message,²¹ decency of online communications,²² and unsolicited e-mail²³—all without regard to the location of the sender of the communication.²⁴

¹⁷See *Minnesota v. Granite Gate Resorts, Inc.*, No. C6-95-7227, 1996 WL 767431 (Minn. Dist. Ct. Dec. 11, 1996), *aff'd*, 568 N.W.2d 715 (Minn. Ct. App. 1997), *aff'd*, 576 N.W.2d 747 (Minn. 1998).

¹⁸According to one author, “there are only two promotional methods that can be used with impunity across the EU—on-pack price cuts and in-store demonstrations.” Thomas W. Reader, *Is Self-Regulation the Best Option for the Advertising Industry in the European Union? An Argument for the Harmonization of Advertising Laws Through the Continued Use of Directives*, 16 U. PA. J. INT’L BUS. L. 181, 202 & n.99 (1995); see also *supra* notes 71-73.

¹⁹Communications Decency Act of 1996, Title V of the Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56, *held unconstitutional in part in Reno v. ACLU*, 521 U.S. 844, 864 (1997). The obscenity and indecency provisions appear at 47 U.S.C. § 223(a), (d) (Supp. II 1996).

²⁰The law requires sellers who offer goods or services, by Internet or any other means, “in this state,” to ship the merchandise or issue a refund within 30 days. It also requires Internet sellers to disclose the seller’s return policy, legal name, and street address from which it conducts business, “when the transaction involves a buyer located in California.” CAL. BUS. & PROF. CODE § 17538 (West 1997). For a criticism of this statute, see Fraser, *supra* note 135, at 236.

²¹A Georgia statute makes it a crime for “any person . . . to transmit any data through a computer network . . . if such data uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person.” GA. CODE ANN. § 16-9-93.1 (1996).

²²A New York statute makes it a crime for a person to use a computer to send a communication to a minor which “in whole or in part, depicts actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors.” N.Y. PENAL LAW § 235.21(3) (McKinney 1998).

²³A Nevada statute makes a person who sends e-mail containing an advertisement liable to the recipient for damages (\$10 per e-mail, plus attorney’s fees and costs), unless there is a prior business relationship or consent, or the e-mail states it is an advertisement and provides the name, street address and e-mail address of the sender, and a notice instructing the recipient how to decline to receive future e-mail advertisements. See NEV. REV. STAT. § 41-730 (1997). A Washington statute forbids sending to a Washington resident any

Some of these initial efforts have been invalidated by the courts. The Communications Decency Act was struck down on free speech grounds to the extent it penalizes the transmission via the Internet of material that is “indecent” but not “obscene.”²⁵ This ruling was predicated largely upon unique characteristics of the online medium: the fact that it is not feasible to determine the age of persons who may access a communication on the Internet, and that all senders of “indecent” communications are therefore subject to prosecution under the Act because they are chargeable with knowledge that at least some recipients may be minors.²⁶

The New York statute forbidding indecent communications was held invalid as an unconstitutional burden on interstate commerce. The court reasoned that the law in question seeks to regulate communications occurring wholly outside the state, imposes a burden on interstate commerce that is disproportionate to the local benefits, and subjects Internet users to inconsistent state obligations.²⁷

commercial e-mail message that misrepresents the origin or routing of the message or contains misleading information on the subject line. *See* WASH. REV. CODE ANN. § 19.190.020 (West 1998). A California law requires that senders of unsolicited commercial e-mail include a mechanism enabling recipients to refuse further messages, and that they honor such refusals. It also prohibits sending UCE in violation of a service provider’s terms of service. *See* CALIF. BUS. & PROF. CODE §§ 17538.4, 17538.45 (West Supp. 1999).

²⁴According to one report, “[i]n 1995 and ‘96, 11 states passed laws that somehow censor speech on the Internet.” Shabbir J. Safdar, *States Censor the Net*, INTERNET WORLD, Jan. 1997, at 20, 20. During the first half of 1998, more than 700 Internet-related bills were introduced in state legislatures. *See* Joan Lowy, *Lawmakers Get in Line to Introduce On-line Bills*, WASH. TIMES, July 13, 1998, at A4.

Some types of local regulation of the Internet do not implicate global issues. For example, the state of Virginia enacted a law that prohibits state employees from using their computers at work to access material “having sexually explicit content.” VA. CODE ANN. § 2.1-805 (Michie 1998). The law does not purport to regulate the conduct of persons located outside of Virginia. Likewise, general deceptive trade practices laws may be enforced against a person located within the territorial jurisdiction of the enforcing sovereign, based on conduct taking place on the Internet, without raising novel issues. *See* *New York v. Lipsitz*, 663 N.Y.S.2d 468 (N.Y. Sup. Ct. 1997) (enforcing New York deceptive trade practices law against New York resident who used bulk e-mail to make deceptive solicitations). This is simply an application of the principle that “general jurisdiction” exists where a defendant’s contacts with the forum state are “continuous and systematic,” even if those contacts are not directly related to the conduct giving rise to the cause of action. Richard S. Zembek, *Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace*, 6 ALB. L.J. SCI. & TECH. 339, 349 n.49 (1996).

²⁵*See* *Reno v. ACLU*, 521 U.S. 844, 864 (1997).

²⁶*See id.* at 876.

²⁷*See* *American Libraries Ass’n v. Pataki*, 969 F. Supp. 160, 183-84 (S.D.N.Y. 1997); *see also* Glenn Harlan Reynolds, *Virtual Reality and “Virtual Welters”: A Note on the Commerce Clause Implications of Regulating Cyberporn*, 82 VA. L. REV. 535 (1996) (concluding that if each state applied its own laws to content on the Internet, the result would be an intolerable burden on interstate commerce in violation of the commerce clause of the U.S. Constitution); Burk, *supra* note 133, at 1096-97 (“[T]he Due Process Clause of the Fourteenth Amendment and the Commerce Clause in its dormant aspect significantly curtail the ability of states to regulate online activities.”).

The EC law analogue to the U.S. dormant Commerce Clause principle is known as “negative harmonization.” This refers to “the removal of barriers of trade by requiring Member States to abolish national rules which are considered to create such obstacles.”

1999]

PROTECTING THE DIGITAL CONSUMER

Taken together, these two rulings point to significant constitutional issues that result from the problem of geographic indeterminacy when legislatures seek to control the content of Internet communications that are received by residents of their territorial jurisdictions.

The Georgia statute requiring that Internet communicators accurately identify themselves, and the Virginia statute forbidding state employees from accessing sexually explicit material, were also invalidated on free speech grounds.²⁸ These rulings did not turn on any of the online medium's special characteristics: they were based on a straightforward application of the federal constitutional guarantee of free speech. These rulings serve as a reminder that the special characteristics of the online medium do not displace the traditional considerations, but rather add an additional layer of analysis when regulation is called into question.

3. Home-Country Control

One possible approach to the problem of geographic indeterminacy is a regime of home-country control. Where this principle is applied, a seller engaging in a cross-border commercial transaction is bound to comply with the rules of law in force in the country in which the seller is established, and not with the rules in effect in the country where the buyer resides.

This principle has been applied in several contexts in European Community ("EC") law as an aspect of the European Union Single Market initiative, which aims to erect a legal structure that makes national borders essentially irrelevant to commercial transactions among residents of the member countries. The benefits of home-country control for sellers within the European Union are obvious: they enjoy a "one-stop regulatory shop," which allows them to market their goods and services throughout the EU without having to comply with the rules of fifteen separate jurisdictions. The seller's compliance costs are reduced, as transparency of the regulatory structure is increased. The principle of home-country control may be seen at work in the "Television Without Frontiers" directive, which (with a few exceptions) prevents television broadcasters from being subject to the regulatory regime of each country in which their broadcasts are received.²⁹ Home-country

GERAINT HOWELLS & THOMAS WILHELMSSON, *EC CONSUMER LAW 2* (1997). *See generally* THIERRY BOURGOIGNIE & DAVID TRUBEK, *CONSUMER LAW, COMMON MARKETS AND FEDERALISM IN EUROPE AND THE UNITED STATES* 159-64 (1987) (discussing the application of Article 30 of the Treaty of Rome to invalidate national trade rules that have an effect equivalent to import restrictions).

²⁸*See* *ACLU v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997) (entering a preliminary injunction against enforcement of the Georgia statute, pending a final determination); *Urofsky v. Allen*, 995 F. Supp. 634 (E.D. Va. 1998) (finding the Virginia statute an unwarranted content restriction), *rev'd sub nom.* *Urofsky v. Gilmore*, 167 F.3d 191 (4th Cir. 1999). The latter case was reversed on narrow grounds applying to restrictions that limit the speech of government employees only.

²⁹*See* Council Directive 89/552 of 3 October 1989 on Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Pursuit of Television Broadcasting Activities, art. 2, 1989 O.J. (L 298) 23, 26. The European Court of Justice has held, however, that this directive does not necessarily preclude the application of the deceptive marketing practices laws of the recipient country to advertising contained in a television broadcast originating in another EU member

control is the governing principle in other Community contexts as well.³⁰ In their policy papers on electronic commerce, the European Commission³¹ and the United States government³² urge that home-country control serve as one of the guiding principles of the regulatory framework, and the EC has made this principle a centerpiece of its proposed directive concerning electronic commerce.³³ One author argues that online transactions should be governed “by the law of the place where the server is physically located”³⁴—which may or may not be the place where either of the parties to the transaction is located. Another has proposed the adoption of an international “Convention on Transfrontier Computer-Network Communications,” which would implement a regime of home-country control applying to all online communications.³⁵

The principle of home-country control with respect to commercial communications, in the form it takes in EC law, is not absolute. Home-country control in EC law has its basis in Articles 59 and 60 of the EC Treaty, which guarantee the free movement of services within the community.³⁶ In general, “[t]he principle of freedom to provide services guarantees that a Member State cannot restrict services emanating from another Member state.”³⁷ However, “restrictions

country. *See* Joined Cases 34-36/95, *Konsumentombudsmannen v. De Agostini (Svenska) Förlag AB and TV-Shop i Sverige AB*, 1997 E.C.R. I-3843. On one view, this ruling demonstrates the inadequacy of the Television Without Frontiers directive, since it “forces advertisers to comply in cases of cross-border advertising with the legislation of the host country with the most restrictive rules.” Marc Lolivier, *The De Agostini Ruling and Advertising Regulation*, COM. COMM., Jan. 1998, at 4, 8.

³⁰*See* European Comm’n, Green Paper on Financial Services: Meeting Consumers’ Expectations 3 (May 1996) (“The single market in financial services is built on the principles of home-country control and mutual recognition based on the implementation of agreed minimum standards of prudential supervision.”), available at <<http://europa.eu.int/en/record/green/gp007en.pdf>>.

³¹*See* A European Initiative in Electronic Commerce: Communication from the Commission to the European Parliament, the Economic and Social Committee, and the Committee of the Regions, COM(97)157 final at 14 (noting that home-country control is preferable except “where mutual recognition does not suffice to remove obstacles in the market or to protect general interest objectives”).

³²*See* WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE § III(8) (1997) (“The rules of the ‘country-of-origin’ should serve as the basis for controlling Internet advertising to alleviate national legislative roadblocks and trade barriers.”).

³³*See* Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market, COM(98)586 final.

³⁴Grossman, *supra* note 58, at 28.

³⁵Gigante, *supra* note 72, at 552-62. This author exempts e-mail from his definition of communications subject to the proposed convention, on the mistaken premise that “the sender of an international e-mail message knows beforehand the message’s destination and hence the foreign law that will apply to determine any legal obligations that might arise from the message.” *Id.* at 554 n.162. As noted above, *supra* note 148, the problem of geographic indeterminacy applies to e-mail communications just as it does to other forms of online communication.

³⁶The European Court of Justice has held that television advertising constitutes provision of a service within the scope of Article 59. *See* Lolivier, *supra* note 167, at 6.

³⁷Green Paper on Commercial Communications in the Internal Market, *supra* note 71, at 5. To the extent that restrictions on commercial communications have the effect of hindering

1999]

PROTECTING THE DIGITAL CONSUMER

on the freedom to provide services can, subject to certain conditions, be justified.”³⁸ In particular, a member state may apply non-discriminatory national rules for “overriding reasons relating to the public interest,” which include “the protection of consumers.”³⁹ In addition, the national rules must satisfy the requirement of “proportionality”: that is, “requirements imposed on the providers of services must be appropriate to ensure achievement of the intended aim and must not go beyond that which is necessary in order to achieve that objective.”⁴⁰

There are several obvious disadvantages to home-country control from the point of view of consumers and consumer protection authorities. First, actions to enjoin behavior that violates the law “have to be brought in a country other than that in which the plaintiff is domiciled.”⁴¹ This is because an injunction issued by a court in the plaintiff’s country cannot be effectively enforced across the border in the country where the enjoined party is located.⁴²

Second, the home-country principle tends to reduce the protections available to consumers by leveling down the regulatory regime to that of the least protective jurisdiction.⁴³ Application of this principle creates an incentive for offerors of goods and services to relocate to the country whose regulatory structure is least burdensome.⁴⁴ The resulting dilution of the protections offered by more protective national regulatory regimes may be unfavorably received by residents of such jurisdictions.⁴⁵

the movement of goods across national borders, the principle of home-country control may also derive support from Article 30 of the Treaty, relating to the free movement of goods.

See id. at 4.

³⁸*Id.* at 5.

³⁹*Id.* at 5-6.

⁴⁰*Id.* at 6 (quoting Case 384/93, *Alpine Investments BV v. Minister van Financiën*, 1995 E.C.R. I-1141).

⁴¹Proposal for European Injunctions, *supra* note 93, at 6.

⁴²*See id.* In this document, the European Commission proposes a directive that will facilitate the institution of actions for injunction, in the courts of the country of origin, by authorities of the country where the consumer is located. The directive works on the principle of mutual recognition of authorities entitled to maintain an injunctive action. However, its scope is “limited to practices coming within the remit of national laws that have been harmonized under” specified enactments of EC law. *Id.* at 8. The approach is therefore of limited utility in a broader international context where harmonized substantive rules cannot be presupposed.

⁴³For this reason, the Rome Convention derogates from the principle of home-country control in the case of certain consumer contracts: as to such contracts, the consumer retains “the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence,” regardless of whether the contract itself specifies some other applicable law. Convention on the Law Applicable to Contractual Obligations, *supra* note 103, art. 5(2), at 3.

⁴⁴*See Jim Murray, Address to the European Consumer Forum on the Consumer and the Information Society*, at 2, BEUC/291/96 (Sept. 3-4, 1996) (arguing that home-country control “may lead to the lowest common denominator in terms of standards”).

⁴⁵*See Consumer Protection: An Essential Priority for Cross-Border Commercial Communications*, COM. COMM., June 1997, at 6.

4. Opting Out

Another approach to the problem of geographic indeterminacy is to provide online marketers with mechanisms allowing them to “opt out” of certain jurisdictions. An example may be drawn from the U.S. experience, which with its federal legal system confronts national marketers with the laws of fifty states, the District of Columbia, and the federal government. Thus, a company offering to sell stock to the public in the United States must comply with the securities laws of all states in which the offering is made. This creates a difficulty if the company wishes to make its offering through a prospectus published on the Internet, and the prospectus does not meet the requirements of all fifty states. A New York brewery faced this problem when it became the first U.S. company to offer securities through an online prospectus. “Its solution was to include on the electronic offering document a warning specifying the states in which the offer was valid.”⁴⁶ The offering was registered in eighteen states and the District of Columbia.⁴⁷ The company refused and returned tens of thousands of dollars in subscriptions it received from residents of states where the offering was not registered.⁴⁸

Marketers that advertise via national communications media other than the Internet must also comply with the deceptive trade practices laws of multiple jurisdictions. Marketers sometimes do so by stating “Void where prohibited” in their advertisements,⁴⁹ and declining to make the advertised offer available to residents of jurisdictions where the offer is not legal.⁵⁰

⁴⁶ Cella & Stark, *supra* note 49, at 823.

⁴⁷ *See id.* at 823 n.40.

⁴⁸ *See* Andrew Klein, *WallStreet.com*, WIRED, Feb. 1998, at 88, 90.

⁴⁹ Another typical formulation used in print advertisements: “This is not an offering to any person in any state where such an offering may not lawfully be made.”

⁵⁰ *See* Accutest Corp. v. Accu Test Systems, Inc., 532 F. Supp. 416, 419-20 (D. Mass. 1982) (discussing a company which advertised nationally, but declined to sell its stock in states where forbidden by law).

1999]

PROTECTING THE DIGITAL CONSUMER

Some Web sites have begun to make use of this mechanism. One online gambling site, which U.S. criminal enforcement authorities had charged with violations of U.S. law, posted a notice stating that it would not accept “wagers originating from or transmitted through the United States of America,” or “any monetary transaction originating from or transmitted through the United States of America.”⁵¹ Many adult-oriented sites warn users that they must be at least eighteen years of age to access the site. The legal effect of these opt-out efforts may vary depending on whether they are effectively implemented. With present technology, this requires some out-of-band communication. For example, the gambling site would have to make efforts to verify the location of its clients, perhaps by requiring a prospective bettor to submit a postal address and verifying that the bettor receives mail at this address. Various third-party adult verification systems have sprung into existence to service adult-oriented sites.⁵² While these verification mechanisms may be circumvented without much difficulty, they may suffice to negate liability that depends on some degree of scienter.

E. Unclear Regulatory Environment

It is not always clear how the existing consumer protection regulatory structure applies to the online medium. “[M]ost of the legal and regulatory mechanisms currently being applied by governments to commercial activity were conceived in an era before the advent of advanced electronic communication systems.”⁵³ For example, some regulatory regimes apply one set of rules to communications made in the print media and another set to the broadcast media.⁵⁴ In such a situation, it may be unclear which set of rules is to govern the Internet, which partakes of characteristics of both media. Further, the novel and hybrid nature of the online medium may also give rise to turf issues among regulatory bodies.⁵⁵

⁵¹*Real Casino and Sportbook* (visited Nov. 11, 1998) <<http://www.realcasino.com>>. Other gambling sites have followed the same strategy. See Jon Swartz, *High Rollers Try Hand at Online Gaming*, S.F. CHRONICLE, May 8, 1998, at B1.

⁵²See, e.g., *The Adult Check System* (visited Apr. 14, 1999) <<http://www.adultcheck.com>>.

⁵³ORGANISATION FOR ECON. CO-OPERATION AND DEV., ELECTRONIC COMMERCE: OPPORTUNITIES AND CHALLENGES FOR GOVERNMENTS 67 (1997).

⁵⁴This is the case in the United Kingdom. The Control of Misleading Advertisements Regulations of 1988, S.I. 1988, No. 915 (Eng.), gives the Director General of Fair Trading authority over print media, including newspapers, magazines, brochures, direct mail, and billboards. A different misleading advertising regime, administered by the Independent Television Commission and the Radio Authority, applies to broadcast media such as television, radio, cable, and satellite services.

In the United States, the First Amendment analysis of content restrictions may vary depending on how the communications medium is characterized. See *Reno v. ACLU*, 521 U.S. 844, 854 (1997) (distinguishing the Internet from broadcast media for purpose of First Amendment analysis); *FCC v. Pacifica Found.*, 438 U.S. 726, 748-50 (1978) (holding that the broadcast media receive narrower First Amendment protection than other media).

⁵⁵For example, the federal government of Canada and the provincial government of Québec disagree as to which level of government has jurisdiction over the language content of Internet sites located in Québec. While the Canadian Constitution assigns jurisdiction over telecommunications to the federal government, the Supreme Court of Canada has recognized provincial jurisdiction over television advertising. It is unclear in which category the Internet belongs. See Peter Menyasz, *Language Defenders Reveal Tension Between*

In addition to classification issues, special characteristics of the online medium raise issues as to how applicable rules are to be interpreted in the online context. For example, how are rules requiring disclosures to be made “clearly and conspicuously” to be applied when the viewing medium shifts from ink on paper to pixels on a monitor? When making a disclosure on a Web site, does a link to the disclosure language meet the “clear and conspicuous” requirement?⁵⁶ Is a Web site disclosure adequate if it appears on a page below the point where the consumer may place an order? Since the cost of adding additional text to an online communication is typically very low, should disclosure requirements be made more elaborate?⁵⁷ In a solicitation conveyed via an e-mail message or newsgroup posting, is it sufficient to include a link to a Web site containing the required disclosure? Are e-mail messages subject to regulations applying to “direct mail”?⁵⁸ Is an electronic document considered to be “written,” “printed,” or “published” for purposes of regulations using those terms?⁵⁹ Where and when are online contracts formed?⁶⁰

*F. Summary: Barriers to the Development of Electronic
Commerce Raised by the Special Characteristics of Online
Communications*

The discussion above highlights several obstacles to the growth of electronic commerce that arise due to certain special characteristics of the online communications medium.

On the demand side, consumers face a heightened risk that they will be victimized by unscrupulous sellers that engage in deceptive marketing practices. Because of the geographic separation between buyers and sellers that is typical with online commerce, consumers have a difficult time ascertaining the reputation of the seller and obtaining satisfaction in case of a dispute. These difficulties are

Federal, Provincial Power over Web Content, 2 Electronic Commerce & L. Rep. (BNA) 653 (June 27, 1997).

⁵⁶Interpretation of Rules and Guides for Electronic Media; Request for Comment, 63 Fed. Reg. 24,996, 25,002 (proposed May 6, 1998) (outlining an FTC effort to clarify applicability of its rules online).

⁵⁷Although the online medium is generally not subject to constraints of physical space and economics that limit the amount of disclosure information that can be provided to consumers in print and broadcast advertisements and on labels, “the explosion of available information may actually cause problems for consumers who have to select appropriate and relevant information.” HOWELLS & WILHELMSSON, *supra* note 165, at 12; *see also* AUSTRALIAN COMPETITION & CONSUMER COMM’N, *supra* note 6, at 8 (“[T]he large volume of information available [on the Internet] may actually hamper consumers from attempting to find specific information and, even then, evaluating and interpreting complex information may be difficult.”).

⁵⁸Interpretation of Rules and Guides for Electronic Media, 63 Fed. Reg. at 25,000-01.

⁵⁹*Id.* at 25,000.

⁶⁰*See id.* at 25,001; ROGER TASSÉ & KATHLEEN LEMIEUX, CONSUMER PROTECTION RIGHTS IN CANADA IN THE CONTEXT OF ELECTRONIC COMMERCE 46-50 (1998) (reviewing adequacy of existing consumer protection legislation as applied to electronic commerce in a report to the Office of Consumer Affairs, Industry Canada), *available at* <http://strategis.ic.gc.ca/pics/ca/full_e.pdf>.

1999]

PROTECTING THE DIGITAL CONSUMER

exacerbated when, as will occur with increasing frequency, online transactions involve a seller in one country and a buyer in another. Law enforcement agencies attempting to police online deceptive marketing practices face significant obstacles in the case of cross-border transactions: the uncertain reach of extraterritorial jurisdiction, difficulties in serving process and enforcing judgments, problems associated with cross-border targeting, the ease with which wrongdoers may evade detection, and an influx of new entrepreneurs.

On the supply side, sellers experience regulatory uncertainty, finding it impossible to restrict the distribution of their marketing messages so as to limit their exposure to assertions of jurisdiction by courts and legislatures throughout the world. Within a given jurisdiction, it is in many cases difficult to know how existing trade practices rules will be applied in the online context. This uncertainty raises the costs of doing business online, and makes electronic commerce a less attractive option for sellers.

V. ROLE OF GOVERNMENT IN CONTROLLING DECEPTIVE
MARKETING PRACTICES IN ELECTRONIC COMMERCE

In market economies, commercial transactions are presumptively regulated by market forces, not by the government. The utilitarian justification for this presumption is the notion that “free markets promote an efficient resource allocation which accords most closely with individual preferences.”⁶¹ However, there is widespread recognition that “in a number of contexts completely free markets do not yield the best performance in terms of economic welfare, with the implied corollary that the performance can be improved by some form of regulation.”⁶² The standard justification for government intervention in these situations is that it helps to correct market imperfections, yielding benefits generally to society.⁶³

Commercial transactions that are conducted by means of online communications media are likewise presumptively best regulated by market forces. Yet, as in other spheres of economic activity, and for the same reasons of market failure, the government has an important, albeit interstitial, role to play in the online arena.

⁶¹M.A. UTTON, *THE ECONOMICS OF REGULATING INDUSTRY* 1 (1986); *see also* Cass R. Sunstein, *Disrupting Voluntary Transactions*, in *MARKETS AND JUSTICE* 279, 281 (John W. Chapman & J. Roland Pennock eds., 1989) (“The basic position is that people know what is in their own best interests and that respect for preferences, as expressed in market transactions, is the best way to promote aggregate social welfare.”). Other justifications for the view that governments should ordinarily respect voluntary market transactions are rooted in the notion of respect for individual autonomy, and a distrust in the rationality of the majoritarian process. *See id.* at 280-82.

⁶²UTTUN, *supra* note 199, at 4; *see also* PETER ASCH & ROSALIND SENECA, *GOVERNMENT AND THE MARKETPLACE* 397-420 (1985) (discussing the rationale for government regulation to protect consumers).

⁶³*See, e.g.*, RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* 122 (5th ed. 1998) (A liar’s “investment in manufacturing and disseminating misinformation” is a complete waste of resources, so the law does not reward it.). Government intervention in private transactions for the purpose of protecting people from fraud is generally recognized as not subject to the objection from liberty. *See* Cass R. Sunstein, *Legal Interference with Private Preferences*, 53 U. CHI. L. REV. 1129, 1132 (1986).

Government regulation has often been conceived simplistically as an interference with the operation of market forces. This unsophisticated conception fails to recognize the various modes in which market forces and government regulation of consumer markets combine and complement each other. Pure forms of market forces and government regulation, if they exist at all, are the exception. In most cases, governments and markets work in tandem to encourage commercial practices that yield the greatest benefits for the economy as a whole.

Avenues for such “co-regulation” are of crucial importance in considering the proper role of government in controlling online deceptive marketing practices. The global information infrastructure “requires a new paradigm for governance that recognizes the complexity of networks, builds constructive relationships among the various participants (including governments, systems operators, information providers, and citizens), and promotes incentives for the attainment of various public policy objectives in the private sector.”⁶⁴

A. Market Forces and Government Regulation

The term “market forces” is typically applied to a variety of constraints on the conduct of actors on the economic stage, having the common characteristic that they operate primarily through decisions made by private entities, singly or in combination, rather than by government through commands backed by threat of sanction. “Government regulation” describes activity by the government that impinges on the free operation of markets. But these two sorts of regulation of economic activity are not natural enemies. In a variety of contexts, they may complement and reinforce each other.

Consumer sovereignty. Consumer sovereignty is the control that consumers exercise over the allocation of society’s productive resources by virtue of their marketplace decisions.⁶⁵ When consumers choose to purchase a particular item, their expenditures result in profits for the item’s producers, giving them a reason to continue producing it. Conversely, if an item does not find favor in the marketplace, it will no longer be produced—at least not for long.⁶⁶ Consumer sovereignty thus dictates how an economy’s productive resources will be allocated and, if it operates properly, directs those resources to their highest-value uses.

For consumer sovereignty to operate effectively, consumers must possess information that is sufficient, and sufficiently accurate, to enable them to make appropriate purchasing decisions—that is, decisions that best promote their own welfare.⁶⁷ For many purchasing decisions, consumers can gather the necessary

⁶⁴Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 EMORY L.J. 911, 912 (1996).

⁶⁵See PETER SMITH & DENNIS SWANN, *PROTECTING THE CONSUMER* 8 (1979) (“The consumer is king—he commands by virtue of the way in which he votes his money.”); see also G. PETER PENZ, *CONSUMER SOVEREIGNTY AND HUMAN INTERESTS* (1986).

⁶⁶“Failure by the producer to obey the dictates of the sovereign consumer is tantamount to signing his own economic death warrant.” ASCH & SENECA, *supra* note 200, at 398 (quoting DAVID HAMILTON, *THE CONSUMER IN OUR ECONOMY* 330 (1962)).

⁶⁷See UTTON, *supra* note 199, at 9 (“A key assumption of the model of competitive markets is that buyers possess full information not only about product prices but also about the characteristics, qualities, and effects of the products they may purchase.”). In recognition of

1999]

PROTECTING THE DIGITAL CONSUMER

information on their own, through inspection of items offered for sale or by making small, experimental purchases. In other cases, however, “the learning process is more difficult and thus more costly. Few buyers can tell from inspection whether a television set or an air conditioner will perform well over time.”⁶⁸ Although this information is theoretically available to consumers, in everyday situations it may be so costly to acquire that it is in practice unavailable.

Closely related to the problem of *insufficiency* of the information on which consumers may base their marketplace decisions is the problem of *inaccuracy* of such information. Vendors of goods and services are one source of inaccurate product information, which they may convey in the form of misleading advertising or fraudulent misrepresentations. Inaccurate product information may also come from a variety of other sources, such as word-of-mouth, makers of competing products, and fictional sources.

The market attempts to remedy this information shortfall through mechanisms that help consumers make informed decisions. One such mechanism is provision of information comparing competing items offered in the marketplace, through third-party publications such as *Consumer Reports* in the United States or *Which?* in the United Kingdom. Private certification systems, such as the Underwriters Laboratories seal of approval, are another aid to consumer sovereignty.

These market-supplied mechanisms, helpful though they may be, in many situations fall short of what is required to enable optimal operation of consumer sovereignty. The information that they convey is simply not comprehensive enough, or detailed enough, to inform the broad range of marketplace decisions that consumers are called upon to make every day.⁶⁹

Governments can facilitate the operation of consumer sovereignty by prescribing *disclosure requirements*, which require vendors to provide consumers with more information; or they may *prohibit the making of false statements*, which results in consumers’ receiving higher quality information. Prescription of disclosure obligations is a widely employed strategy for improving the operation of consumer

the crucial role that a free flow of information plays in a market economy, the freedom of speech guaranteed by the First Amendment has been held to apply to speech whose object is purely commercial. See *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 763 (1976) (“As to the particular consumer’s interest in the free flow of commercial information, that interest may be as keen, if not keener by far, than his interest in the day’s most urgent political debate.”).

⁶⁸ASCH & SENECA, *supra* note 200, at 399. Conditions in the marketplace have evolved over time so as to make it more difficult for consumers to get the information they require through direct experience. The early English legal doctrine of *caveat emptor* assumed that the consumer was responsible for protecting himself and would do so by applying his intelligence and experience in negotiating the terms of any purchase. In early times the consumer may have been able to protect himself. Products were less sophisticated. They could be inspected before purchase. Today . . . it is fairly generally accepted that conditions have changed.

SMITH & SWANN, *supra* note 203, at 8.

⁶⁹In the 1960s, long before the widespread availability of personal computers, the suggestion was put forth that comparative product information should be stored on computers and made available to consumers “through computer outlets scattered throughout the country.” William C. Whitford, *The Functions of Disclosure Regulation in Consumer Transactions*, 1973 WIS. L. REV. 400, 454.

sovereignty.⁷⁰ For example, the U.S. government requires sellers to convey pre-purchase information to consumers concerning franchises,⁷¹ energy consumption of home appliances,⁷² securities,⁷³ the hazards of products such as cigarettes,⁷⁴ and the ingredients and nutritional content of foods.⁷⁵

Disclosure requirements impose costs on the consumer marketplace. These costs are felt directly by the marketers to whom they apply, but their ultimate incidence may fall on consumers. Overly enthusiastic disclosure requirements may, therefore, introduce inefficiency, as “the cost of supplying the additional information may be greater than the additional benefit derived from it by consumers.”⁷⁶

Virtually all developed market economies have laws prohibiting vendors from making false or misleading statements to induce consumers to purchase their products. These laws vary widely in terms of the specificity of their prohibitions. At their most general, such laws may simply forbid “unfair and deceptive practices.” At the opposite end of the spectrum, deceptive marketing practices laws may specify prohibited practices in great detail.

⁷⁰A disclosure requirement is the less intrusive of two possible regulatory responses to information asymmetry, the more intrusive option being to ban the product or service from the marketplace. *See* Sunstein, *supra* note 199, at 291.

⁷¹*See* Disclosure Requirements and Prohibitions Concerning Franchising and Business Opportunity Ventures, 16 C.F.R. pt. 436 (1998) (requiring franchisors to provide prospective franchisees with a disclosure statement containing specified categories of information).

⁷²*See* Rule Concerning Disclosures Regarding Energy Consumption and Water Use of Certain Home Appliances and Other Products Required Under the Energy Policy and Conservation Act, 16 C.F.R. pt. 305 (1998) (requiring manufacturers of household appliances to label them for energy consumption).

⁷³Section 5 of the Securities Act of 1933, 15 U.S.C. § 77e (1994), requires a registration statement to be filed with the Securities and Exchange Commission before a security may be offered for sale. The purpose of the registration statement, whose content is prescribed in great detail, *see* 17 C.F.R. §§ 229.10-.103 (1998), “is to assure that the investor has adequate information upon which to base his or her investment decision,” THOMAS LEE HAZEN, *THE LAW OF SECURITIES REGULATION* 60 (2d ed. 1990). The disclosure approach to regulation of securities was profoundly influenced by the thinking of Louis Brandeis, who “had strongly urged publicity as a remedy for social and industrial diseases.” LOUIS LOSS & JOEL SELIGMAN, *FUNDAMENTALS OF SECURITIES REGULATION* 25 (3d ed. 1995). In the words of Brandeis’s familiar epigram: “Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.” LOUIS D. BRANDEIS, *OTHER PEOPLE’S MONEY* 92 (1914).

⁷⁴Federal law requires that cigarette packaging and advertisements display a specified set of “Surgeon General’s Warnings.” 15 U.S.C. § 1333 (1994).

⁷⁵Food that is offered for sale must carry a label setting forth its ingredients as well as specified nutritional characteristics. *See* 21 U.S.C. § 343(i), (q) (1994).

⁷⁶UTTON, *supra* note 199, at 10. However, disclosure requirements may yield widespread benefits to consumers even when disclosures have little direct impact on consumers’ purchasing decisions. If disclosures affect the shopping habits of even a small number of consumers, the result may be to heighten competition among sellers for the business of these consumers and thereby to improve generally the quality of offerings in the marketplace. *See* Whitford, *supra* note 207, at 431.

1999]

PROTECTING THE DIGITAL CONSUMER

Industry self-regulation. Another force at work in the marketplace is industry self-regulation.⁷⁷ This form of self-regulation usually takes the form of a code of conduct that an association of traders within a particular industry promulgates and makes applicable to the association's membership. Adherence to the code may be wholly voluntary, or it may be enforced by a private form of sanction such as the threat of expulsion from the trade association or reference to a law enforcement agency.⁷⁸ "[P]roperly designed and well administered self-regulatory systems provide a swift, flexible, inexpensive and effective means of enabling the responsible majority of the industry to restrain the irresponsible minority."⁷⁹

"Voluntary codes are usually a response to the real or perceived threat of a new law, regulation or trade sanctions, competitive pressures or opportunities, or

⁷⁷One treatment of the various modes of marketplace governance classifies self-regulation as a non-market-based form of governance, distinguishing among the "pure market model," "pure enforcement" by governments, and "self-regulation." Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, in PRIVACY AND SELF REGULATION IN THE INFORMATION AGE 3 (U.S. Dep't of Commerce ed. 1997). But it is difficult to see why self-regulation should not be viewed as a type of market mechanism. The essence of market-based governance mechanisms is that discipline results from the economic effect of decisions made by private market participants, rather than from the threat (or imposition) of sanctions by the state. Businesses submit to self-regulation in response to market forces: They believe that the cost of compliance will be outweighed by the benefits they receive by virtue of membership in a trade association that sponsors a code, displaying the emblem of a third-party certification body, or gains to the reputation of the industry as a whole. Self-regulation is simply the collective aspect of the discipline that each individual seller exercises over its own behavior in order to find favor in the marketplace.

⁷⁸For example, the U.S. Direct Marketing Association ("DMA") maintains a Committee on Ethical Business Practice, which investigates alleged deviations from its voluntary self-regulatory Guidelines for Ethical Business Practice. If the Committee believes that a marketer has failed to adhere to the Guidelines, it may contact the marketer to seek voluntary compliance. If the conduct appears to constitute a law violation, the Committee may refer the case to the appropriate law enforcement agency. See DMA ETHICS AND CONSUMER AFFAIRS DEP'T, CASE REPORT FROM THE DIRECT MARKETING ASSOCIATION'S COMMITTEE ON ETHICAL BUSINESS PRACTICE (1997) (on file with author).

Industry associations may also act as a first line of defense against violations of legal rules by their members. The Council of Better Business Bureaus, a trade association of marketers in the United States and Canada, operates a National Advertising Division ("NAD") whose function is to evaluate advertising claims and determine whether they are adequately substantiated. If the NAD finds a claim to be unsubstantiated, it asks the advertiser to modify the claims. If the advertiser disagrees, the matter may be reviewed by the National Advertising Review Board ("NARB"), composed of advertising professionals from the private and public sectors. If the advertiser refuses to comply with NARB's decision, NARB will refer the matter to an appropriate law enforcement agency. Such referrals are exceedingly rare. See Nikhil Deogun, *Winn-Dixie's 'Lower Price' Tactic Is Referred to the FTC by Board*, WALL ST. J., Dec. 23, 1996, at B6. For a description of the operation of this self-regulatory system, see Better Bus. Bureau, National Advertising Review Board, *Brief Summary of Procedures* (visited Apr. 14, 1999)

<<http://www.bbb.org/advertising/narb.html>>.

⁷⁹EUROPEAN ADVERTISING STANDARDS ALLIANCE, EASA GUIDE TO SELF-REGULATION 8 (1997) (on file with author).

consumer and other market or public pressures.”⁸⁰ Firms may choose to adhere to a voluntary code in the expectation that doing so will improve their bottom lines—perhaps by increasing consumer confidence in the industry, or preventing inroads by unethical sellers.⁸¹ Governments can encourage the development of self-regulatory regimes “by outlining the alternative increased regulatory and enforcement action that would be required to address market failures if self-regulatory measures were not introduced,”⁸² by “insist[ing] on adherence to voluntary codes as a condition of issuing a license,”⁸³ or through “allocation[s] of liability, that will induce networks themselves to adopt desirable public policies.”⁸⁴

Government officials may be quite explicit in urging industry to self-regulate or be subject to government regulation,⁸⁵ and industry members may be likewise explicit⁸⁶ in urging their competitors to adopt self-regulation as a means of avoiding presumptively worse-tasting medicine. Industry self-regulation may therefore not reflect the action of pure market forces. Instead, it may reflect industry’s effort to anticipate the marketing practices that government regulators are likely to perceive as desirable, and to devise a regulatory scheme that accomplishes this at as low a cost to industry members as possible.⁸⁷

⁸⁰[CANADIAN] OFFICE OF CONSUMER AFFAIRS, VOLUNTARY CODES: A GUIDE FOR THEIR DEVELOPMENT AND USE 8 (1998) [hereinafter VOLUNTARY CODES].

⁸¹See Roscoe B. Starek, III & Lynda M. Rozell, *The Federal Trade Commission’s Commitment to On-Line Consumer Protection*, 15 J. MARSHALL J. COMPUTER & INFO. L. 679, 695 (1997) (“[R]esponsible businesses often find it advantageous to take steps both to build consumer confidence in their industries and to protect consumers from being lured away by deceptive practices.”). Another form of voluntary code, technical standards, can benefit adherents through network externalities. See Swire, *supra* note 215, at 10.

⁸²AUSTRALIAN COMPETITION & CONSUMER COMM’N, *supra* note 6, at 58.

⁸³VOLUNTARY CODES, *supra* note 218, at 21.

⁸⁴Reidenberg, *supra* note 202, at 929; see Hardy, *supra* note 76, at 1043-46 (advocating imposition of strict liability on system administrators).

An example of an allocation of liability that discourages self-regulation is provided by *Stratton Oakmont, Inc. v. Prodigy Services Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), which holds that an online service provider increases its exposure to defamation liability if it undertakes to screen message postings for inappropriate content. This decision was legislatively overturned by the Communications Decency Act of 1996. See *Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997).

⁸⁵Ira C. Magaziner, the primary architect of the U.S. government’s position paper on electronic commerce, stated in a speech to Internet advertisers that if industry did not devise effective self-regulation in the areas of privacy and content, “we will have to go the legislative route.” Stuart Elliott, *A Clinton Advisor Argues the Economic Case for Self-Regulation of Sales Pitches in Cyberspace*, N.Y. TIMES, Nov. 4, 1997, at D13.

⁸⁶The president of a company in the direct marketing field urged industry members to respect the concerns of consumers when they use unsolicited commercial e-mail, for fear that otherwise “we could prompt the FTC to enter the picture” with unwanted regulation. Ed Mullen, *Urge Netizens to Opt In for Everyone’s Benefit*, DM NEWS, Oct. 6, 1997, at 26, available in LEXIS, News Library, DMNEWS File. The president of the Canadian Direct Marketing Association likewise stated, “In the end, if self-regulation doesn’t work, the government will have to intervene in the marketplace.” Peter Menyasz, *Canadian Direct Marketing Group Issues Guidelines on Acceptable Use of E-Mail Ads*, 2 Electronic Commerce & L. Rep. (BNA) 1115, 1115 (Oct. 29, 1997).

⁸⁷See Eli M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, in PRIVACY AND SELF REGULATION IN THE INFORMATION AGE, *supra* note 215, at 21, 25

1999]

PROTECTING THE DIGITAL CONSUMER

Both governments and non-governmental organizations can also facilitate the development of effective codes by developing model codes or other sorts of guidance on the elements of an effective code.⁸⁸ Governments may have an ongoing role with respect to self-regulatory regimes, with enforcement action serving as a last resort in cases where an industry member fails to comply voluntarily with industry-ordained standards.⁸⁹

Another type of industry self-regulation may develop when one group of traders, which plays a crucial role in allowing consumer transactions to occur, is in a position to control the conduct of another group of traders. For example, media outlets such as newspapers, magazines, and broadcasters can constrain the ability of vendors to offer their products to the public by refusing to run advertisements that they consider inappropriate because they are misleading, in bad taste, or otherwise offensive. The network television broadcasters in the United States have developed elaborate sets of standards that they use in evaluating the suitability of a proposed advertisement, and they refuse to air advertisements that do not conform to those standards.⁹⁰ Catalogue sellers exercise discretion in deciding what goods they will carry, and how those goods will be described. Credit card associations, such as VISA and MasterCard, impose conditions on issuers and merchants before allowing them access to their payment systems. Those conditions require issuers to honor chargebacks by consumers, and may call for termination of merchants who engage in deceptive marketing practices. Western Union has agreed to stop transporting funds from the residents of one state to offshore gambling operations.⁹¹ Advertising agencies can refuse to lend their support to marketing campaigns that are deceptive. Operators of online malls may require their tenants to conform with codes of conduct or face eviction.

Contract. A third form of regulation by market forces is the realm of contract. A contract represents an agreement by two market participants as to their rights and responsibilities *inter se*. It is arrived at through negotiation, reflecting the classic market mechanisms of supply and demand. But contracts do not depend solely on market forces. The essence of a contract is its enforceability: the contracting parties are aware that if they do not perform their end of the bargain, they risk

("[S]elf-regulation is rarely voluntary . . . : it usually occurs only under the threat of state regulation, and it can therefore be considered a variant of direct regulation.").

⁸⁸See AUSTRALIAN COMPETITION & CONSUMER COMM'N, *supra* note 6, at app. 10

(presenting a summary of essential elements of codes of conduct developed by the Australian Ministerial Council on Consumer Affairs).

⁸⁹ See *id.* at 58. For example, companies that do not adhere to decisions rendered by the Better Business Bureau's National Advertising Division review process may be referred for possible enforcement action to the FTC. See *supra* note 216. Such enforcement action is possible only if a firm's conduct violates not merely a voluntary code, but also a legal rule—which might occur if a company represents that it will comply with a voluntary code, but then fails to do so. See *infra* text accompanying note 331.

⁹⁰See GORDON E. MIRACLE & TERENCE NEVETT, VOLUNTARY REGULATION OF ADVERTISING 139-41 (1987). Broadcast media in a number of other countries likewise enforce their own codes of advertising practice. See JEAN J. BODDEWYN, GLOBAL PERSPECTIVES ON ADVERTISING SELF-REGULATION 27-137 (1992).

⁹¹See Ben Greenman, *Sinking Offshore Bookies*, WIRED, Apr. 1998, at 70, 70. Western Union's undertaking is in the form of an agreement it signed with the office of the Florida Attorney General. See *id.*

enforcement of the terms of the contract by the threat of government sanction. This contrasts with consumer sovereignty, which is entirely self-enforcing, and industry self-regulation, where such enforcement as may occur is accomplished by private entities.

Under real-world conditions, the enforceability of contracts does not adequately protect consumers from overreaching by sellers. "In real markets, almost invariably consumers have markedly less power and information than suppliers. . . . The common law of contracts simply cannot afford consumers the protection they would seek if they were rational, fully informed, and equal in economic power to the supplier."⁹²

Governments are inevitably involved in facilitating the operation of the regime of contract, as they must provide a forum for the enforcement of contractual obligations that are in dispute.⁹³ In addition to acting as the adjudicator of contract disputes, and the enforcer of the resulting resolution, government can facilitate the effectiveness of a contract regime by taking the part of one of the disputants. This is in effect what occurs when a government agency brings a civil enforcement action based on violation of laws prohibiting deceptive marketing practices. Depending on the applicable enforcement scheme, an enforcement agency may bring such an action either in its own name or as *parens patriae* on behalf of injured consumers. Where the remedy is based on a contract measure of damages owed to injured consumers,⁹⁴ the economic effect of such an enforcement action is similar to that of a class-action breach-of-contract suit.

Government regulation that is indifferent to market forces. A nearly pure form of government regulation is that which is indifferent, or in opposition, to market forces. Examples of such regulation for the benefit of consumers include

⁹²John Goldring, *Netting the Cybershark: Consumer Protection, Cyberspace, the Nation-State, and Democracy*, in *BORDERS IN CYBERSPACE*, *supra* note 152, at 322, 324-25.

⁹³Even when contractual disputes are resolved by binding arbitration, governments must stand prepared to enforce arbitral awards.

⁹⁴Under U.S. law, a contract measure of damages is generally applicable to actions based on fraudulent misrepresentations. According to the Restatement of Torts, "[t]he recipient of a fraudulent misrepresentation in a business transaction" is entitled to "damages sufficient to give him the benefit of his contract with the maker, if these damages are proved with reasonable certainty." *RESTATEMENT (SECOND) OF TORTS* § 549(2) (1965). The Comment to this provision states that U.S. courts have adopted "a broad general rule giving the plaintiff, in an action of deceit, the benefit of his bargain with the defendant in all cases, and making that the normal measure of recovery in actions of deceit." *Id.* at cmt. g. An annotation on this subject states that where the plaintiff enters a contract

in reasonable reliance upon the defendant's fraudulent misrepresentation as to the value of the property, goods, or services plaintiff was to receive, the courts have frequently recognized, as the proper measure of compensatory damages, that plaintiff was entitled to receive the benefit of the bargain as defendant represented it, so that the measure of damages was the difference between the actual value of what plaintiff received and its value as represented by defendant.

J. F. Rydstrom, "*Out of Pocket*" or "*Benefit of the Bargain*" as Proper Rule of Damages for Fraudulent Representations Inducing Contract for the Transfer of Property, 13 *A.L.R.3d* 875, 885 (1967).

1999]

PROTECTING THE DIGITAL CONSUMER

regulation of the purity of food, drink, and medicines,⁹⁵ the safety of consumer products,⁹⁶ and the procedures relating to the extension of consumer credit.⁹⁷

Hybrid market governance mechanisms. Marketplace governance may occur through a confluence of actions taken by governments, businesses, technological standards groups, and consumers. This may be the most appropriate, and inevitable, regulatory model for the Internet.⁹⁸ An example is the development of user-side Web filtering software. Congress's 1996 enactment of the Communications Decency Act, which among other things sought to prevent the transmission of "indecent" material to children, gave impetus to the development of technologies enabling parents to limit the material that their children could access via the Internet.⁹⁹ The crucial elements of the technology were user-side filtering software, with names like "Net Nanny" and "CYBERSitter," that allowed parents to choose what types of content (nudity, violence, references to homosexuality, hate speech) would be blocked, and the Platform for Internet Content Selection ("PICS"), a standard allowing both self-rating and third-party rating through meta-data tags describing the content of Web pages. Four separate interest groups played a crucial role in bringing about this form of regulation: the government, through enactment of a heavy-handed regulatory regime (which was subsequently invalidated as unconstitutional¹⁰⁰); business, through development of the necessary technology; technological standards groups, through development of PICS;¹⁰¹ and consumers, who choose on an individual basis whether to make use of the technology and what categories of content to block. Regulation of this sort may fly under the radar of those who conceive of law in the Austinian sense as "a command backed by threats, issued by a sovereign who acknowledges no superior,

⁹⁵Prior to the introduction of anti-adulteration legislation, market forces had brought about this situation:

The addition of water to milk and to beer was commonplace. Exhausted tea leaves were added to fresh tea, the exhausted leaves being glazed with black lead. Coffee had roast vegetable material, such as acorns, added to it. Bread was bulked up by inclusion of mashed potato and alum was added as a bleach. Mustard was adulterated by the addition of wheat flour, pea flour and much else. Sand was added to sugar.

SMITH & SWANN, *supra* note 203, at 101.

⁹⁶The Consumer Product Safety Commission is charged with protecting "the public against unreasonable risks of injury associated with consumer products," 15 U.S.C. § 2051(b)(1) (1994), and has the power, among other things, to ban unreasonably hazardous consumer products from the marketplace, *see id.* at § 2057.

⁹⁷Applicable statutes include the Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692-1692o (1994 & Supp. II 1996); the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (1994 & Supp. II 1996); and the Fair Credit Billing Act, 15 U.S.C. §§ 1666-1666j (1994).

⁹⁸*See* Reidenberg, *supra* note 202, at 926 ("For global networks, governance should be seen as a complex mix of state, business, technical, and citizen forces. Rules for network behavior will come from each of these interest centers.").

⁹⁹*See supra* text accompanying note 157.

¹⁰⁰*See supra* note 157.

¹⁰¹*See infra* note 283.

directed to a geographically defined population which renders that sovereign habitual obedience.”¹⁰²

Another, less exotic, hybrid market governance mechanism consists of the adoption of industry-created codes as law. For example, state and local building codes typically incorporate industry-created technical standards, effectively elevating such standards to the status of law.¹⁰³ Industry’s participation in the legislative process through the vehicles of lobbying and making campaign contributions may be viewed as a less visible example of this mechanism.

*B. The Need for Government Intervention to Control
Deceptive Conduct in Electronic Commerce*

The necessity of government intervention in the marketplace to protect consumers against deceptive marketing practices is nearly universally recognized. Mainstream economists agree that it is justified on grounds of market failure, and the propriety of government activity in this realm is not open to serious challenge.¹⁰⁴

The arguments that justify government regulation aimed at preventing deceptive marketing practices conveyed via print, telephone, or broadcast media equally support a government role in protecting consumers from similar conduct occurring online. The same market failures are present whether a consumer makes purchasing decisions based on a direct mail piece, an electronic mail message, or a Web-based sales presentation; is looking at a paper-and-ink catalog, or an online version; receives an interactive sales pitch from a telemarketer or in a chat session; or views an advertisement in a newspaper, on a physical bulletin board, or in a Usenet newsgroup. In fact, information asymmetries are likely to be exacerbated in the context of online commerce.¹⁰⁵ Deceptive marketing practices result in the

¹⁰²James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 189-95 (1997). Some critics argue that “private” forms of censorship, such as user-side Web filtering software, as well as technical specifications like PICS that enable label-based filtering, pose a greater threat to free speech than heavy-handed regulation like the Communications Decency Act. See Lawrence Lessig, *Tyranny in the Infrastructure*, WIRED, July 1997, at 96, 96 (“Software code—more than law—defines the true parameters of freedom in cyberspace.”); Amy Harmon, *Technology to Let Engineers Filter the Web and Judge Content*, N.Y. TIMES, Jan. 19, 1998, at D1 (contending that in developing PICS, the World Wide Web Consortium “is taking on a quasi-governmental role” and “will have more influence than most national governments will have”); Andrew L. Shapiro, *The Danger of Private Cybercops*, N.Y. TIMES, Dec. 4, 1997, at A30 (“[T]echnology can be an even more cunning censor than law.”).

¹⁰³See Swire, *supra* note 215, at 8.

¹⁰⁴See ASCH & SENECA, *supra* note 200, at 420 (“The real question . . . is not whether government should be ‘in’ or ‘out’ of the consumer protection field; but whether *marginal* changes in its role are, on balance, beneficial.”) (emphasis in original).

¹⁰⁵See AUSTRALIAN COMPETITION & CONSUMER COMM’N, *supra* note 6, at 7.

Asymmetry of information is likely to be a greater problem for transactions that do not involve face to face transactions because consumers cannot see the products they are purchasing or the set-up of the retailer or service provider, or check for features like dispute resolution mechanisms, money back guarantees and privacy safeguards.

Id.

1999]

PROTECTING THE DIGITAL CONSUMER

same consumer injury whether payment is made with cash or e-cash; whether with a credit card number tendered by telephone, or one transmitted over a secure online connection.

Policymakers who have addressed the question have uniformly concluded that governments have a role to play in enforcing laws prohibiting deceptive marketing practices in the context of Internet commerce. Thus, the U.S. administration policy paper on global electronic commerce, while advocating “a non-regulatory, market-oriented approach to electronic commerce,”¹⁰⁶ recognizes a special role for government with respect to preventing fraud:

In order to realize the commercial and cultural potential of the Internet, consumers must have confidence that the goods and services offered are fairly represented, that they will get what they pay for, and that recourse or redress will be available if they do not. This is an area where government action is appropriate.¹⁰⁷

The paper also commits the U.S. government to exploring “opportunities for international cooperation to protect consumers and to prosecute false, deceptive, and fraudulent commercial practices in cyberspace.”¹⁰⁸ Similarly, Australia’s policy paper states: “The successful enforcement of laws relating to trading practices and fraud is crucial to establishing a favourable environment in which consumers can do business.”¹⁰⁹

*C. Four Dogmas of Cyberspace Utopianism: The Argument
Against Government Regulation of Electronic Commerce*

¹⁰⁶CLINTON & GORE, *supra* note 170, at 2.

¹⁰⁷*Id.* at 27.

¹⁰⁸*Id.*

¹⁰⁹[AUSTRALIAN] FEDERAL BUREAU OF CONSUMER AFFAIRS, *supra* note 75, at 24; *see also* MINISTRY OF CONSUMER AFFAIRS, ELECTRONIC COMMERCE AND THE NEW ZEALAND CONSUMER 12-13 (1997); *Ministerial Declaration ¶¶ 20-21* (visited Apr. 14, 1999) <<http://www.echo.lu/bonn/final.html>>.

Some critics have argued that governments should play a far more limited role in regulating the Internet than they do in regulating economic activity taking place via other communications media. Several grounds, both positive and normative, have been advanced in support of this point of view.

1. “Cyberspace Is a Self-Contained Jurisdiction, over Which
Territorially Based Sovereigns Have No Legitimate
Authority.”

One prominent set of critics advocates “conceiving of Cyberspace as a distinct ‘place’ for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the ‘real world.’”¹¹⁰ The view that “[c]yberspace radically undermines the relationship between legally significant (online) phenomena and physical location,”¹¹¹ thereby rendering unusable all territorially based notions of jurisdiction and choice of law, is based on several observations: (1) “[t]he effects of cyberspace transactions are felt *everywhere*, simultaneously and equally in all corners of the global network”;¹¹² (2) “the cost and speed of message transmission on the Net is almost entirely independent of physical location”;¹¹³ (3) “there is no necessary connection between an Internet address and a physical jurisdiction”;¹¹⁴ (4) the Internet allows transactions between people “who do not and *cannot* know the physical location of the other party”;¹¹⁵ and (5) certain types of online communications, such as Usenet newsgroups, “have no recognizable tie at all to physical places but take place only on the network itself.”¹¹⁶ In sum, “events in cyberspace take place ‘everywhere if anywhere, and hence no place in particular,’”¹¹⁷ and therefore no territorial sovereign has legitimate authority over any such events.¹¹⁸

2. “Attempts by Territorially Based Sovereigns to Exert
Control over Online Transactions Will Inevitably Prove
Futile.”

¹¹⁰David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378 (1996).

¹¹¹*Id.* at 1370.

¹¹²David G. Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155, 162 (1996) (emphasis in original).

¹¹³Johnson & Post, *supra* note 248, at 1370.

¹¹⁴*Id.* at 1371.

¹¹⁵Post, *supra* note 250, at 161 (emphasis in original).

¹¹⁶*Id.* at 160.

¹¹⁷*Id.* at 159 (quoting Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1404 (1996)); see Paul Edward Geller, *Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked World*, 20 COLUM.-VLA J.L. & ARTS 571, 573 (1996) (“It is no longer possible to localize works at any single point in transterritorial cyberspace, which William Gibson prophetically called the ‘space that wasn’t space.’”).

¹¹⁸See Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 JURIMETRICS J. 1, 9 (1994) (“An attempt to impose and enforce real world laws on this cyber society would be akin to an attempt to impose a new legal system on a conquered or colonized nation.”).

1999]

PROTECTING THE DIGITAL CONSUMER

This, the argument runs, is because “[i]ndividual electrons can easily, and without any realistic prospect of detection, ‘enter’ any sovereign’s territory. The volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities.”¹¹⁹ Government efforts to erect barriers preventing unwanted online communications from reaching their citizens will fail, as “the determined seeker of prohibited communications can simply reconfigure his connection so as to appear to reside in a location outside the particular locality, state, or country.”¹²⁰ “[A]ny effort to regulate people’s activities from the privacy of their homes is . . . doomed to fail.”¹²¹

3. “If One Government May Apply Its Laws
Extraterritorially, So May All Others, Resulting in a Clash of
Jurisdictions and a Requirement to Comply with All Nations’
Laws Simultaneously.”

¹¹⁹Johnson & Post, *supra* note 248, at 1372; see Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J.L. & PUB. POL’Y 475, 502 (1997) (asserting that online communications “permit a user to enter, or at least to cross numerous national, state, or local borders without either the user or national authorities being aware of the user’s passage”).

¹²⁰Johnson & Post, *supra* note 248, at 1374.

¹²¹Grossman, *supra* note 58, at 28.

If Minnesota may exert jurisdiction over persons located outside its borders, it is said, then the same is true of all other territorial sovereigns. This would mean, for example, “that Singapore or Iraq or any other sovereign can regulate the activities of U.S. companies operating in Cyberspace from a location physically within the United States.”¹²²

4. “Online Conduct Can Be Effectively Regulated by Those Who Engage in It.”

The argument that cyberspace is a “place” separate from any territorial jurisdiction leads the critics of government regulation to conjure a utopian vision of a self-governing Republic of Cyberspace, drawing upon an analogy with the *lex mercatoria* that governed international commerce in the Middle Ages.¹²³ Since government regulatory authorities cannot legitimately seek to control fraudulent online activity that originates from outside the jurisdiction, this task should be left to “[t]hose who establish and use online systems,” who “have an interest in preserving the safety of their electronic territory,” and “are more likely to be able to enforce their own rules.”¹²⁴ “Like any other community, online communities use censure and other peer group actions to enforce their own rules. . . . When legal action is sometimes required, the standards of the local community are applied, not those of a distant town in another state, nor those of any hypothetical national censorship body.”¹²⁵

D. The Dogmas Dissected: Cyberspace Utopianism Has No Clothes

¹²²Johnson & Post, *supra* note 248, at 1374.

¹²³*See id.* at 1389-90; *see also* Hardy, *supra* note 76, at 1021. The law of outer space, the law maritime, and the law of Antarctica have also been advanced as suitable analogies. *See* Burnstein, *supra* note 105, at 103-12.

¹²⁴Johnson & Post, *supra* note 248, at 1383.

¹²⁵Brief for Amicus Curiae Electronic Frontier Foundation, *Thomas v. United States*, 74 F.3d 701 (6th Cir. 1996) (Nos. 94-6648, 94-6649), *available at* <http://www.eff.org/pub/Legal/Cases/AABBS_Thomas_Memphis/eff_aa_041995_amicus.brief>.

1999]

PROTECTING THE DIGITAL CONSUMER

The cyberspace utopians¹²⁶ reach their anti-regulatory conclusions through arguments that are flawed in several respects. First, they mischaracterize the salient aspects of online communications. Second, they exaggerate the difficulties that the special characteristics of online communications pose for extension of the existing regulatory regime to online commercial transactions, ignoring the fact that many of those characteristics apply also to other communications media. Third, they make no effort to adapt the existing regulatory regime to the requirements of the new medium. Fourth, they make unsupported assumptions about the ability of users of online communications to control deceptive marketing practices.

1. The Special Characteristics of Online Communications Do
Not Undermine the Legitimacy of Territorially Based
Jurisdiction

The key flaw in the normative component of the utopians' argument is that the harmful effects of deceptive marketing practices accomplished through use of the Internet are felt not solely in the realm of cyberspace, but also and unavoidably by a flesh-and-blood resident of a real-world geographic area subject to the territorial jurisdiction of a sovereign.¹²⁷ If a sovereign has the right and responsibility to protect its citizens from fraudulent solicitations delivered by postal mail, telephone, radio, television, or print media, it has an equal right and responsibility to protect them from fraud delivered via the Internet. "[T]he legitimacy of regulation turns upon effects. If the [Inter]net has an effect on that half of the cybercitizen that is in real space, if it has an effect on third parties who are only in real space, then the claim of a real space sovereign to regulate it will be as strong as" in the case of like effects brought about through other media.¹²⁸

The person responsible for online deceptive marketing practices is likewise a resident of a geographic territory subject to the jurisdiction of a territorial sovereign. Physical presence within the territorial jurisdiction of a sovereign has since ancient times stood as the paradigm basis for assertion of jurisdiction in personam.¹²⁹ No reason appears why a wrongdoer should be able to nullify this basis of jurisdiction merely by choosing to communicate through the online medium, rather than through other means of communication at a distance.

¹²⁶“Utopian” is an apt description of the point of view set forth above in two senses. First, holders of this view conceive of cyberspace as a utopian realm whose citizens can live in perfect harmony without the need for supervision by government. Second, the word “utopia” derives from Greek terms meaning “no place”—which is where the cyberspace utopians believe their realm to exist.

¹²⁷See William S. Byassee, *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Commun*, 30 WAKE FOREST L. REV. 197, 199 (1995) (“The interactions between users in cyberspace have effects in real world jurisdictions, and the inhabitants of cyberspace are also citizens of a physical jurisdiction.”); Hardy, *supra* note 76, at 1012 (“[R]esidents of cyberspace are also residents of ‘real’ spaces.”).

¹²⁸Lessig, *supra* note 255, at 1404. To the same effect, see Zembek, *supra* note 162, at 347 (stating that cyberspace is not a separate realm, but rather “a communication medium through which real persons do real things”).

¹²⁹See 4 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, *FEDERAL PRACTICE AND PROCEDURE* § 1064, at 227-34 (2d ed. 1987).

a. Online Communications, Though
Universally Accessible, Have Locally
Differentiated Impact

The contention that “[t]he effects of cyberspace transactions are felt *everywhere*, simultaneously and equally in all corners of the global network,”¹³⁰ is factually incorrect. It is true that certain types of online communications, such as Web sites and newsgroup postings, are simultaneously and equally *accessible* from any geographic location with the necessary online access. However, the *effects* resulting from that access may vary greatly from place to place. Most pertinently to the present context, a solicitation to enter into a fraudulent transaction has a very different effect in a jurisdiction where a resident actually enters into the proposed transaction than in other jurisdictions where residents read the solicitation but do not act upon it. In both jurisdictions there is some resulting pollution of the commercial dialogue, by virtue of the misinformation that is conveyed to consumers, but only in the former jurisdiction does any consumer suffer direct financial injury. Therefore, it is hardly “indeterminate” to speak of online conduct that “has or is intended to have substantial effect within [a State’s] territory”¹³¹—one standard formulation of the principle governing whether a state has jurisdiction to prescribe rules applicable to a person located outside its territorial scope.¹³² We may conclude that the mere maintenance of a Web site, without more, does not satisfy this criterion. But there is no logical or doctrinal difficulty with a finding that one who enters into a commercial transaction with a person, knowing that person’s geographic location, both has and intends to have substantial effects within that jurisdiction.

b. Cost and Speed Advantages of Online
Communications Create Only Practical Issues

¹³⁰See Post, *supra* note 250, at 162 (emphasis in original).

¹³¹*Id.* (quoting RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW, *supra* note 77, § 402(1)(c) (1987) (alteration in original)).

¹³²Jurisdiction to prescribe and to adjudicate are discussed *supra* at text accompanying notes 78-92.

1999]

PROTECTING THE DIGITAL CONSUMER

The fact that “the cost and speed of message transmission on the Net is almost entirely independent of physical location”¹³³ creates practical problems for law enforcement authorities, but does not radically undermine the territorial basis of jurisdiction. The cost of first-class postage within the United States is typically the same regardless of the geographic separation of the sender and recipient, and it may take only a few days longer for a letter to cross the country than it does to cross a state or a city. The cost of overnight mail delivery within the United States, and the length of time required for delivery, are the same or nearly the same no matter where the sender and recipient are located. The cost of an interstate telephone call within the United States varies little with the distance between the two speakers. Yet we do not consider that the use of direct mail or telemarketing as a medium for conveying commercial communications radically undermines the geographic basis for jurisdiction within the United States; we do not declare “telespace” or “mailspace” to be a “place” unconnected with any territorial jurisdiction. Instead, the legal systems of the various jurisdictions within the United States have developed a more-or-less elaborate jurisprudence for determining under what circumstances a seller located in one state may be brought within the jurisdiction of a court located in another state.

The novelty of online communications, as discussed above,¹³⁴ is that the cost and speed of communications remain invariant even when crossing national boundaries. This factor opens the door to a great expansion of international commercial transactions that were previously infeasible, due to the high costs and time delays associated with international mail and telephone service. But the logical and doctrinal bases of territorially based jurisdiction remain unchanged. The challenge is rather to devise jurisdictional rules applicable in the online context that take account of the factors that have traditionally been considered relevant to resolving questions of jurisdiction—such as the effects of the defendant’s conduct in the forum jurisdiction, the defendant’s state of mind, the burden on the defendant of being forced to defend herself in a foreign forum, the interests of the forum, and the interests of the plaintiff in obtaining a remedy—with the goal of striking an appropriate balance among the competing interests.

¹³³Johnson & Post, *supra* note 248, at 1370.

¹³⁴*See supra* text accompanying note 75.

c. Virtual Addressing Does Not Undermine
Territorial Sovereignty

The fact that “there is no necessary connection between an Internet address and a physical jurisdiction”¹³⁵ likewise gives rise to practical difficulties, but does not call into question the territorial basis for jurisdiction. This fact may make it difficult for injured parties and enforcement authorities to identify the perpetrator of prohibited conduct, but is without any deeper significance. It is equally true that there is no necessary connection between a toll-free telephone number—the only “address” that a purchaser may ever have for a vendor that operates via telemarketing—and the physical location of the vendor communicating through that telephone number. Mail forwarding services likewise divorce a seller’s address from his physical location. Yet assertion of jurisdiction by territorially based sovereigns is not thought on that account to be illegitimate.

d. Physical Location of Online Interlocutors Is
Not Unknowable

The assertion that the Internet allows transactions between people “who do not and *cannot* know the physical location of the other party”¹³⁶ is not quite correct. The statement refers to the fact, as discussed above,¹³⁷ that an online address — whether an e-mail address, the URL of a Web site, or a pseudonym used in a chat session—does not itself reveal the physical location of the person who communicates using that address. In many of the most common types of interactions that occur online, it is true that neither party knows the physical location of the other. For example, the owner of a Web site may not know the location of those who access the site; those who access a Web site may not know the location of the owner of the site; those who read newsgroup postings may not know the location of the message posters; and recipients of unsolicited commercial e-mail messages may not know the location of the sender. However, it is not true that online communicators *cannot* know the location of their interlocutors. Most obviously, there is nothing to prevent a Web site, e-mail message, or newsgroup posting from stating the physical address of the person communicating through it.

In the more particular case of online commerce, the vendor most typically *can and does* know the location of his customers. This is because most of the online commerce that takes place at present involves shipping a physical good (flowers, computers, books, compact disks, etc.) to a geographic address. In many cases, even sellers of digital goods that are transmitted via the network likewise *can and do* know the location of their customers. This is so when there is an ongoing commercial relationship between the two parties which involves sending invoices or other physical items to the customer’s geographic location. There are, it is true, commercial transactions involving digital goods in which the nature of the transaction does not *require* either party to know the location of the other—for example, the transmission of information via the network on a one-time basis, with

¹³⁵Johnson & Post, *supra* note 248, at 1371.

¹³⁶Post, *supra* note 250, at 161.

¹³⁷*See supra* text accompanying notes 146-52.

1999]

PROTECTING THE DIGITAL CONSUMER

payment by credit card or digital cash. However, even in those cases there are steps that a seller can take—some more reliable, but more cumbersome, than others—to ascertain the physical location of the buyer. For example, the seller may require the buyer to provide a telephone number or fax number, which indicates the buyer's physical location; may perform a pre-sale verification of location through postal mail; or may access motor vehicle or voter registration records.¹³⁸ In the future, digital certificates indicating the holder's address may become available.

It is of course an everyday occurrence to communicate by telephone or postal mail without being aware of the location of one's interlocutor. A toll-free telephone number gives no indication of the location of the holder of the number. An incoming telephone call does not disclose its geographic origin, unless the recipient subscribes to a caller ID service *and* the caller elects not to have his number blocked. Commercial correspondents frequently make use of a post office box address, or a private mailbox service, that does not reveal their geographic position. This ordinarily raises no issues: when I call the toll-free number of a catalog company to order a product, it is of no concern to me where the order-taker is located; it is of no more concern to me where my e-mailed order to the same company is received or read.

¹³⁸A system for online verification of a purchaser's geographic location is currently in use by Netscape Communications Corp. Netscape makes its browser software available for download via the Internet. *See* Netscape Prods., *Installation Options* (visited Apr. 14, 1999) <http://home.netscape.com/download/client_options.html>. The version of the software incorporating strong encryption is, under U.S. law, available only to citizens of the United States and Canada. *See id.* As Netscape explains on its Web site:

The strong U.S./Canada-only encryption version is available in French and English to U.S. and Canadian citizens and to permanent residents of the United States only. Because the U.S. government restricts export of any product using 128-bit encryption, you will be asked to fill out an Eligibility Declaration stating that you are a U.S. or Canadian citizen or a legal permanent resident of the United States before you will be allowed to download the software you've selected. The Eligibility Declaration will be stored in a database and made available to the U.S. government upon request.

Id. The Eligibility Declaration form requires submission of one's physical address, and indicates that a verification of the submitted information will be performed. *See id.*

The ability of wrongdoers to conceal their location when using these traditional means of communication is viewed by law enforcement officials as an impediment to law enforcement that must be handled with due regard for privacy interests; it has never been considered a factor that divests territorially based sovereigns of their authority to enforce the law. Likewise, the fact that it is possible to communicate via the Internet without revealing one's physical location does not undermine the geographic basis of jurisdiction over online transactions.

e. The Relevant Factor Is the Location of the
Communicators, Not the Location of the
Communication

The assertion that certain types of online communications, such as Usenet newsgroups, "have no recognizable tie at all to physical places but take place only on the network itself"¹³⁹ does nothing to clarify the issues. The statement is true in a sense: Usenet is a distributed system, and postings do not reside in any central location. But the statement obscures the fact that both the person who posts a newsgroup message and the person who reads it *do* have an ascertainable physical location. The authority of territorially based sovereigns to assert jurisdiction over a transaction arising from a newsgroup posting is not based upon the wholly indefinable location of the *communication*, but rather on the locations of the *communicators*. The "location" of a telephone call, or of a letter sent through the postal system, is just as indefinable as the "location" of a Usenet posting. Yet we do not for that reason deny the legitimacy of government regulation of telemarketing or direct mail solicitations.

2. The Argument from Futility Refutes Only One,
Particularly Poor, Enforcement Approach

Attempting to police borders within cyberspace is said to be futile because of the large number of border crossing points. "Physical roads and ports linking sovereign territories are few in number, and geographic boundaries can be fenced and policed. In contrast, the number of starting points for an electronic 'trip' out of a given country is staggering, consisting of every telephone capable of connecting outside the territory."¹⁴⁰ Furthermore, the volume of online communications is so great that "a customs house on an electronic border would cause a massive traffic jam."¹⁴¹ The same is true, however, of communications by telephone and postal mail. Since both voice and data are transmitted along the same copper and fiber optic pathways, it is as infeasible to bottle up telephone conversations as it is to contain online communications. The routes by which postal mail moves from sender to recipient are likewise "staggering" in number. The volume of postal mail is so great that each item can be subjected to no more than a perfunctory customs clearance procedure, and the idea of screening all telephone calls for content is so ridiculous that it has probably never been seriously proposed.

¹³⁹ Post, *supra* note 250, at 160.

¹⁴⁰ Johnson & Post, *supra* note 248, at 1372 n.17.

¹⁴¹ *Id.*

1999]

PROTECTING THE DIGITAL CONSUMER

The basic flaw in the argument from futility is that it assumes the wrong enforcement paradigm—namely, preventing prohibited communications from reaching residents of a particular territorial jurisdiction.¹⁴² Although governments have attempted to apply this paradigm—notably Germany, in its efforts to prevent its citizens from gaining access to pornography and hate speech, and Singapore, which requires local Internet service providers to filter out “prohibited material”¹⁴³—this is not the only approach available to a territorial sovereign that wishes to protect its citizens from deceptive commercial communications. The better approach is the one that is currently applied to communications at a distance. No restrictions are placed on a seller’s ability to communicate with potential buyers. However, if a seller proposes or procures a commercial transaction through deceptive marketing methods, in violation of the law of the jurisdiction where a buyer is located, the seller may be subject to enforcement action by the government of that jurisdiction.

3. The Problem of Overlapping Jurisdiction Can Be Addressed Through Approaches Less Drastic Than Abdication

The problem of overlapping jurisdiction is a real one, which arises from the facts that: (1) given present technology, the maker of an online communication cannot limit the locations in which the communication may be received; and (2) laws applying to online conduct vary from one jurisdiction to another. The appropriate solution to the problem, however, is not to bar all exercises of jurisdiction by government (whether acting in a legislative, adjudicative, or enforcement role), but rather to constrain such exercises of jurisdiction in a way that balances the various interests at stake. In the case of business-to-consumer commercial transactions, the approach proposed below is to allow online sellers to “opt out” of assertions of jurisdiction by particular states by limiting the extent of their contacts with residents of those states.

4. Deceptive Marketing Practices Are Not Likely To Be Adequately Controlled by Market Forces Alone

The cyberspace utopians argue that market forces are sufficient to prevent and redress consumer injury from deceptive marketing practices, and that government intervention is therefore unnecessary. This view fails to take account of the fact that the problem of fraud—whether perpetrated online or via some other means of communication—is highly resistant to control by market forces. It also oversimplifies by failing to recognize the interaction between regulation by market forces and government regulation.

¹⁴²“The fallacy is to focus on the electronic bits, which indeed are very hard to control. Communications are a matter not just of signals but of people, institutions and physical hardware; the arm of the law can reach them.” Eli M. Noam, *An Unfettered Internet? Keep Dreaming*, N.Y. TIMES, July 11, 1997, at A27.

¹⁴³See *supra* note 152.

It is easy to see why online deceptive marketing practices are unlikely to be controlled by market forces alone. The main lines of defense that the market erects—consumer sovereignty, industry self-regulation, and contract—are overmatched by online swindlers. By conveying misinformation to consumers, swindlers intend to interfere with the workings of consumer sovereignty, and they often succeed. While the market has evolved several mechanisms for improving the flow of information to online consumers—certification systems have been put into practice;¹⁴⁴ ratings systems allow consumers to filter out certain categories of Web sites;¹⁴⁵ non-governmental organizations provide consumers with information about online scams¹⁴⁶—these are simply online versions of mechanisms that pre-existed the Internet. Although they can certainly help in alleviating the problem of

¹⁴⁴The Council of Better Business Bureaus (of the United States and Canada) has implemented a Web-site certification program called BBBOnLine. Businesses that comply with certain conditions established by the BBB, including agreeing to participate in BBB's advertising self-regulation program, are entitled to display a "BBBOnLine" icon on their Web site. See Oldenburg, *supra* note 127, at D5; Better Business Bureau, *supra* note 127. The Internet Industry Association of Australia has a similar program. See [AUSTRALIAN] FEDERAL BUREAU OF CONSUMER AFFAIRS, *supra* note 75, at 27. A Web site called "Public Eye" maintains a directory of what it describes as "Certified Safe Shopping Sites." *Public Eye* (visited Mar. 20, 1999) <<http://www.thepubliceye.com>>. The American Institute of Certified Public Accountants ("AICPA") and the Canadian Institute of Chartered Accountants operate a Web-site certification program called CPA WebTrust. See Christopher J. Dorobek, *CPAs Hope to Build Trust in Electronic Commerce*, REP. ELECTRONIC COM., Sept. 23, 1997, at 10, 10; AICPA, *AICPA Online* (last modified Mar. 19, 1999) <<http://www.aicpa.org>>.

¹⁴⁵The World Wide Web Consortium, an international industry consortium formed to promote growth of the Web through development of technical protocols, has formulated a protocol known as the Platform for Internet Content Selection ("PICS"), which allows Web users to set their browsers to block access to certain categories of Web documents. See W3C, *Platform for Internet Content Selection* (last modified Jan. 3, 1998) <<http://www.w3c.org/PICS>>. Using PICS, Web sites or documents may be rated by third-party rating organizations, using any conceivable set of rating criteria—sexual content, hate speech, privacy protection, violent content, political or religious criteria. The Web user selects which rating system to implement, and the browser automatically blocks access to Web documents that do not carry an acceptable rating. See Paul Resnick, *Filtering Information on the Internet*, SCI. AM., Mar. 1997, at 62. "Such rating systems could tell you immediately which cyber malls or cyber sellers have been rated as reliable by a disinterested third party, such as the FTC or the Better Business Bureau." Pridgen, *supra* note 65, at 254.

Rating and filtering systems, however, carry a cost: they may result in "blocking access to a significant amount of the individual, idiosyncratic speech that makes the Internet a unique medium of mass communication. Filtering software, touted as a speech-protective technology, may instead contribute to the flattening of speech on the Internet." Jonathan Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J. 453, 477 (1997).

¹⁴⁶Several Web sites are devoted to this purpose, including NETrageous, Inc., *Internet ScamBusters* (visited Apr. 14, 1999) <<http://www.scambusters.org>>; *MMF Hall of Humiliation* (visited Feb. 11, 1999) <<http://www.ga.to/mmf/>>; National Fraud Info. Ctr., *Internet Fraud Watch* (visited Apr. 14, 1999) <<http://www.fraud.org/internet/intset.htm>>; Stopspam.org, *Welcome to www.stopspam.org* (visited Apr. 14, 1999) <<http://www.stopspam.org>>; and Webguardian Inc., *Webguardian* (last modified Jan. 1, 1999) <<http://www.webguardian.com>>.

1999]

PROTECTING THE DIGITAL CONSUMER

fraud in online commercial transactions, they are not likely to be significantly more effective than their offline analogues.

Vendors have also put into effect various types of online self-regulation: trade associations have promulgated industry codes of conduct,¹⁴⁷ which may be implemented through a “hallmark” program;¹⁴⁸ operators of online malls offer redress to consumers who are victimized by certain types of fraud at their sites,¹⁴⁹ and screen the businesses that they allow to set up shop;¹⁵⁰ one large Internet

¹⁴⁷The U.S. DMA has established principles for the use of unsolicited commercial e-mail. These principles provide, for example, that marketers should follow the stated policies of newsgroups, bulletin boards, and chat sessions with respect to online solicitations; clearly identify commercial e-mail as such; and provide recipients of unsolicited e-mail with a mechanism for opting out of future solicitations. See Direct Mktg. Assoc., *Responsibly Conquer a New Frontier with the DMA's Marketing Online Privacy Principles and Guidance* (visited Apr. 14, 1999) <<http://www.the-dma.org/busasst6/busasst-onmarkprivpr6a7.shtml>>. Beginning July 1, 1999, U.S. DMA members will be required to honor an industry-wide opt-out list of consumers who do not wish to receive unsolicited commercial e-mail. See Rajiv Chandrasekaran, *Direct Marketing Group Adopts New Guidelines*, WASH. POST, Oct. 16, 1997, at C3; Leslie Miller, *On-line Lament: Deliver Us from Junk E-mail*, USA TODAY, Nov. 5, 1997, at D4. The Canadian Direct Marketing Association has released a set of guidelines for e-mail marketing that are mandatory for its membership, and that require marketers to obtain a consumer's consent before sending an e-mail solicitation. See Menyasz, *supra* note 224, at 1115; Canadian Mktg. Assoc., *CMA* (visited Mar. 20, 1999) <<http://www.cdma.org>>.

The International Chamber of Commerce (“ICC”) has set forth guidelines applying to commercial communications on the Internet, which incorporate the ICC's guidelines on marketing in general and add several elements applying specifically to the online medium. International Chamber of Commerce, *ICC Revised Guidelines on Advertising and Marketing on the Internet* (last modified Apr. 2, 1998) <http://www.iccwbo.org/Commissions/Marketing/Internet_Guidelines.html>. For other examples of a trade association's self-imposed code of conduct, see the Internet Indus. Assoc. of Austl., *Internet Industry Code of Practice* (visited Apr. 14, 1999) <<http://www.intiaa.asn.au/Code4.html>>; Internet Alliance, *IA Addresses Unsolicited Bulk E-Mail* (visited Mar. 24, 1999) <http://interac.baweb.com/policy/spamming_guidelines.html>.

¹⁴⁸The Interactive Media in Retail Group (“IMRG”), an international association of businesses involved in electronic commerce, has produced a Code of Practice for Electronic Commerce. IMRG members who undertake to comply with the Code are allowed to display the IMRG Hallmark on their Web site. See IMRG, *The IMRG Code of Practice for Electronic Commerce & IMRG Hallmark* (visited Apr. 14, 1999) <<http://www.imrg.org/hallmark/default.htm>>.

¹⁴⁹Netmarket promises: “If your credit card number is stolen online while using Netmarket and fraudulent charges are made to that credit card, Netmarket will reimburse you for the amount of fraudulent charges not covered by your credit card issuer.” Netmarket, *Netmarket Security* (visited Apr. 14, 1999) <<http://www.netmarket.com>>. America Online (“AOL”) and Excite have similar policies. America Online, *Secure Transactions* (visited Apr. 14, 1999) <http://www.aol.com/amc/secure_transactions.html>; Excite, Inc., *Safe Shopping Guarantee & Certified Merchants* (visited Apr. 14, 1999) <<http://www.excite.com/shopping/guarantee>>. This sort of protection is quite limited, covering only consumer losses associated with unauthorized use of a credit card, which is in most cases limited by law or practice to \$50. It does not address the problem of deceptive solicitations.

¹⁵⁰AOL operates a “Certified Merchant” program. America Online, *Certified Merchants* (visited Apr. 14, 1999) <http://www.aol.com/amc/certified_merchants.html>. Sellers in

service provider “has decided not to provide website hosting or Internet access services to entities engaged in Internet-based gambling or other wagered activities which are determined to be illegal”;¹⁵¹ the online industry is engaged in a coordinated effort to develop software tools enabling parents to filter the online material to which their children are exposed.¹⁵² Yet these initiatives too are likely to fall short of what is required to control online deceptive marketing practices, for the simple reason that self-regulation “only binds the ‘good guys.’ Companies that do not have a reputation at stake have no ethical or business incentive to abide by self-regulatory principles”¹⁵³ Legitimate marketers recognize that a reputation for honesty is a prerequisite to long-term business success. The market provides them with a strong incentive to keep their customers happy. But perpetrators of fraud have no such interest. They do not need or expect to profit from repeat business or referrals from satisfied customers, and do not expect to remain long in the market. They have no incentive to follow voluntary codes of conduct. Once a fraudulent operation becomes known in the marketplace as such, its perpetrator simply pulls up stakes and moves on to the next scam.

In addition, one important type of self-regulation that is applied by traditional communications outlets—media screening—is of doubtful effectiveness in the online context. In the case of the traditional print and broadcast media, the number of media outlets that enable a vendor to get a marketing message to a regional, national, or multinational audience is relatively limited, and the owners of these outlets are relatively well-established business concerns. But with the online media, the number of outlets available to give an advertiser access to a global audience is virtually unlimited—any Internet hosting service, located anywhere in the world, will serve equally well—and not all of these providers will perceive an interest in enforcing standards of advertising conduct that are protective of consumer interests.

Contract-based solutions to the problem of online deceptive marketing practices are also inadequate. Most consumer-vendor disputes do not involve enough money

AOL’s online mall that meet a specified set of criteria are designated as “certified,” and agree to adhere to certain customer service guidelines. *Id.* Excite has a similar program. *See* Excite, Inc., *supra* note 287.

iMall, the proprietor of an online mall (<<http://www.imall.com>>), upon learning that one of its merchants had been the target of law enforcement action based on deceptive trade practices, “promised to study ways to prescreen multi-level marketing companies.” Laurianne McLaughlin, *Online Vendors: How Can You Tell the Good from the Bad?*, PC WORLD, Feb. 1997, at 56, 58.

¹⁵¹MCI WorldCom, *Internet Policy Vision* (Mar. 18, 1997) (visited Mar. 24, 1999) <<http://www.mci.com/mcisearch/aboutus/company/news/internetpolicy/contents.shtml>>.

¹⁵²*See* Melissa Healy, *Filters Planned for Internet to Shield Children*, L.A. TIMES, Dec. 2, 1997, at A12. This form of self-regulation is best viewed as a hybrid of industry self-regulation and consumer empowerment, brought about by the threat of government regulation. *See supra* text accompanying notes 236-41. The ACLU has harshly criticized this approach, finding it an unwarranted interference with the free expression of ideas on the Internet. *See* ACLU, *Fahrenheit 451.2: Is Cyberspace Burning?* (visited Apr. 14, 1999) <<http://www.aclu.org/issues/cyber/burning.html>>.

¹⁵³Angela Drolte, *U.S. Consumer Advocate Doubts Effectiveness of Industry-Initiated Online Privacy Policies*, 2 Electronic Commerce & L. Rep. (BNA) 601, 601 (June 13, 1997) (quoting the testimony of Janlori Goldman at an FTC public workshop on consumer information privacy).

1999]

PROTECTING THE DIGITAL CONSUMER

to justify bringing a breach-of-contract action, and class actions will only rarely be available. This effect will become more pronounced as a larger number of online transactions take on an international character. Even where money losses are high, the online medium makes it easy for swindlers to disguise their identity and location, rendering contract actions useless.

The Internet Alliance (“IA,” formerly the Interactive Services Association, or “ISA”), a trade association consisting of businesses involved in providing products or services relating to the online medium, has well expressed the view that online fraud is a special case requiring government intervention. The IA believes that the general problem presented by bulk commercial e-mail—the fact that most recipients and members of the online industry consider it an unwanted and costly intrusion—is best addressed through self-regulation and technological solutions, rather than legislative prohibitions.¹⁵⁴ However, the organization also believes that law enforcement action is required to address the fraudulent aspects of bulk e-mail, including both fraudulent solicitations contained in the content of such e-mails and deception in the use of forged headers and other means of disguising the source of the e-mail.¹⁵⁵

Governments can and should intervene in online commercial transactions in a manner that is unobtrusive and complements the workings of market-based control mechanisms. They can facilitate the working of consumer sovereignty by requiring vendors to disclose certain categories of information to prospective purchasers where appropriate, forbidding sellers to make deceptive or misleading representations, and promoting consumer education. They can serve as a catalyst by encouraging industry to create self-regulatory mechanisms to control fraud. They can facilitate the functioning of the contract regime by bringing breach-of-contract actions on behalf of injured consumers and acting as adjudicator in private actions.

In the absence of a functioning system to control online deceptive marketing practices, frustrated users are likely to resort to self-help.¹⁵⁶ But a regime of online vigilantism is not an entirely attractive prospect. As with all types of vigilantism, when denizens of cyberspace take matters into their own hands there is a risk of arbitrariness and collateral damage.¹⁵⁷ In one such episode, online users who believed that UUNet, a major Internet service provider, was not taking adequate steps to prevent spamming, began a campaign of canceling all newsgroup

¹⁵⁴ “[T]he ISA believes that the most effective ultimate solution will be through technology and the organization and its members are committed to help in finding such a solution.” Internet Alliance, *ISA Addresses Unsolicited Bulk E-Mail (June 24, 1997)* (visited Mar. 24, 1999) <<http://www.isa.net/news/970624.html>>.

¹⁵⁵ “[T]he ISA believes that in order for self-regulation to work in this context, the Federal Trade Commission and the States Attorneys General must take an aggressive approach to enforcement of their rules about fraudulent or unfair and deceptive trade practices.” *Id.*

¹⁵⁶ See Byassee, *supra* note 265, at 216-17.

¹⁵⁷ See Michael W. Carroll, *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations*, 11 BERKELEY TECH. L.J. 233, 256 (1996) (“Vigilante justice generally is a troubling form of regulation because results are unpredictable and often appear more arbitrary than the results under a more formal system.”).

messages posted by UUNet subscribers.¹⁵⁸ While the action persuaded UUNet to work harder at controlling spam, it also prevented many innocent UUNet subscribers from posting legitimate newsgroup messages.¹⁵⁹ In another incident, an opponent of anonymous remailers set up a “cancelbot”—a software program that deletes newsgroup postings—to cancel messages posted from a particular remailer.¹⁶⁰ However, due to a programming error the cancelbot had the unintended effect of deleting other messages as well.¹⁶¹

Vigilante tactics to counter unsolicited commercial e-mail by launching a fusillade of return e-mail messages “typically backfire.”¹⁶² Online users who respond to unwanted commercial e-mail messages by mail-bombing the sender assist the spammer by verifying the validity of the recipient’s e-mail address.¹⁶³ In addition, mail-bombers may catch innocent victims in the crossfire. One technique frequently employed by bulk e-mailers is to disguise their online identity, in an effort to foil mail-bombing and avoid flame responses and undeliverable bounce-backs.¹⁶⁴ In some cases, spammers forge the “From” line of their messages by substituting someone else’s e-mail address, or a fictional address at a legitimate domain, for their own. The result is that the unfortunate victim, which may be an innocent Internet service provider (“ISP”), receives the abuse intended for the spammer. If the victim is a business that relies on e-mail to communicate with its customers, or an ISP whose operations are disrupted, vigilantism by mail-bombing can cause significant economic harm.¹⁶⁵ The victims in at least one such situation brought a lawsuit against the spammer seeking to recover their losses.¹⁶⁶

Online vigilantism may have the opposite of the intended effect, spawning new disputes. In one such example, AOL responded to Cyber Promotions’s repeated barrages of junk e-mail by bouncing undeliverable messages back to Cyber

¹⁵⁸See Janet Kornblum, *Death Penalty Lifted Against UUNet*, CNET NEWS.COM (Aug. 6, 1997) <<http://www.news.com/News/Item/0,4,13122,00.html?st.cn.nws.rl.ne>>.

¹⁵⁹See *id.*

¹⁶⁰See Gaffin & Messmer, *supra* note 23, at 1.

¹⁶¹See *id.*

¹⁶²Leslie Miller, *How To Steer Clear of Spammers’ Radar*, USA TODAY, Nov. 5, 1997, at D4 (quoting Ray Everett-Church, an Internet consultant and anti-spam activist).

¹⁶³See *id.*

¹⁶⁴Because bulk e-mailers want recipients of their communications to respond by sending money, they almost always provide some way of getting in touch with them: usually a postal address, Web-site address, telephone number, or fax number.

¹⁶⁵See Paul McNamara, *Four Days in Spam Hell*, NETWORK WORLD, Mar. 30, 1998, at 1 (News section), available in LEXIS, News Library, Papers File; see also Riedman, *supra* note 70, at 68.

¹⁶⁶See *Parker v. C.N. Enters.*, No. 97-06273 (Travis County, Tex. Dist. Ct., injunction entered Nov. 10, 1997); see also *Web Site Operators, ISP Groups Sue Alleged Junk E-Mailer in Texas Court*, 2 Electronic Commerce & L. Rep. (BNA) 587 (June 6, 1997). The court ruled in favor of the plaintiffs, issuing a permanent injunction and awarding damages, attorney’s fees, and costs. See *Texas Court Enjoins Spammer from Sending Bulk E-Mail with Disguised Return Addresses*, 2 Electronic Commerce & L. Rep. (BNA) 1242 (Nov. 26, 1997).

1999]

PROTECTING THE DIGITAL CONSUMER

Promotions's servers, thereby rendering them temporarily unusable.¹⁶⁷ Cyber Promotions countered by hitting AOL with an old-fashioned lawsuit.¹⁶⁸

Online vigilantism may also act as a form of private censorship. For example, one prominent critic of anonymous remailers was targeted with a mail-bombing campaign so disruptive that he discontinued his public statements on the issue.¹⁶⁹

In exceptional circumstances, online communities may devise mechanisms of self-government that incorporate highly evolved applications of due process. A notable example of this occurred in the case of a multi-user dungeon ("MUD")¹⁷⁰ known as LambdaMOO. One participant in the MUD engaged in conduct, described as "sexually explicit verbal rape,"¹⁷¹ that other participants found highly offensive. "After much discussion and consternation, especially with respect to what constituted a proper trial and due process," the MUD participants decided that the offender should be "toaded," or banished from the MUD.¹⁷² The incident prompted the MUD participants to debate at great length "how to handle such aberrant behavior in the future," which was an attempt to apply basic principles of democratic self-governance to the virtual world constituted by the MUD.¹⁷³ The result was establishment of "a system for arbitrating disputes among individuals that provides mutually acceptable judges who may impose a wide range of punishments, including banishment from the system."¹⁷⁴

The LambdaMOO incident illustrates why we should not rely upon the development of self-governance mechanisms to solve the problem of online deceptive marketing practices. First, although LambdaMOO was a relatively small and well-defined community, resolution of this controversy demanded a great deal of time and effort, and engendered considerable controversy. In an online community with participants numbering in the millions, a debate of this sort could go on indefinitely, with no consensus resulting. Second, the "judgment" rendered by the MUD turned out to be unenforceable: the miscreant managed to evade the decree of banishment, rejoining the MUD under a new pseudonym shortly after the

¹⁶⁷ See *Cyber Promotions, Inc. v. America Online, Inc.*, 948 F. Supp. 436, 437 (1996).

¹⁶⁸ See *id.* at 437. AOL prevailed in the action, establishing that Cyber Promotions had no free-speech right to send unsolicited e-mail to America Online's subscribers. See *id.* at 446; see also Pridgen, *supra* note 65, at 254.

¹⁶⁹ See Gaffin & Messmer, *supra* note 23, at 1.

¹⁷⁰ One description of a multi-user dungeon, or "MUD," is as follows:

Communicating from remote locations, members of the MUD utilize shared software and rules of participation to create virtual landscapes, including objects such as gardens or houses with specific properties and location on the landscape. Users also each create characters with particular personalities who inhabit the landscape. On-line participants then may animate the characters in real time. Textual descriptions by each participant flow across the screen of each other participant, providing descriptions of characters and explanations of interactions between characters and character movement through the landscape.

Byassee, *supra* note 265, at 203.

¹⁷¹ Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1662 (1995).

¹⁷² *Id.*

¹⁷³ *Id.* at 1662-63.

¹⁷⁴ Byassee, *supra* note 265, at 218.

toading.¹⁷⁵ We should likewise not be surprised if online swindlers were unmoved by the expressed moral outrage of the online community.

Effective self-governance becomes even less likely as commerce comes to the Net. Money changes everything. Gentle cybercitizens who were willing to limit their prerogatives for the sake of the online community are transformed into *homo economicus*, whose imperative is maximization of profits. As evidenced by the behavior of junk e-mailers, who do not shrink from antagonizing the vast majority of the recipients of their marketing messages as long as the activity brings net profits, mechanisms of online self-governance such as shame and a desire to be part of a community will not alone be effective against a significant sector of online sellers.

5. Summary

The cyberspace utopians' penchant for viewing cyberspace as a "place" that is separate from the sphere of ordinary discourse¹⁷⁶ leads them to frame the question, wrongly, as: "Should the government regulate cyberspace?" Cyberspace is not a place, but rather an obfusatory reference to a means by which people may communicate with each other. The right question is therefore, "What is the appropriate role of government in regulating commercial transactions that are carried out through the use of online communication technologies?" The discussion above is intended to show that the government does have a role to play in this area. The following discussion lays out what I believe are the proper roles for governments and the private sector in controlling deceptive marketing practices in electronic commerce.

VI. LETTING ONLINE COMMERCE GROW

As the above discussion shows, deceptive marketing practices in online commerce threaten to inhibit consumers' confidence in the online medium, and to undercut substantially their willingness to engage in online commercial transactions. On the other hand, an overly aggressive governmental response to online deceptive marketing practices would interfere with the willingness of sellers to make the most effective use of the online medium. To avoid these outcomes, governments must seek solutions that control online deceptive marketing practices while at the same time being sensitive to sellers' need for regulatory transparency.

¹⁷⁵ See Branscomb, *supra* note 309, at 1662 n.103.

¹⁷⁶ Definition of cyberspace as a "place" has had the curious consequence of creating a need for a term that describes everyplace else—a need that did not exist when everything else was all there was. Some cyberpundits refer to what I call the sphere of ordinary discourse as "real space" or the "real world," with "real" highlighting the distinction from the "virtual" world of cyberspace. Others use the term "meatspace," which emphasizes the bits/atoms distinction, and evidences at least a mild distaste for the non-virtual world. For example: "In plain English, the Internet Tax Freedom Act would ban state and local authorities from imposing extra taxes on Internet-based businesses that aren't already imposed on businesses in meatspace." Will Rodger, *Read Their Lips: No Net Taxes*, WIREd, May 1998, at 101, 101.

1999]

PROTECTING THE DIGITAL CONSUMER

A strategy that achieves these goals will include several types of approaches. *First*, governments must improve the transparency of the legal frameworks applying to online commerce, and make adjustments to them as necessary to take account of the special characteristics of the online medium. *Second*, governments, industry participants, and consumer advocates must pursue strategies aimed at enhancing the effectiveness of market-based solutions to the problem of online deceptive marketing practices. *Third*, governments must exercise restraint in attempting to control deceptive marketing practices that originate from outside their territorial boundaries. *Fourth*, governments must improve their ability to cooperate internationally, so as to overcome the legal and practical obstacles to law enforcement in the context of cross-border deceptive marketing practices.

The remainder of this Article recommends a set of strategies that follows this approach.

*A. Improving the Transparency of the Legal Framework, and
Adapting It to the Online Environment*

1. General Rule of Parity

Governments should make clear to market participants that, except where the special characteristics of the online medium require otherwise, existing law protecting consumers from deceptive marketing practices is fully applicable to commercial conduct that is conducted via online communications.

Deceptive marketing practices result in the same consumer injury regardless of the means of communication that are used in perpetrating them. The existence of market failures likewise does not depend on the mode of communication. Accordingly, the legal regimes that have been developed to control deceptive marketing practices carried out via print, broadcast, or telephonic media should, generally speaking, be equally applicable to deceptive online conduct.

This principle follows logically from the notion, embodied in the UNCITRAL Model Law on Electronic Commerce and elsewhere,¹⁷⁷ that a communication should not be denied legal effect solely on the ground that it is generated or transmitted through electronic means. If the legal effect of a commercial communication is unaffected by the medium through which it is made, then the rules prohibiting deceptive marketing practices should apply equally regardless of the medium through which such practices are communicated.¹⁷⁸

¹⁷⁷UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE art. 5 (1996) (“Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.”); see Government Paperwork Elimination Act, S. 2107, 105th Cong., 2d Sess. § 10 (1998) (“Because there is no meaningful difference between contracts executed in the digital world and contracts executed in the analog world, it is the sense of the Congress that such contracts should be treated similarly under [federal and] state law.”); Uniform Electronic Transactions Act § 106(a) (draft Jan. 29, 1999) (“A record or signature may not be denied legal effect solely because it is in electronic form.”).

¹⁷⁸This principle also appears, for example, in the U.S.-Japan Joint Statement on Electronic Commerce, 34 WEEKLY COMP. PRES. DOC. 884, 886 (May 15, 1998) (“Electronic

In order to promote regulatory transparency, governments should make it widely known to market participants, through issuance of policy statements or by other means, that they will enforce existing deceptive marketing practices laws in the online context.

This rule of parity must be qualified. The online medium exhibits certain novel characteristics that make it unclear in some instances how the existing rules of law should be applied. The discussion that follows addresses some of these instances.

2. Reasoning from Analogy with Other Means of Communication

In instances where the application of an existing rule of law to online commercial conduct is unclear, analysis should proceed by analogy with the application of the rule to similar conduct occurring via whichever other means of communication presents, under the circumstances, the closest analogy to the online medium.

The online medium presents several aspects, which may be most closely analogous to various other communications media, depending on the context. For example, e-mail resembles postal mail as a point-to-point method of communication with message initiation in the hands of the sender. However, in a context where matters turn on the sender's knowledge of the location of the recipient at the time the message is received—as, for example, when evaluating whether the message had foreseeable effects in a foreign jurisdiction—the analogy to postal mail breaks down. When e-mail is sent using an open Internet mailing list, it may more closely resemble broadcast media, as a one-to-many form of communication that is made available for reception by a broad audience at the recipients' discretion. Newsgroup postings may be found analogous to print communications (static text), and chat sessions analogous to telephone conversations (real-time exchanges). A Web site may be viewed as analogous to “a national toll-free number with a recorded message”¹⁷⁹ or “an advertisement in a national magazine.”¹⁸⁰ Where a useful analogy is found, rules of law should be interpreted in the online context analogously to the way in which they have been applied to another medium.¹⁸¹

commerce should afford consumers the same level of protection as is provided in other forms of commerce.”).

¹⁷⁹Robert W. Hamilton & Gregory A. Castanias, *Tangled Web: Personal Jurisdiction and the Internet*, LITIG., Winter 1998, at 27, 29.

¹⁸⁰Hearst Corp. v. Goldberger, 96 Civ. 3620 (PKL) (AJP), 1997 U.S. Dist. LEXIS 2065, at *31 (S.D.N.Y. Feb. 26, 1997).

¹⁸¹See Edward V. Di Lello, *Functional Equivalency and Its Application to Freedom of Speech on Computer Bulletin Boards*, 26 COLUM. J.L. & SOC. PROBS. 199, 212 (1993) (describing “functional equivalency” as a mode of analysis). The “functional equivalency” approach may also be used to develop legislative rules in response to new technology. The drafters of the UNCITRAL Model Law on Electronic Commerce explain that, in developing rules to govern the legal status of data messages, they followed the “‘functional equivalent approach,’ which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.” *Guide to Enactment of the*

1999]

PROTECTING THE DIGITAL CONSUMER

For example, ascertaining the location of an online event presents many of the same issues that arise in determining the location of an event that occurs in the course of or by virtue of a telephone conversation. The place of contracting of a contract may be relevant to a determination of which court has jurisdiction to resolve a dispute, or which country's substantive law is applicable to the dispute. Authorities have arrived at (differing) rules for determining the place of contracting of a contract that is concluded by telephone.¹⁸² The rule that a particular jurisdiction has applied in the context of telephonic communications may well be applicable in the online context.

This mode of analysis has been employed historically with the development of new communications technologies—"[t]he telegraph was analogized to railroads, the telephone to the telegraph, and cable television to broadcasting"¹⁸³—but it must be used with care lest it obscure rather than enlighten analysis.

3. Clarification and Updating of Regulatory Regimes

Regulatory authorities should clarify how the existing deceptive marketing practices legal framework will be applied to online transactions, and should update the legal framework as necessary to take account of special characteristics of the online medium.

Adaptation of disclosure and other requirements to the online context raises a variety of policy issues, as discussed above.¹⁸⁴ Government agencies may find it useful to publish policy statements clarifying how disclosure and other legal requirements apply in the online context.

4. Educating Online Entrepreneurs

Governments and relevant private entities, such as trade associations, should direct resources towards educating new online entrepreneurs as to the legal framework applicable to their trade practices.

Because the barriers to entry are so low, many sellers are setting up businesses for the first time online. Many of these new entrepreneurs are not well acquainted with the legal rules applying to their activities. Because these sellers will in many cases fail to seek out such information, governments and relevant private parties, such as trade associations, should devise imaginative proactive approaches. For example, law enforcement agencies can monitor the Web, newsgroup postings, and unsolicited commercial e-mail; identify online sellers that appear to be

UNCITRAL Model Law on Electronic Commerce ¶ 16 (visited Feb. 11, 1999)

<<http://www.un.or.at/unictral/en-index.htm>>.

¹⁸² Compare *Linn v. Employers Reinsurance Corp.*, 139 A.2d 638, 640 (Pa. 1958) (“[A]n acceptance by telephone is effective, and a contract is created at the place where the acceptor speaks.”), with *Entores, Ltd. v. Miles Far East Corp.*, 2 Q.B. 327, 334 (Eng. C.A. 1955) (“[T]he contract will be completed when the acceptance is received.”). See also 2 SAMUEL WILLISTON, A TREATISE ON THE LAW OF CONTRACTS § 6:61 (4th ed. 1990).

¹⁸³ ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 7 (1983).

¹⁸⁴ See *supra* text accompanying notes 194-98.

engaging in deceptive marketing practices; and send informational messages to those sellers. Agencies can also attempt to reach online entrepreneurs by sending representatives to address them at gatherings of industry participants, and organizing educational workshops. Trade associations should find it in their members' interests to take the lead in educating industry participants, both to forestall government regulation and to reduce the incidence of unfair competition.

5. Negotiating an International Baseline Consumer Protection Regime

Governments should enter into multilateral conventions establishing a baseline consumer protection regime applicable to online and other cross-border commercial conduct.

Many of the issues that arise from cross-border disputes are exacerbated by the fact that deceptive marketing practices laws vary from one jurisdiction to the next. Because of varying legal systems and cultural assumptions, it would be neither possible nor desirable to erect a comprehensive, universal legal regime regulating marketing practices. However, following the approach of several directives of the European Commission,¹⁸⁵ it may be feasible and useful to establish a baseline regime of consumer protection applicable to cross-border transactions to which all or nearly all countries can subscribe.

6. Protecting Online Privacy

In adapting trade practices laws to the online context, and in encouraging private parties to devise methods to protect consumers from online deceptive marketing practices, governments should pay due regard to consumer privacy concerns.

The online medium lends itself to intrusions on the privacy interests of individuals who engage in electronic commerce. Computerized data management and online accessibility add a new dimension to the problem of controlling personally identifiable information.¹⁸⁶ Online sellers may collect information from Web-site visitors without the visitor's knowledge. Personal transactional information may be correlated with other data to generate individual profiles. Personal information that is in digital form may be easily transferred to other commercial entities with which the data subject has no relationship. If inaccurate information becomes associated with an individual, it may be difficult for the

¹⁸⁵See, e.g., Council Directive of 10 September 1984 Concerning Misleading and Comparative Advertising, 1984 O.J. (L 250) 17, as amended by 1997 O.J. (L 290) 18, corrected at 1998 O.J. (L 194) 54; Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144) 19.

¹⁸⁶"The difference between the costly and time-consuming search once required and the easy and inexpensive retrieval of information now possible can be viewed as a difference in kind, not just degree." FEDERAL TRADE COMM'N, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS 3 (Dec. 1997).

1999]

PROTECTING THE DIGITAL CONSUMER

individual to detect and correct. Governments must take heed of these factors in their efforts to control online deceptive marketing practices.¹⁸⁷

B. Enhancing the Effectiveness of Market-Based Solutions to the Problem of Online Deceptive Marketing Practices

1. Facilitating Consumer Sovereignty

Governments, in partnership with business and consumer representatives, should facilitate the operation of consumer sovereignty in the context of online commerce, through means including:

- a. devoting resources to consumer education, making use of novel methods made possible by the online medium in combination with traditional methods;*
- b. assuring that disclosure requirements are applied to online marketing practices in a manner that best promotes the ability of consumers to make informed decisions in the marketplace;*
- c. assisting in the vindication of contract rights by bringing targeted enforcement actions; and*
- d. supporting development of technological means, such as digital signatures, to assist consumers and enforcement authorities in identifying sellers.*

The online medium provides vehicles for educating consumers that do not exist in any other media. One innovative approach involves the use of “teaser sites” on the Web, designed so as to draw consumers’ attention and to deliver an educational message. The home page of a teaser site proposes an offer that seems too good to be true, such as a get-rich-quick scheme, diet program, or discount vacation plan. As the user clicks through to subsequent pages, he may view even more outrageous claims or testimonials, and is invited to become a participant by sending money. The final page reveals that the site was constructed by a government agency for the purpose of demonstrating to consumers how easy it is to fall for scams, and directs the user to sources of further information about how to avoid becoming a victim.¹⁸⁸ Governments should also make use of tried-and-true approaches to educating consumers about how to protect themselves from

¹⁸⁷For discussions of online privacy issues, see ANDRÉ BACARD, *THE COMPUTER PRIVACY HANDBOOK* (1995); Joel R. Reidenberg & Françoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105 (1995); Heather Green et al., *A Little Privacy, Please*, BUS. WK., Mar. 16, 1998, at 98; National Info. Infrastructure Task Force, *Options for Promoting Privacy on the National Information Infrastructure (April 1997)* (visited Apr. 14, 1999)

<<http://www.iitf.nist.gov/ipc/privacy.htm>> (presenting a Draft for Public Comment). For a skeptical approach to privacy issues, see Solveig Singleton, *Privacy as Censorship*, CATO POL’Y ANALYSIS, No. 295, Jan. 22, 1998.

¹⁸⁸See Ted Bridis, *FTC’s On-Line Ruse Warns of Rip-Off Ads*, WASH. TIMES, June 26, 1998, at B12. One example of such a teaser site appears at *The Ultimate Prosperity Page* (visited Apr. 14, 1999) <<http://www.ari.net/prosper>>.

online deceptive marketing practices. Consumers who are skeptical of offers that seem too good to be true are the best defense against deceptive marketing practices.

Government agencies can make better use of resources devoted to consumer education by forming partnerships with industry participants, such as trade associations, and consumer groups. Legitimate companies have an interest in educating consumers to prefer their offerings over those proposed by less scrupulous traders.

Existing disclosure requirements should be applied to online marketing practices with a view to ensuring that they serve their intended purpose. For example, a disclosure that is placed on a Web site in such a way that site visitors may easily overlook it is not of much value.¹⁸⁹

By bringing law enforcement actions against sellers who engage in a pattern of violations of deceptive marketing practices laws, governments can help to hold sellers to the bargains they have struck with consumers.

One of the obstacles to controlling deceptive conduct in online transactions is the difficulty in identifying sellers who are located at a distance, and possibly in another country. Digital signatures may offer a means of securely identifying sellers located at a distance.¹⁹⁰ Governments may have a role to play in establishing a legal regime supporting a public key infrastructure.¹⁹¹

2. Industry Self-Regulation

Industry participants should implement various types of self-regulation aimed at controlling online deceptive marketing practices, such as:

- a. mandatory codes of conduct applicable to online commercial activities;*
- b. refusal by legitimate businesses to lend support to illegal conduct;*
- c. third-party certification systems; and*
- d. complaint centralization systems.*

Industry participants should take the lead in devising self-regulatory solutions to consumer protection problems arising from electronic commerce, through both formal and informal channels. Governments have an important role to play in encouraging and cajoling the private sector in this endeavor. There is nothing like the threat of government regulation to spur an industry into self-regulation.

Codes of conduct are most effective when adherence is mandatory, and meaningful penalties are imposed on those who fail to comply. The trade association that creates or sponsors a code may enforce compliance by expelling violators from its membership—a sanction that may be more or less effective,

¹⁸⁹See *FTC v. Audiotex Connection, Inc.*, CV-97-0726 (E.D.N.Y. order entered Nov. 13, 1997) (requiring disclosures in interactive media to be made in a way that is “unavoidable” by the viewer).

¹⁹⁰See R. Christian Bruce, *Regulators Clear National Bank’s Bid To Identify Parties in Electronic Commerce*, 3 *Electronic Commerce & L. Rep.* (BNA) 55, 55 (Jan. 21, 1998).

¹⁹¹On the role of governments in encouraging the development of technological solutions to online governance issues, see Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 *TEX. L. REV.* 553, 586-91 (1998).

1999]

PROTECTING THE DIGITAL CONSUMER

depending on the perceived benefits of membership.¹⁹² Regulatory authorities may also institute enforcement actions grounded on the violator's deceptive representation that it would comply with the code.¹⁹³

Businesses may regulate their own conduct without reference to a particular code. Those businesses that provide services that are crucial for the operation of a deceptive marketing scheme should take care not to lend their support to such schemes. ISPs, operators of payment services, owners of online malls, and advertising agencies are examples of businesses that can choose not to facilitate deceptive marketing practices.¹⁹⁴ Failure to exercise such restraint may in some cases lead to liability as an aider or abettor.¹⁹⁵

Third-party certification systems enable a seller that is adhering to a high standard of conduct to obtain "credit" for its conduct in the marketplace. If a certification system becomes widely recognized, the absence of certification has a stigmatizing effect, which encourages sellers to raise their standards in order to qualify for the certification. Regulatory supervision of third-party certification authorities may become necessary in cases of abuse.

¹⁹²The threat of expulsion is the ultimate mechanism of compliance where membership in a trade association is a prerequisite to the right to pursue a trade. This is the case with self-regulation of securities dealers in the United States through the National Association of Securities Dealers ("NASD"), as "[a]ny securities broker/dealer that wishes to do business with the public must become a member of the NASD, and register all branch offices as well." NATIONAL ASS'N OF SEC. DEALERS, INC., *SECURITIES REGULATION IN THE UNITED STATES* 27 (3d ed. 1996), available at <http://www.nasd.com/pr_section7.html>. However, the extreme prejudice resulting from expulsion may make it unlikely that the trade association will resort to that penalty in any but the most extreme cases of non-compliance.

¹⁹³See FEDERAL TRADE COMM'N, *supra* note 324, at 29 & n.297; *In re GeoCities*, No. C-3849, 1999 F.T.C. LEXIS 17 (Feb. 5, 1999).

¹⁹⁴See Stacy Lu, *World Medical Community Frets over Unregulated Medicine Sales on Web*, N.Y. TIMES, Mar. 23, 1998, at D1 (discussing an Internet service provider located in the United States which removed advertisements for do-it-yourself abortion and sterilization kits posted by a customer in Colombia on request of the Food and Drug Administration, on grounds that by violating U.S. law the customer violated its terms-of-service agreement).

¹⁹⁵See *In re Kent & Spiegel Direct, Inc.*, No. C-3769, 1997 F.T.C. Lexis 304 (F.T.C. Sept. 16, 1997) (holding infomercial producer liable for deceptive weight loss claims); *In re Grey Adver., Inc.*, 122 F.T.C. 343 (1996) (holding advertising agency liable for deceptive claims and demonstrations in advertisements); *In re Sharper Image Corp.*, 116 F.T.C. 606 (1993) (holding catalogue seller liable for unsubstantiated claims about products offered in catalogue); Telemarketing Sales Rule, 16 C.F.R. § 310.3(b) (1998) ("It is . . . a violation of this Rule for a person to provide substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any act or practice that violates . . . this Rule.").

Where sales are made at a distance, it may be difficult for the purchaser to evaluate the seller's reputation. This difficulty may be reduced if consumers have easy access to a system that collects and centralizes consumer complaints about sellers. Such a system will be most effective if it is accessible via an open network (such as the Internet), at no cost to the consumer. An acceptable system must include appropriate safeguards of the privacy interests of consumer complainants, as well as mechanisms to prevent sellers from being unfairly stigmatized by spurious complaints.

3. Adapting Existing Alternative Dispute Resolution Mechanisms

Governments and industry participants should adapt existing alternative dispute resolution mechanisms as necessary to make them available for resolving disputes between sellers and consumers that arise in online commerce, and should encourage international cooperation among these bodies.

Many countries have small claims courts, consumer complaint boards, and other alternative dispute mechanisms designed for resolving disputes involving relatively small losses. The rules and procedures governing the functioning of these bodies may need to be updated to make them available, both technically and practically, for resolving online disputes.

4. Developing New Alternative Dispute Resolution Mechanisms

Industry participants should develop alternative methods of resolving disputes between sellers and consumers that arise in online commerce, as well as mechanisms through which consumers may obtain redress for losses due to online deceptive marketing practices. For example:

- a. credit card associations should establish a comprehensive international chargeback regime;*
- b. operators of online shopping malls, and other industry participants that act as intermediaries between retailers and consumers, should guarantee that consumers are satisfied with their purchases; and*
- c. online sellers should participate in online arbitration and mediation systems.*

Industry participants that control access to necessary components of online commerce are well placed to devise regimes through which consumers can obtain redress for losses resulting from deceptive marketing practices, without the need for government intervention. Enlightened industry participants will be willing to bear the costs this entails, recognizing that they will themselves be among the prime beneficiaries: as consumer confidence in the online medium increases, so will online purchases. Just as the owner of a bricks-and-mortar shopping mall finds it advantageous to spend money for security guards in order to create surroundings that consumers will find safe and comfortable, the owner of an online mall may find that the benefits of absorbing the losses resulting from deceptive marketing

1999]

PROTECTING THE DIGITAL CONSUMER

practices by its tenants outweigh the costs. Furthermore, industry participants that provide online businesses with a means of getting their offerings before prospective purchasers may be in a position to require the sellers to indemnify them for the costs of guaranteeing that consumers are satisfied with their transactions. This serves a cost-spreading function.

Some countries require credit card associations to operate a billing dispute or chargeback regime for domestic transactions, and some card associations have voluntarily extended their domestic regime to cover international transactions. The establishment of a comprehensive international chargeback regime will greatly enhance consumers' willingness to enter into online transactions with distant sellers, and will provide consumers with an avenue of redress. A chargeback regime may also have the effect of shifting the losses resulting from deceptive marketing practices onto the lowest-cost avoider of those losses. When a consumer disputes a credit card charge through a chargeback procedure, the cost is often borne by the acquirer, who maintains the seller's merchant account and thereby allows the seller access to the credit card system. The threat of incurring these costs encourages acquirers to exercise discretion in taking on merchants, refusing to deal with sellers thought to be at high risk of generating chargebacks.

Online arbitration and mediation systems will be most effective if they are easily accessible to consumers, operate transparently, and require no payment from consumers. Several third-party online arbitration and mediation systems have been set up. The best known of these, the Virtual Magistrate, offers "arbitration for rapid, interim resolution of disputes involving (1) users of online systems, (2) those who claim to be harmed by wrongful messages, postings, or files and (3) system operators."¹⁹⁶ The Online Ombuds Office offers online mediation services.¹⁹⁷ The Cyber Tribunal is an experimental French- and English-language online arbitration/mediation service operated by the University of Montreal.¹⁹⁸ Arbitral awards that are rendered online might be enforceable under existing law.¹⁹⁹

¹⁹⁶The Virtual Magistrate Project, *Concept Paper (July 24, 1996)* (visited Apr. 14, 1999) <<http://vmag.vcilp.org/docs/vmpaper.html>>. The Virtual Magistrate is operated by a partnership composed of the Center for Information Law and Policy, the American Arbitration Association, the National Center for Automated Information Research, and the Cyberspace Law Institute. See The Virtual Magistrate Project, *Welcome* (last modified May 21, 1996) <<http://vmag.vcilp.org>>. Apparently only a single case has been decided since the inception of the project in March 1996. See The Virtual Magistrate, *Decided Cases* (last modified May 21, 1996) <<http://vmag.vcilp.org/cases/decided.html>>.

¹⁹⁷See Center for Info. Tech. and Dispute Resolution, *Online Ombuds Office* (visited Apr. 14, 1999) <<http://aaron.sbs.umass.edu/center/ombuds/default.htm>>. The Online Ombuds Office is operated by the Center for Information Technology and Dispute Resolution at the University of Massachusetts. It was established in June 1996. A transcript of the first online mediation it conducted is available. See *id.*

¹⁹⁸See Cyber Tribunal, *Cyber Conflict Resolution Centre* (visited Mar. 24, 1999) <<http://www.cybertribunal.org/english/defaulteng.htm>>.

¹⁹⁹Signatories to the New York Convention agree to enforce arbitral awards rendered within the territory of other signatory nations. See Convention on the Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 38. However, some aspects of the Convention, such as those concerning writing requirements and geographical limitations, might need to be modified for it to apply to online arbitrations.

Governments continue to have a role to play even in the context of robust alternative dispute resolution systems, since such systems may not thrive in an atmosphere deprived of the threat of state-imposed sanctions.²⁰⁰

C. Restraint in Extraterritorial Assertions of Jurisdiction

In their efforts to reach deceptive marketing practices that originate from outside their territorial jurisdiction, governments must take account of the geographic indeterminacy of online communications and the overlapping jurisdiction of a multiplicity of government agencies. Unlike the case with most other forms of commercial communication, online sellers face technological constraints that prevent them from limiting the geographic scope within which their communications may be accessed, and from knowing the geographic location of an online interlocutor. Rules of jurisdiction (both prescriptive and adjudicative), and choice-of-law rules, must be updated to reflect this characteristic of online communication. Updated rules of jurisdiction should effectuate the following principles.²⁰¹

1. Limiting What Is Deemed to Constitute Foreseeable Extraterritorial Effects

A seller who transmits a commercial communication that is accessible by residents of a particular state should not be deemed to have caused foreseeable effects within that state solely by virtue of that communication, if the communication was transmitted via a medium that, by its very nature, prevents the maker of a communication from restricting the geographic area in which it may be received, or from ascertaining the geographic location of one's interlocutor.

This principle allows a seller to make use of the various modes of online communication without risking being held subject to the jurisdiction of every state in the world. The rules of jurisdiction should enable an online seller to make a conscious decision to do business in certain countries, thereby potentially subjecting himself to the jurisdiction of the courts of those countries, and of substantive rules prescribed by legislatures in those countries, while refraining from doing business in other countries, thereby avoiding the risk of assertion of jurisdiction by courts and legislatures in those countries.²⁰² Application of this

See Frank A. Cona, *Application of Online Systems in Alternative Dispute Resolution*, 45 BUFF. L. REV. 975, 993 (1997). From a more utopian standpoint, the sanction imposed by a "virtual court" could consist of "the usual private association sanction of expulsion or suspension from the relevant part of cyberspace." Hardy, *supra* note 76, at 1053.

²⁰⁰Since "some disputes can be resolved voluntarily only because of the possibility of judicial remedies," the effectiveness of private dispute resolution systems "may depend largely on the practical availability of more conventional courts as a last resort." Henry H. Perritt, Jr., *Jurisdiction in Cyberspace: The Role of Intermediaries*, in BORDERS IN CYBERSPACE, *supra* note 152, at 164, 164.

²⁰¹This section expands on the argument in Rothchild, *supra* note 146, at 300-01.

²⁰²In the online context, courts have found a defendant's efforts to avoid having contacts with a particular place, and the absence of such efforts, relevant factors in jurisdictional

1999]

PROTECTING THE DIGITAL CONSUMER

guideline domestically in the context of a federal legal system, such as that of the United States, would likewise allow a seller to limit his exposure to the assertion of jurisdiction by particular sub-jurisdictions of the federal system.

Thus, for example, the following activities should not, by themselves, support a finding that the maker of a communication caused foreseeable effects within a state: (1) maintaining a World Wide Web site that is accessible by residents of that state;²⁰³ (2) posting a message in a Usenet newsgroup, or on any other electronic

analysis. In *Hasbro, Inc. v. Clue Computing Inc.*, 45 U.S.P.Q.2d (BNA) 1170, 1178 (D. Mass. 1997), the court found a sufficient basis for asserting in personam jurisdiction, noting that the defendant had “taken no measures to avoid contacts in the forum state.” Conversely, in *Smith v. Hobby Lobby Stores, Inc.*, 968 F. Supp. 1356, 1365 (W.D. Ark. 1997), the court held that the fact that a defendant “did not contract to sell any goods or services to any citizens of [the forum state] over the Internet site” was grounds for finding insufficient contacts with the forum to support jurisdiction. *Id.*

²⁰³This rule is consistent with the holdings of nearly all U.S. courts that have considered the issue. See *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414 (9th Cir. 1997); *Bensusan Restaurant Corp. v. King*, 126 F.3d 25 (2d Cir. 1997); *Blackburn v. Walker Oriental Rug Galleries, Inc.*, 999 F. Supp. 636 (E.D. Pa. 1998); *SF Hotel Co. v. Energy Invs., Inc.*, 985 F. Supp. 1032 (D. Kan. 1997); *Weber v. Jolly Hotels*, 977 F. Supp. 327 (D.N.J. 1997); *IDS Life Ins. Co. v. SunAmerica, Inc.*, 958 F. Supp. 1258 (N.D. Ill. 1997), *aff’d in part and rev’d in part*, 136 F.3d 537 (7th Cir. 1998); *Hearst Corp. v. Goldberger*, 96 Civ. 3620 (PKL) (AJP), 1997 U.S. Dist. LEXIS 2065 (S.D.N.Y. Feb. 26, 1997); *Agar Corp. v. Multi-Fluid, Inc.*, No. 95-5105, 1997 U.S. Dist. LEXIS 17121 (S.D. Tex. June 25, 1997); *Transcraft Corp. v. Doonan Trailer Corp.*, 45 U.S.P.Q.2d (BNA) 1097 (N.D. Ill. 1997); *McDonough v. Fallon McElligott, Inc.*, 40 U.S.P.Q.2d (BNA) 1826 (S.D. Cal. 1996). *But see* *Telco Communications v. An Apple a Day*, 977 F. Supp. 404 (E.D. Va. 1997) (holding that the defendant’s maintenance of a Web-site advertisement constituted the regular solicitation of business and a persistent course of conduct in the forum state, for purposes of a state long-arm statute); *Inset Sys., Inc. v. Instruction Set, Inc.*, 937 F. Supp. 161 (D. Conn. 1996) (holding that the maintenance of a Web site displaying a toll-free telephone number constitutes the purposeful doing of business in any state whose residents may access the Web site, for purposes of a state long-arm statute).

Courts that have found personal jurisdiction based on the maintenance of a Web site have usually relied upon additional factors tending to a finding that the defendant purposely availed itself of the privilege of doing business within the forum state, such as the fact that defendant intentionally interfered with the business of a company that he knew was located in the forum state, *see Panavision Int’l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998); that the defendant made sales in the forum state, maintained a toll-free number, received significant income from the forum state, and advertised both on its Web page and via other nationally circulated media, *see Rubbercraft Corp. v. Rubbercraft, Inc.*, No. CV 97-4070-WDK, 1997 WL 835442 (C.D. Cal. Dec. 17, 1997); that the defendant made sales to a retailer in the forum state, *see Gary Scott Int’l, Inc. v. Baroudi*, 981 F. Supp. 714 (D. Mass. 1997); that the residents of the forum state engaged in commercial transactions with the defendant after visiting the defendant’s Web site, *see Superguide Corp. v. Kegan*, 987 F. Supp. 481 (W.D.N.C. 1997); that a license agreement called for the application of the law of the forum state, *see Digital Equip. Corp. v. AltaVista Tech., Inc.*, 960 F. Supp. 456 (D. Mass. 1997); that the defendant had 3,000 paid subscribers in the forum state, *see Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997); that the defendant sent defamatory e-mails to the plaintiff’s customers, *see EDIAS Software Int’l, L.L.C. v. Basis Int’l*, 947 F. Supp. 413 (D. Ariz. 1996); that Web-site contacts resulted in the defendant’s sending advertisements by e-mail into the forum state, *see Maritz, Inc. v. CyberGold, Inc.*, 947 F. Supp. 1328 (E.D. Mo. 1996); that the defendant placed an advertisement in a newspaper circulated in the forum state, *see Heroes, Inc. v. Heroes*

bulletin board system, that is accessible by residents of that state;²⁰⁴ (3) transmitting a message to an Internet mailing list whose membership includes residents of that state;²⁰⁵ or (4) making a statement in a chat session that includes a participant who is a resident of that state.

To support extraterritorial jurisdiction in the online context, there must be “[a]dditional conduct”²⁰⁶ beyond merely making a communication available within a particular state. Sufficient additional conduct will exist where: (1) the online communication results²⁰⁷ in a commercial transaction involving the shipment of a physical good to an address located in the state that asserts jurisdiction; (2) the communication results in a commercial transaction involving the transmission of a digital good²⁰⁸ to a recipient who resides in that state, if at the time the transaction was consummated the sender knew or reasonably should have known that the purchaser resided in that state; (3) the person made affirmative and unmistakable

Found., 41 U.S.P.Q.2d (BNA) 1513 (D.D.C. 1996); and that the Web site placed a resident of the forum state on its mailing list, *see* *Minnesota v. Granite Gate Resorts, Inc.*, 568 N.W.2d 715 (Minn. Ct. App. 1997), *aff’d*, 576 N.W.2d 747 (Minn. 1998). In *Hasbro, Inc. v. Clue Computing Inc.*, 45 U.S.P.Q.2d (BNA) 1170 (D. Mass. 1997), the court attempted, albeit unconvincingly, to demonstrate that the defendant had purposely directed its solicitations to Massachusetts, by virtue of having noted on its Web site that it had performed services for a large and well-known company located in Massachusetts.

²⁰⁴*See* *Mallinckrodt Med., Inc. v. Sonus Pharm., Inc.*, 989 F. Supp. 265, 272 (D.D.C. 1998) (stating that a posting on an electronic bulletin board “is not an act purposefully or foreseeably aimed” at all states in which it may be accessed, and therefore does not support personal jurisdiction over a message poster).

²⁰⁵*See* *Perritt*, *supra* note 338, at 170 (arguing that one who posts a message to an Internet mailing list “usually has no knowledge of the extent of the list and thus the dissemination of his posting to a particular person is usually neither purposeful nor foreseeable”).

²⁰⁶*Asahi Metal Indus. Co. v. Superior Court*, 480 U.S. 102, 112 (1987). The Court described several types of conduct that may support a finding that a defendant purposely directed his activities towards a particular jurisdiction: “designing the product for the market in the forum State, advertising in the forum State, establishing channels for providing regular advice to customers in the forum State, or marketing the product through a distributor who has agreed to serve as the sales agent in the forum State.” *Id.*

²⁰⁷It is a factual question whether a particular communication “results” in a transaction. Sometimes it will be obvious, as when the consumer responds to an e-mail solicitation by ordering the product advertised in a return e-mail, or responds to a Web-site solicitation through a form contained on the site. A more difficult issue may be presented where the seller advertises both online and through other means, and where orders are placed through a postal address or telephone number that is publicized in various media.

²⁰⁸In transactions involving digital goods—that is, goods consisting of a stream of bits (such as software, information, graphic images, or multimedia material) that is delivered via a computer network—additional difficulties are introduced, since the goods are shipped to a virtual address rather than a physical one. If the purchaser pays for the order by transmitting a credit card number online or by telephone, or with digital cash, the seller will not necessarily know the location of the purchaser, either at the time the purchaser places the order or at the time the purchaser takes “delivery” of the transmitted good. The proposed rule makes jurisdiction appropriate in the purchaser’s place of residence if the seller knew or should have known the place of residence. The jurisdictional determination should not turn on the recipient’s *location* at the time she receives the digital goods, which is entirely outside the seller’s control and knowledge, but rather on the seller’s knowledge of the recipient’s state of *residence*, which is a less transient attribute.

1999]

PROTECTING THE DIGITAL CONSUMER

efforts to direct the communication or transmission to residents of that state,²⁰⁹ or to injure a person located in that state;²¹⁰ or (4) the person knew, or reasonably should have known, that the transaction would have effects within that state.²¹¹ Conversely, assertion of extraterritorial jurisdiction will be less appropriate where the seller takes steps to *avoid* doing business by residents of a particular country, such as by posting a notice indicating the geographic or political limits within which the offer is intended to be valid,²¹² declining to ship goods into particular jurisdictions,²¹³ or making efforts to ascertain the location of a prospective customer and limiting one's commercial activity accordingly.²¹⁴

²⁰⁹Sufficient indicia of an intention by the maker of the communication to solicit residents of the recipient country might include: making the communication in a language that is understood almost exclusively by residents of the recipient country; advertising within the recipient country through other, more targeted, media; offering a means of responding to the solicitation by domestic communications (such as a local telephone number or mailing address) within the recipient country; or touting benefits that would be of value only to residents of the recipient country.

For example, if a Web site is worded in Swedish, and has not demonstrably resulted in any transactions, the owner of the site may still be subject to jurisdiction of the courts of Sweden, on the ground that the site is purposely directed to residents of Sweden. Whether jurisdiction would lie in the courts of Finland, where a substantial proportion of the population understands Swedish, is a difficult question. The Web site would not subject the owner to jurisdiction in the United States, despite the fact that a substantial number of U.S. residents, constituting a very small proportion of the population, understand Swedish.

As another example, a Web site "that emphasize[s] the investor's ability to avoid U.S. income taxes on the investments" would be deemed to be directed at residents of the United States. Statement of the Commission, *supra* note 154, at 14,808.

²¹⁰See *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998) (holding that defendant intended to interfere with business of company known to be located in forum state). The *locus classicus* of this idea is *Calder v. Jones*, 465 U.S. 783 (1984).

²¹¹Actual knowledge was the basis for the holding in *United States v. Thomas*, 74 F.3d 701 (6th Cir. 1996), that the defendants who operated an adult-oriented electronic bulletin board system from their home in California could be convicted of violating federal obscenity laws based on community standards prevailing in Tennessee. In that case, a Postal Inspector in Tennessee applied for and became a member of the bulletin board system, and then obtained sexually explicit materials from the system. In applying for membership, the Postal Inspector provided his telephone number in Tennessee, and received a call at that number from the defendant. The Postal Inspector also ordered sexually explicit videotapes, which the defendant delivered to his Tennessee address by postal mail.

²¹²In a deceptive trade practices lawsuit against defendants offering gambling via a Web site, the state of Minnesota sought an injunction "directing [the defendants] either to stop sending their advertisements to Minnesota computer users or to post in their advertisements that their services are illegal in Minnesota." See Respondent's Brief and Appendix, *Minnesota v. Granite Gate Resorts, Inc.*, 576 N.W.2d 747 (Minn. 1998) (No. C6-97-89), available at <<http://www.ag.state.mn.us/consumer/news/OnlineScams/gg0111156.html>>.

²¹³See Lu, *supra* note 332, at D1 (describing a Dutch seller of marijuana seeds and hallucinogenic mushrooms who prudently avoids shipping them to U.S. addresses).

²¹⁴See Statement of the Commission, *supra* note 154, at 14,807-09 (discussing circumstances under which the SEC will consider an offshore Web-site offer as targeted at residents of the United States).

2. Focus on Location of People, Not of Computers

Jurisdiction should not depend on the physical location of the various computers that enable online communications, or the location of the owners of those computers, but rather on the location of the parties to online communications.

An online communication may involve a large number of computers, located in a multiplicity of jurisdictions that bear little or no connection to the parties to a transaction involving the communication. For example, the computer on which the files constituting a World Wide Web site are hosted may be located anywhere in the world. Using file transfer protocol and e-mail, the site owner is able to maintain the site with equal ease regardless of his geographic separation from the host computer. Several computers may be involved in gaining access to the Internet or some other computer network. One of those computers is likely to be located in immediate proximity to the user, but others may not: a user may obtain access through a telephone connection to a computer located in another jurisdiction, or via a telnet session involving a distant computer. When data is sent across a computer network using packet-switching technology, any number of computers may store and forward a transmission on its course from the sender to the recipient. A commercial transaction may call for a purchaser to download information from a computer in some remote location.²¹⁵ In a distributed system such as Usenet, newsgroup postings may be stored on computers located in places unconnected to either the poster or reader of a message.

The location of any of these computers should be accorded little or no weight in determining whether a state in which it is located may assert jurisdiction over a person who makes some use of the computer in an online communication. The contrary position, applied to other media of communication, would have absurd results: for example, it would imply that conduct occurring in the course of an international telephone conversation should give rise to jurisdiction in every country through which the communication is switched, or that a print solicitation sent via air mail should be subject to the jurisdiction of every place where the transport plane touches down to refuel.²¹⁶

The same is true for the location of the owners of computers that enable online communications. Thus, a resident of Italy who obtains access to the Internet through CompuServe should not be subject to the jurisdiction of the courts of the United States merely by virtue of the fact that CompuServe, Inc. is headquartered there.

The location of the *parties* to a communication is far more relevant under traditional jurisdictional doctrine than is the location of the *computers* through

²¹⁵See *Pres-Kap, Inc. v. System One, Direct Access, Inc.*, 636 So. 2d 1351, 1353 (Fla. Dist. Ct. App. 1994) (holding that a defendant located in New York is not subject to the jurisdiction of the Florida courts solely by virtue of its having accessed data from a database maintained by the plaintiff on a computer located in Florida).

²¹⁶See Katherine C. Sheehan, *Predicting the Future: Personal Jurisdiction for the Twenty-First Century*, 66 U. CIN. L. REV. 385, 419 (1998) (noting that at one time "most Federal Express packages, regardless of origin or destination, were routed through Memphis, Tennessee").

1999]

PROTECTING THE DIGITAL CONSUMER

which they communicate. But due to the geographic indeterminacy of online communications, online communicators will not necessarily be aware of the location of their interlocutors. Therefore, assertions of jurisdiction should be limited by the rule that the location of an event associated with an online communication may be deemed to occur in the jurisdiction where any recipient of the communication resides only if the sender of the communication knew or reasonably should have known that the communication would be received there. The “knew or should have known” standard is needed to prevent online communicators from wilfully avoiding knowing where the consequences of their communications are felt. The jurisdictional determination should not turn on the recipient’s location at the time she accesses the communication, which is entirely outside the control and knowledge of the sender of the communication, but rather on the more knowable factor of the place of the recipient’s residence.

Where a dispute involves more than one jurisdiction, the determination of which substantive rules of law to apply will depend upon the conflict-of-laws rules in effect in the forum state. In a regulatory action to enforce rules of public law, under traditional principles the substantive law applied is that of the forum state, and the conflict-of-laws analysis collapses into the jurisdictional analysis. This same rule should apply in regulatory enforcement actions arising from online communications.

In actions between private parties, the application of existing conflict-of-laws rules, which depend primarily on the location of various events associated with the transaction giving rise to the dispute, will often be ambiguous, given the difficulty in ascertaining the location of various online events.²¹⁷ This analysis, like the jurisdictional analysis, will be more transparent if the focus is on the location of the parties to a communication rather than that of the various computers that enable the communication. This will be true, for example, when ascertaining locational issues that are of central importance in traditional conflict-of-laws rules,²¹⁸ such as: (1) the location of a person who communicates or transmits data via a computer network; (2) the place for performance of a contract involving communication or transmission of data via a computer network; (3) the place of occurrence of tortious conduct consisting of communication or transmission of data via a computer network; (4) the place of negotiation of a contract; or (5) the location of the subject matter of a contract. Likewise, as with jurisdiction, the location of an online event that is relevant to a conflict-of-laws analysis may be deemed to occur in the jurisdiction where any recipient of the communication resides only if the sender of the communication knew or reasonably should have known that the communication would be received there.

*D. International Cooperation Among Law Enforcement
Authorities*

1. Mechanisms to Improve International Cooperation

Governments should improve their ability to work cooperatively in combating online deceptive marketing practices by:

- a. entering into bilateral and multilateral cooperation agreements, on the model of existing agreements pledging cooperation among agencies that enforce antitrust laws;*
- b. examining confidentiality laws with a view to facilitating the sharing of information among law enforcement agencies in different countries;*
- c. maintaining databases of consumer complaints that may be accessed by law enforcement authorities from other countries, and cooperating with other governments in establishing international databases;*
- d. participating in international organizations of enforcement authorities; and*
- e. facilitating communication among law enforcement officials located in different countries and time zones making use of online communications media.*

²¹⁷But this analysis may not be any more complex than that which is required in the case of certain transnational commercial transactions that do not involve the use of online communications. See Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1234-37 (1998).

²¹⁸See *supra* text accompanying notes 97-105.

1999]

PROTECTING THE DIGITAL CONSUMER

Some existing mutual legal assistance treaties are limited in scope to cover only criminal matters. International cooperation of law enforcement agencies would be facilitated by establishment of agreements covering civil investigations as well.

Facilitating international information sharing may require the modification of national confidentiality laws. It may be helpful to begin with less controversial types of information sharing, such as access to consumer complaints, and progressing to the sharing of investigational information as trust develops between law enforcement agencies in different countries. For example, the FTC recently began allowing Canadian law enforcement agencies to access consumer complaints in the telemarketing complaint system established by the FTC and the National Association of Attorneys General.²¹⁹

International associations of enforcement authorities, such as the International Marketing Supervision Network, the International Organization of Securities Commissions, and the North American Securities Administrators Association, can play a crucial role in facilitating cooperation among consumer protection law enforcement agencies by providing forums in which law enforcement officials may make contacts with their counterparts in other countries, organize concerted action against transnational deceptive marketing practices,²²⁰ exchange ideas about techniques that have proven effective in protecting consumers, and receive early warning about new types of deceptive marketing practices that have not yet reached their shores.

2. Positive Comity

Governments should enter into agreements to exercise positive comity where appropriate.

A state's sovereignty is traditionally exclusive within its own borders, and ineffective elsewhere. Yet all countries have an interest in extending their sovereignty outside their own borders in order to protect their important interests. International comity "is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation."²²¹ As a correlative, it calls upon nations to exercise forbearance in pursuing their objectives when they impinge on the territorial sovereignty of another nation. Comity "is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other."²²²

²¹⁹See *supra* note 124.

²²⁰For example, in October 1997 the International Marketing Supervision Network organized an "International Internet Sweep Day," in which law enforcement agencies from 23 countries identified over 1000 Web sites offering dubious get-rich-quick opportunities. Participating agencies sent e-mail messages to the operators of these sites, informing them of the legal requirements applicable to their online offerings. See *Internet Fast-Buck Artists Warned Against Peddling Fraudulent Wares*, 2 Electronic Commerce & L. Rep. (BNA) 1238 (Nov. 26, 1997). The Network conducted another Sweep Day in 1998. See International Mktg. Supervision Network, *International Internet Sweep Days* (visited Mar. 24, 1999) <<http://www.imsnricc.org/imsn/activities.htm>>.

²²¹Hilton v. Guyot, 159 U.S. 113, 164 (1895).

²²²*Id.* at 163-64.

One application of the comity principle that may be employed to reduce conflicts between national governments in pursuing cross-border enforcement is known as “positive comity.” Under this approach, enforcement authorities of one country may bring to the attention of enforcement authorities in another country conduct within the latter’s territory that has effects within the former’s territory, and may request that authorities in the country where the conduct is situated take enforcement action. An approach of this sort will be especially helpful in overcoming the problem of cross-border targeting, in which a law violator targets only consumers residing outside the jurisdiction in which he is located. Competition law enforcement authorities have entered into international agreements that implement the principle of positive comity.²²³ Another, less clearly defined, application of the comity principle is found in the Organisation for Economic Co-operation and Development’s 1984 recommendation that member countries use “moderation and restraint” before taking actions that may result in the imposition of conflicting requirements on multinational business enterprises.²²⁴

²²³ See U.S.-CANADA TELEMARKETING REPORT, *supra* note 111, at 19-20; U.S.-EC Agreement, *supra* note 125, art. 3.6.

²²⁴ ORGANISATION FOR ECON. CO-OPERATION AND DEV., MINIMIZING CONFLICTING REQUIREMENTS: APPROACHES OF “MODERATION AND RESTRAINT” 41 (1987).

In contemplating new legislation, action under existing legislation or other exercise of jurisdiction which may conflict with the legal requirements or established policies of another Member country and lead to conflicting requirements being imposed on multinational enterprises, the Member countries concerned should . . . [e]ndeavour to avoid or minimise such conflicts and the problems to which they give rise by following an approach of moderation and restraint, respecting and accommodating the interests of other Member countries.

Id. (citation omitted).

Some OECD member countries view the approach of “moderation and restraint” as a requirement of international law, rather than an application of the comity principle. *See id.* at 9-10.

1999]

PROTECTING THE DIGITAL CONSUMER

In the absence of such agreements, countries may engage in an informal sort of positive comity, by exercising a reciprocal willingness to expend enforcement resources in pursuing law violators located on their own soil, even if all the victims are located outside the country.²²⁵

3. Recognition of Foreign Judgments

Governments should liberalize the standards under which their courts recognize judgments entered by courts in other member countries.

Facilitation of enforcement of foreign judgments may be accomplished by modification of national law, negotiation of bilateral mutual recognition agreements, and participation in the negotiation of multilateral mutual recognition agreements, such as the present effort by the Hague Conference to negotiate a Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters.²²⁶

4. Removing Obstacles to Cross-Border Investigations

Governments should make efforts to remove obstacles to effective and expeditious investigations by law enforcement authorities in cross-border situations. Useful actions include:

- a. requiring domain name registrars to make efforts to validate the identifying information submitted by a registrant before setting up an Internet domain;*
- b. requiring the operators of commercial mail receiving agencies to make efforts to collect, validate, and maintain information concerning the identity of their customers; and*

²²⁵An example of this in the online context occurred when Australian authorities took action to shut down an allegedly deceptive Web site, despite the fact that few of the victims were Australian. The Web site offered domain name registration services, operating through the address "http://www.internic.com". U.S. consumer protection authorities considered this address confusingly similar to the address "http://www.internic.net", which is used by the official domain name registrar, Network Solutions, Inc. The Australian company charged \$250 for a two-year registration, considerably more than the \$100 charged by the official site. According to an FTC official, whose staff referred the matter to the Australian Competition & Consumer Commission, "There are relatively few Australian victims but the Australian authorities recognize that in the future of the Internet we are going to have to move to protect people globally." Jeri Clausen, *Australian Web Company Accused of Misleading Domain-Name Buyers*, N.Y. TIMES (CYBERTIMES), Aug. 22, 1997 (on file with author); see also Rajiv Chandrasekaran, *Australian Firm Offers Costly Web Site Rights*, WASH. POST, Aug. 22, 1997, at G1 (stating that Australian authorities began an investigation of the fraudulent Web site after notice from the FTC). The Australian Competition & Consumer Commission filed fraud charges against the company. See *Australian Consumer Commission Charges InterNIC Copycat with Misleading Conduct*, 3 Electronic Commerce & L. Rep. (BNA) 624 (May 13, 1998).

²²⁶See *supra* notes 88, 107.

- c. *investing in computer equipment, software, and training of law enforcement personnel, so that law enforcement authorities have the tools they need to control online deceptive marketing practices.*

Domain name registrars currently make no effort to validate the identification information they receive from persons who register Internet domain names. This can render unavailable to law enforcement authorities, and to private parties, one avenue for determining the identity of those who engage in online deceptive marketing practices.

A verification requirement would unavoidably create additional costs for domain name registrars, which would be borne by Internet users and industry participants, in exchange for the benefits resulting from an enhanced ability to identify the owner of a domain. The costs of such a requirement would vary, depending on how it is crafted. On the less burdensome end of the scale is a simple verification that the registrant does in fact receive mail at the address he specified in the registration. The procedure that Network Solutions, Inc. (“NSI”) currently follows in registering names in the .com, .org, and .net Global Top Level Domains—adopted, apparently, not in response to any threat of government sanction—comes close to this level of verification.²²⁷ NSI sends the registrant an invoice for the registration fee by both e-mail *and postal mail*. It appears that, under the present system, the registrant may pay the fee without receiving the postal mail version of the invoice, using a credit card or online payment. However, the system could be modified, at no great cost, to require receipt at the postal address: NSI could include in the postal letter a code number, generated automatically, and could refuse to accept payment unless it was accompanied by the code number.

Stronger forms of verification would be correspondingly more burdensome, for both registrar and registrant. Thus, the registrar could be required to obtain from the registrant two forms of photo identification, and to verify that the registrant’s picture appears on the identifications. This would require in-person registrations, which the registrar might accomplish by setting up branch offices at multiple convenient locations, or by contracting with a third party that already has the necessary infrastructure (such as post offices or banks). A system like this, though potentially quite useful where a Web site or e-mail domain is used to commit law violations, would be relatively costly, and would be unlikely to win much support.

A verification requirement also raises free-speech issues, as it interferes with the ability of online users to communicate anonymously. Acknowledging that the interest of online speakers in anonymity is legitimate and of constitutional dimension,²²⁸ it is also undeniable that anonymous speech has its dark side, facilitating certain types of antisocial behavior. Therefore, it seems justifiable to limit the availability of certain modes of anonymous online speech, while leaving other channels unrestricted. In particular, it seems reasonable for governments to require that one who establishes a commercial Web site be identifiable. A Web site is a relatively permanent establishment, in online terms, which has a

²²⁷The registration procedure is described in NSI’s statement of policy. *See Fee for Registration of Domain Names* (visited Nov. 1, 1998) <<http://www.internic.net/domain-info/fee-policy.html>>.

²²⁸*See supra* text accompanying notes 139-42.

1999]

PROTECTING THE DIGITAL CONSUMER

correspondingly greater potential to be used as a tool of deception than e-mail messages and newsgroup postings. A well-designed Web site can create an illusion of substantiality, in a way that e-mail messages and newsgroups postings cannot. A restriction on anonymous commercial speech via Web site, which does not affect the availability of anonymous speech via e-mail and newsgroup postings, may be viewed as a time, place, and manner restriction that is justified by society's interest in deterring and redressing fraudulent, misleading, and criminal conduct.²²⁹

Because swindlers who operate online often hide behind private mailbox services, rules requiring the operators of these services to obtain and maintain information identifying their customers can provide substantial assistance to law enforcement officials.²³⁰

VII. CONCLUSION

Online commerce promises enormous rewards for both consumers and online sellers, if the obstacles to its development can be overcome. This Article focuses on two such obstacles: the fear by consumers that they will be swindled by sellers that are known to them only through the embassy of pixels on a computer monitor, and the unwillingness of sellers to venture online without a clear understanding of their potential legal liabilities.

Governments, industry participants, and consumers all have a role to play in overcoming these obstacles. Interested parties must cooperate in facilitating the operation of market forces that can control the incidence of deceptive marketing practices—consumer sovereignty, industry self-regulation, and contract. Governments can and should intervene in online commercial transactions in a manner that is unobtrusive and complements the workings of market-based control mechanisms. They can facilitate the working of consumer sovereignty by requiring vendors to disclose certain categories of information to prospective purchasers where appropriate, forbidding sellers to make deceptive or misleading representations, and promoting consumer education. They can serve as a catalyst by encouraging industry to create self-regulatory mechanisms to control fraud. They can facilitate the functioning of the contract regime by bringing breach-of-contract actions on behalf of injured consumers and acting as adjudicator in private actions. Where market forces are unsuccessful, and especially where fraud is involved, governments must be aggressive in bringing enforcement actions.

²²⁹It is noteworthy that Stewart Brand, when he set up a pioneering online communications system called the WELL, insisted that anonymous speech *not* be allowed, and that this feature was built right into the infrastructure. He did so after seeing another online community with which he was associated self-destruct under pressures brought about by the irresponsible use of anonymity. See RHEINGOLD, *supra* note 28, at 49; ESTHER DYSON, *RELEASE 2.0*, at 241 (1997). Anonymity may be very useful in facilitating speech that is unpopular yet valuable. It is not very helpful in creating a community.

²³⁰The U.S. Postal Service recently amended its rules concerning delivery of mail to private mailboxes maintained by a commercial mail receiving agency ("CMRA"). Under the new rules, a person who wishes to receive mail at a private mailbox must submit two forms of identification to the CMRA, and provide documentation establishing her true residence or business address. The owner or manager of a CMRA is likewise required to register with the Postmaster, and provide similar documentation of identity and residence. See *Delivery of Mail to a Commercial Mail Receiving Agency*, 64 Fed. Reg. 14,385 (1999).

At the same time, governments must pay due regard to the problem of geographic indeterminacy, and the concomitant problem of overlapping jurisdiction. They can do so by interpreting legal rules that turn on notions of foreseeability and location in a way that recognizes the special characteristics of the online medium. More generally, governments must be willing to abide by the principle of comity: limiting the reach of their own jurisdiction, and giving up their traditionally exclusive jurisdiction over conduct occurring on their own territory, in exchange for the willingness of other jurisdictions to do the same.