March, 2000

Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdictional Issues Created by the Internet

Margaret G. Stewart, Chicago-Kent College of Law

Available at: http://works.bepress.com/margaret_stewart/1/
Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet*

AMERICAN BAR ASSOCIATION
GLOBAL CYBERSPACE JURISDICTION PROJECT

SPONSOR
SECTION OF BUSINESS LAW
COMMITTEE ON THE LAW OF CYBERSPACE

CO-SPONSORS
SECTION OF INTELLECTUAL PROPERTY
SECTION OF INTERNATIONAL LAW AND PRACTICE
SECTION OF PUBLIC UTILITY, COMMUNICATIONS, AND TRANSPORTATION LAW
SECTION OF SCIENCE AND TECHNOLOGY
SECTION OF TAXATION

PROJECT STEERING COMMITTEE

Chairman
THOMAS P. VARTANIAN
Chair, Committee on the Law of Cyberspace

Vice-Chairman
HENRY H. PERKITT, JR.
Dean, Chicago-Kent College of Law

Project Director and Reporter
MARGARET STEWART
Professor of Law, Chicago-Kent College of Law

Co-Reporter
ELIZABETH DEGRAZIA BLUMENFELD
Co-Chair, Internet Law Subcommittee

Project Manager
JONATHAN TAYLOR
Chicago-Kent College of Law

Committee Advisors
AGNE LINDBERG
Co-Chair, International Transactions Subcommittee

THOMAS M. PITEGOFF
Co-Chair, International Transactions Subcommittee

JOHN MORGAN
Vice-Chair, International Transactions Subcommittee

*Report of the American Bar Association (ABA) Jurisdiction in Cyberspace Project empaneled in 1998 under the title, “Transnational Issues in Cyberspace: A Project on the Law Relating to Jurisdiction.” The views expressed herein have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the policy of the American Bar Association.
## Working Groups

### Advertising/Consumer Protection

**Co-Chairs**

Ron Plessner

Chris Millard

**Vice-Chairs**

David Johnson

Roger Cochetti

Elizabeth DeGrazia

Stuart Ingis

Blumenfeld

**Members**

Niranjan Arasaratnam

Paula Bruening

Becky Burr

Steve Cole

Susan Crawford

Ruth Day

Judith Herrman

John Kamp

Sandra Kirsch

Jeff Maganau

Carla Michelotti

Peter Sand

Shirely Sarna

Keith Scarborough

Al. Sheldon

Roger Tasse

Jody Westby

Douglas Wood

### Data Protection

**Co-Chairs**

W. Scott Blackmer

Marcia Sullivan

**Members**

Lynne Barr

Pierre-Gilles Belanger

Julie Brill

John Byrne

Sally Cowan

Mallory Duncan

James F. F crib

L. Richard Fischer

Libby Fishman

Amy Friend

Francoise Gilbert

Amy M. Gizzarelli

Daniel Greenwood

Robert Grohowski

Andrew Grosso

Susan Hart

Jeffrey V. Havercroft

Janine Hiller

Richard Hornbeck

Oliver Ireland

Sandra Kirsch

Kathy Kohler

David Leifer

Robert Litan

Sanley Mabbitt

James Maxeiner

John Messing

Daniel Morton

Shannon Nebolsky

Ronald Plessner

Mary Revell

Ralph Rohner

Linda Schmid

Jay Soloway

BARRY SoKMAN

Forrest Stanley

Paul Tackaberry

Charles Terribile

George Trubow

Robert Vastine

Clint Walker

Joan Warrington

Hillel Weinberg

Jody Westby

Rafael Zahraldeen

### Intellectual Property

**Co-Chairs**

Ian Ballon

Leonard Nuara

Nuara & Associates, P.C.

### Payment Systems/Banking

**Co-Chairs**

Henry L. Judy

Steven Patrick Rodeman

**Members**

Sergio Gimenez Binder

Phillip Corwin

Juliana Duan

T. McTaggart

Broox Peterson

### Public Law/Gaming

**Chair**

Alan N. Sutin

**Members**

Joseph J. Rosenbaum

Philip McGuigan

David Quist

Stephen B. Chaneles

Ellen Goldberg

Lisa Cohen

Mark Kravitz

1. Members of each working group participated in that group's discussion but are not responsible for other portions of the report.
Sale of Goods
Co-Chairs

JOHN GEDID
CURTIS A. WOLFE

Members
ERIK BARSTOW
JOHN J. A. BURKE
LAWRENCE D.W. GRAVES
JOHN MESSING
SCHUYLER M. SIGEL
MONTY TRIPP

BEN BEARD
FRANCOISE GILBERT
THEODORE LING
BERNARD F. MEYER-HAUSER
FREDERICK W. STEIN

SERGIO GIMENEZ BINDER
JAMES M. GOLDBERG
PETER MANTAS
MICHAEL RUSTAD
SAUL TREIMAN
PATRICK WHALEN

Sale of Services
Chair
MICHAEL A. GEIST

Members
CAROLE ACIMAN
MICHIE FORZLEY
STEVEN HOFFER
DAVID PAMENTER

CHAD BAYNE
SUHESH GUPTA
SEAN HOPKINS

KURTIS DUMAW
ERNST HALPERIN
PETER MANTAS
MARC J. PLOTKIN

Securities
Chair
DENIS T. RICE

Members
ADAM BALINSKY
DAVID POST
HAROLD FEDEROW

BROC ROMANEK
MONT ETZLER
H.G. STEPHENSON
MARC J. PLOTKIN

GARY HAND
BARBARA STETTNER
ROBERT HUDSON

Taxation
Chair
PETER V.Z. COBB

Members
KENNETH BARDEN
HANK GUTMAN

KAYE CALDWELL
STANLEY KATZ

ALAN CHAN
CHELSEA LYFORD

INTERNATIONAL COMMENTATORS

Australia
MALLESONS STEPHENS JAQUES, SOLICITORS

Patrick Quirk

Australia

Brazil
NORONHA ADVOCADOS

Canada
ARLAN GATES, PAUL TACKABERRY, ADAM BALINSKY

David Pamentner

Canada

China
YUNYING SUN

Colombia
LEWIN & WILLS

France
BLANDINE POIDEVIN

Hong Kong
NEIL THOMSON

India
RISHI AGRAWALA

Italy
EMILIO TOSI

Japan
TOKUSHIGE YOSHIMURA

Luxembourg
JAMES A. GRAHAM

Philippines
CARLOS PRADE

Romania
Alexandru Harsany

Switzerland
Bernhard Meyer-Hauser

Taiwan
SPENSER HOR

Uruguay
ALVARO TARABAL, ANABELA ALDAG
# TABLE OF CONTENTS

INTRODUCTION ........................................................................................................ 1806

1. The American Bar Association’s Commitment to the
   Development of a Jurisdictional Infrastructure ........................................... 1810
2. Technology ......................................................................................................... 1813
3. Organization ..................................................................................................... 1819

OVERVIEW ............................................................................................................... 1819

1. SOLUTIONS FOR GLOBAL CONSIDERATION ........................................ 1819
   1.1. Jurisdictional Default Rules ................................................................. 1820
   1.2. Contractual Choice of Law and Forum .................................................. 1822
   1.3. Hybrid Alternative .................................................................................. 1822
   1.4. The Future Global Agenda to Address Jurisdiction
       in Cyberspace .......................................................................................... 1823

2. IN SUPPORT OF THE SOLUTIONS:
   HOW TECHNOLOGY HAS CHANGED
   JURISDICTIONAL PARADIGMS ................................................................. 1824
   2.1. Jurisdictional Principles ......................................................................... 1824
   2.2. The Relevance of Physical Location ....................................................... 1826
   2.3. Targeting .................................................................................................... 1827
   2.4. Power Parameters ..................................................................................... 1829
   2.5. Contractual Choice ................................................................................... 1831
   2.6. The Intersection Between Jurisdiction and
       Substantive Liability for Intermediaries ................................................... 1832

3. THE DOCTRINAL FRAMEWORK .................................................................... 1833
   3.1. Personal Jurisdiction .............................................................................. 1834
       3.1.1. Classic Jurisdiction ......................................................................... 1834
       3.1.2. Jurisdiction Over Defendants Never Physically
               Present in the Forum ........................................................................... 1837
           3.1.2.(a). Jurisdiction Based on Indirect
                    Economic Benefit ........................................................................... 1837
           3.1.2.(b). Jurisdiction Based on Intentional
                    Causation of Effect ........................................................................ 1841
           3.1.2.(c). Jurisdiction Based on Intentional
                    Affiliation ......................................................................................... 1845
       3.1.3. Jurisdiction and the Internet .............................................................. 1848
       3.1.4. General Jurisdiction .......................................................................... 1855
       3.1.5. Contractual Choice of Forum ............................................................ 1860
   3.2. Prescriptive Jurisdiction .......................................................................... 1862
       3.2.1. Constitutional and Other Local Restraints ....................................... 1862
       3.2.2. The Restraint of International Law ..................................................... 1866
       3.2.3. American and European Approaches
               to Choice of Law ................................................................................ 1869
       3.2.4. Torts ................................................................................................. 1870
3.2.5. Contracts ................................................................. 1871
3.2.6. Consumer Contracts ............................................. 1872
3.2.7. The Internet and International Law ...................... 1873
3.2.8. Choice of Law and Personal Jurisdiction ............. 1874
3.3. Enforcement Jurisdiction ........................................ 1874

REPORTS OF THE WORKING GROUPS ................................. 1876
1. Advertising/Consumer Protection ............................... 1876
2. Data Protection ........................................................... 1884
3. Intellectual Property .................................................... 1897
4. Payment Systems/Banking .......................................... 1905
5. Public Law/Gaming ..................................................... 1915
7. Sale of Services: The Example of Telemedicine ........... 1926
8. Securities ................................................................. 1931
9. Taxation ................................................................. 1937

CONCLUSION ....................................................................... 1945
INTRODUCTION

The advent of the Internet has revolutionized the global marketplace. Products and services once offered only at the local store are now available to consumers in every corner of the planet. Thousands of traditional brick-and-mortar stores are taking their businesses online, hoping to stake their claim to Internet fortunes, while explosions of Internet start-up companies with no apparent geographic locale are altering the most conventional business practices. At the same time, automated artificial intelligence represented by software programs, "cookies," applets, and other technological wizardry are acting as programmable and even intrusive agents that assimilate and evaluate information and consummate business-to-consumer and business-to-business transactions. In 1999, retail online commerce is estimated to have reached $18 billion.² Millions of individuals, in every corner of the world, are logging on each day seeking information, communicating ideas, and transacting business.

The result of this fierce competition is a rapidly evolving worldwide market. Businesses must open their doors to fundamental change, while consumers must put faith in the new electronic stores.³ As adaptation to electronic commerce transpires, it is becoming commonplace to refer to its growth and that of the economy it is creating as exponential,⁴ reflecting the combination of Moore’s Law (every 18 months, processing power doubles while cost holds constant)⁵ and Metcalfe’s Law (the usefulness, or utility, of a network equals the square of the number of users).⁶

3. “[W]hile the internet should result in a reduction in business costs it will also lead to an increase in competition. New companies can enter industries more easily. One issue will be the extent to which people are prepared to trust the new businesses and execute transactions online.” Schroeder Economics, Economic Perspective: Quarterly Economic and Market Analysis, First Quarter 2000 (Jan. 10, 2000).
Achieving Legal and Business Order in Cyberspace 1807

nential” is an adjective that in only a few, rare instances—bacterial replication and rabbit procreation—has historically been used accurately to describe numerical growth. Whether electronic commerce should be added to that elite list is yet to be seen, but the growth has been, and is expected to remain, exceptional. This prolific growth is fueled by the relative ease of transmitting information nationwide or worldwide, instantly. Ease of use, powerful and effective communications that are interactive and in many instances occur in real-time, and a culture that encourages the use of computers has created the “virtual storefront.” Without question, the Internet is redefining the way that business is done worldwide.

The growth and pace of change in the communications industry are unlike anything since its inception. Each minute, over five million e-mail messages are now being sent around the world. While it took more than a century to install the first 700 million telephone lines, the next 700 million will be installed in less than 15 years—300 million in China and India alone. In that same period, there will be 700 million new wireless


8. A major “selling point” of the World Wide Web is its ability to offer a “virtual storefront” to anyone, from an individual to a multinational corporation, with a product to market. Commercially available software packages enable even those computer users who are not versed in the intricacies of programming to create customized Web sites quickly and at a relatively low cost. The swift development of this technology and a cultural shift towards encouraging on-line commerce have led to dramatic growth in the demographics and dollar amounts of the on-line marketplace, which in turn offers a challenging new context for the application of the Uniform Commercial Code’s (“UCCs”) established and emerging concepts of the sale of “goods.”


11. Id.
subscribers. One thousand new communication service providers are forecast to be established worldwide within the next two years.

In recent years, the number of computers and users connected to the Internet has skyrocketed as well. The number of computers hooked up to the Internet globally in 1992 totaled only 1.3 million, whereas currently there are more than 85 million worldwide. Today, there are nearly 260 million worldwide Internet users, and forecasts project there will be over 765 million users by 2005. The number of Internet users in the United States equaled 110 million at the end of 1999. In Europe, Internet users in 2000 will climb to nearly 99 million, the Asia-Pacific region will reach over 72 million, while South and Central America will climb to 19.6 million.

Forecasts of e-commerce revenues vary greatly, but market research companies concurrently envision a robust market on the horizon. Forrester Research, for example, projects that by 2003 U.S. business-to-business revenues will reach $1 trillion, while Boston Consulting Group and shop.org set this figure at $2.8 trillion. Business-to-consumer revenues, according to IDC Corp., will surpass $75 billion by 2003, yet Dataquest predicts nearly twice that amount—$147 billion. In the international arena, forecasters anticipate total European e-commerce revenues to reach $1.6 trillion by 2004. In light of worldwide e-commerce revenues in 1996, which amounted to less than $10 billion, the astronomical forecasts for the

12. Id.
13. Id.
18. Almanac, supra note 16.
19. Catch-up, supra note 17.
20. Id.
21. Id.
24. Vanessa Hua, E-Shopping: Online Predictions; Despite huge stakes, Net sales estimates no more than educated guesses, SAN FRANCISCO EXAMINER, Dec. 6, 1999, at A14.
25. Id.
27. Fiorina, supra note 10.
coming years mean e-commerce will become increasingly important for everyone, ranging from educators to athletes to government officials across the world.

The United States government has recognized the potential economic benefits the Internet and e-commerce present to global commerce. It proposed that "[t]he legal framework supporting commercial transactions on the Internet should be governed by consistent principles across state, national, and international borders that lead to predictable results regardless of the jurisdiction in which a particular buyer or seller resides." At least one U.S. federal district court has suggested that the Internet is more properly the province of federal jurisdiction and oversight rather than state-by-state application of laws.

One critical element of the predictability necessary for electronic commerce to evolve profitably and efficiently is businesses’ and consumers’ knowledge of what regulatory regimes will apply to the businesses in which they engage and with which they interact. Compliance with the law is simply not possible without an understanding of whose law (or laws) is (or are) applicable. Willing compliance of businesses with that law, of course, will frequently obviate the need to answer a second question—where legal disputes may properly be resolved—which also requires a predictable answer. Decreasing the number of disputes requiring judicial resolution is a goal of all interested parties. If a legal dispute arises, however, it is necessary to determine both where and under what law to judge the conduct of the parties.

A century and a half ago, most people were born, lived, and died within a small geographical area. Inter-sovereign contact was rare, whether that contact be defined as interstate contact within a federal system or international contact. Territoriality provided a simple, workable principle to define both the personal and the prescriptive jurisdiction of a state. When parties to the action lived and the activities in dispute occurred in a single state, that state’s courts and laws were the only, obvious, and uncontroversial jurisdictional choices. Similarly, no other state needed to recognize the legitimacy of a resulting judgment because the court ren-


29. Id.


31. Personal jurisdiction is the authority of a state to insist that a defendant appear and defend a claim brought against it or suffer the entry of an enforceable default judgment against it. It is part of a broader universal requirement that a court possess adjudicatory jurisdiction, which encompasses subject matter jurisdiction as well.

32. Prescriptive or regulatory jurisdiction is the authority of a state to regulate an entity’s conduct and to penalize its failure to comply with that regulation, either in an enforcement action brought by the state or through the use of its law by its courts to determine the merits of a private claim.
dering the judgment had the power to enforce it against the property or person of the defendant in the state.

Long before the Internet, however, societal changes made the purely territorial jurisdictional universe unworkable. Populations became mobile, and more economic enterprises developed multi-state or multi-national businesses. Inter-sovereign contact became common, and it was necessary to develop jurisdictional rules to deal with defendants whose past presence in a state or whose activities outside the state had caused effects within the state. Territoriality remained in many instances a valid basis for the assertion of personal jurisdiction, but it was joined by the concept of contacts between a foreign defendant and the forum sufficient to make the forum's assertion of jurisdiction fair and just. Much more frequently than in the past, a state with jurisdiction over the defendant would not apply its own law to resolve the conflict, choosing rather to apply the substantive law of another state (often the state where the cause of action arose, if the basis of its personal jurisdiction was the territorial power it wielded over the defendant).

On the other hand, a state whose assertion of jurisdiction over the defendant was based on the contacts between it and the defendant might frequently be the place where the cause of action arose. Hence, the state might hear and decide the case under its own law but rely on another state, where the assets of the defendant were located, to enforce its judgment. 33

The volume of cross-state contacts has increased and will continue to increase at a more rapid rate by virtue of the proliferation of electronic communications and the use of the Internet in commercial applications. Whether that increase will require a normative rethinking of jurisdictional principles similar to that which occurred in the middle of the twentieth century is at the heart of much of the current consideration of effective Internet dispute resolution.

THE AMERICAN BAR ASSOCIATION'S COMMITMENT TO THE DEVELOPMENT OF A JURISDICTIONAL INFRASTRUCTURE

The increasing novelty, complexities, and costs of conflicting jurisdictional questions affecting online commerce are an impediment to its efficient growth. In 1998, the American Bar Association launched a global study to focus attention on potential jurisdictional conflicts and their res-

33. In the United States, the potential for such state "aid" in the enforcement of another state's judgment is constitutionally acknowledged in the "full faith and credit clause." U.S. CONST. art. IV, § 1. Similarly, the Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, Sept. 30, 1968, 1978 O.J. (L 304) 36 [hereinafter Brussels Convention], Title III, provides for recognition and enforcement of a judgment rendered by one contracting state by other contracting states.
olution (Project). Accordingly, the ABA has committed significant resources to promoting, through this Project, a legal infrastructure that can provide the requisite elements of certainty and predictability, allowing electronic commerce to flourish and grow as economically and efficiently as market forces dictate.

The discussion of jurisdiction in the Internet context involves, in a simple sense, the question of whether the law should view Cyberspace as a place, a means of communication, or a technological state of mind. How that question is answered, to some degree, affects how concepts of jurisdiction should be evaluated.

When an online purchase is made, either directly or through the intervention of an electronic robotic agent or “Bot,” programmed with the background, assets, and preferences of its human principal/buyer, has the buyer stepped into a new place or simply used a different means of communication, much like a telephone, fax, or satellite link, to effect that purchase? More specifically, if a buyer orders a book online from her home in Virginia from an online provider physically located in India, is it as if the bookseller brought its inventory to the buyer in Virginia, or as if the buyer flew to India to purchase the book? Does the “push” and “pull” of technology make a difference in how the law of jurisdiction should be applied?

The defense that jurisdiction should not attach when the information is “pulled” into a locale was unsuccessfully made in United States v. Thomas, when Thomas argued that given the nature of digital technology, he did not “push” pornographic pictures into Tennessee, for example, by sending an e-mail to the recipient. Rather, they were “pulled” into that jurisdiction by someone there whose computer could gather the 0s and 1s from his server in Los Angeles and whose software could create a pornographic picture. The argument may be unconvincing on those facts, but the question seems valid, particularly as electronic agents perform an increasing number of commercial tasks on the Internet.

The art of determining jurisdiction has traditionally been viewed as an arcane exercise involving the question of where someone can be sued and whose laws should be applied. While understanding where one may be

34. The Project is directed by a Steering Committee composed of members of the Cyberspace Law Committee of the ABA’s Section of Business Law and representatives from Chicago-Kent College of Law. See <http://www.kentlaw.edu/cyberlaw>.


36. 74 F.3d 701 (6th Cir. 1996).
haled into court is worthwhile, other jurisdictional issues in Cyberspace are frequently far broader and important. For example, when an online distributor of financial products in Dresden, Germany sells those products to a purchaser in Denver, there are jurisdictional questions that both parties may be interested in beyond the question of where one party may sue the other. Where does the seller reside for purposes of organization, franchise, and community responsibility purposes? Whose laws apply to such Cyberspace solicitations, advertisements, and sales transactions, whether across borders or not? Who regulates the company and is that the same regulator as the regulator of the transaction? Who taxes the business and the transaction? How are the transaction’s terms enforced?

Raising other technologically related possibilities significantly complicates this analysis. For example, if the words of a book are sold online and are downloaded to the purchaser rather than actually shipping a hard copy of the book, do the legal consequences of that transaction change? Has technology blurred the lines of demarcation between what should be considered a sale of a service and the sale of a product? If an electronic agent or Bot is executing decisions for a party in a way that does not necessarily suggest a physical location for the action, how is the jurisdictional analysis affected?

The ABA’s Project was designed to address personal, prescriptive, and enforcement jurisdiction issues separately with respect to the areas of substantive law most commonly implicated by electronic commerce from the perspective of the United States and certain European and Asian countries. Ultimately, the goal of this project is to determine whether there is a workable set of legal standards that can form a basis to answer the question of whose laws apply to Internet commerce and where disputes involving that commerce should be resolved. As the materials and analysis that follow indicate, while technology changes how parties communicate, it does not and can not change the fact that parties themselves exist in physical space—the key to any jurisdictional analysis. Cyberspace may be a “place,” but it is inhabited by bits and bytes, not by people. It may change how people understand their boundaries, and thus affect their state of mind, but in the end it is a means of communication.

Initial research and exploratory drafts from the working groups established by the ABA in each of nine substantive areas revealed a greater degree of commonality in the issues presented than might have been expected. Moreover, it has become apparent that the willingness of nation-

37. The substantive areas are advertising/consumer protection, intellectual property, payment systems/banking, data protection, public law/gaming, sale of goods, sale of services, securities, and taxation.
38. See <http://www.kentlaw.edu/cyberlaw> for the Project’s Terms of Reference, etc. The Project is sponsored by the ABA Section of Business Law and cosponsored by the Sections of Intellectual Property Law, International Law and Practice, Public Utility, Communications and Transportation, Science and Technology, and Tax.
states to assert jurisdiction and enforce judgments rendered by others depends on the nature of the judgment, the jurisdictional rationale of the rendering state, and, in some cases, the willingness of the rendering state to enforce the judgments of others, rather than on the substance of the underlying claim. Indeed, to some extent, the nub of the jurisdictional issue is the need to accommodate traditional governmental interests in the void created by the apparent transcendence of borders that is an earmark of online commerce. States, countries and other confederations of jurisdiction seem unwilling to forego the potential tax dollars that online commerce may bring, or the obligation to protect citizens from civil or criminal incursions engineered through the Internet. But can a business comply with the consumer protection, securities, criminal, intellectual property, sales, and other substantive laws of every state, country, or confederation of countries every time that it offers a service or product on the Internet (which, of course, can be accessed any place on the planet)? Obviously, the answer is no. Yet equally obviously, some law must apply to electronic transactions. The hard question for business is which laws do (and should) apply to regulate its online activities and what states will enforce those applicable laws or judgments based upon them. The ABA can perform an important role by conducting the cold, hard research that the world will need to reach agreements that will answer these questions and allow electronic commerce to continue to grow at the exceptional rate that it has. While this step by the ABA may only be the first of many taken by similar groups around the world, it is a critical one upon which important decisions are likely to be based.

TECHNOLOGY

Familiarity with the technologies composing the Internet is essential to understanding some of the unique jurisdictional issues the Internet creates. The term Internet has been used to describe a worldwide group of connected networks that allows the public to access information and services. A computer network is a group of computers connected by communications equipment and software for the purpose of sharing information among

39. See GEORGE S. MACHOVEC, TELECOMMUNICATIONS, NETWORKING AND INTERNET GLOSSARY 56 (1993) (defining the Internet as “[t]he collection of networks that connect government, university, and commercial agencies . . . any set of interconnected, logically independent networks”); see also CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1260 n.2 (6th Cir. 1996) (defining the Internet as “[t]he world’s largest computer network, often described as a ‘network of networks.’”) (citations omitted); Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161, 163 (D. Conn. 1996) (defining “[t]he Internet [as] a global communications network linked principally by modems which transmit electronic data over telephone lines”); American Civil Liberties Union v. Reno, 929 F. Supp. 824, 830-45 (E.D. Pa. 1996) (defining the Internet as “not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks.”).
colleagues. While each of the networks that make up the Internet is owned by a public or private organization, no single organization or government owns or controls the Internet.

The Internet began in 1969 as a network of four computers located at the University of California at Los Angeles, the University of California at Santa Barbara, the University of Utah, and the Stanford Research Institute. The U.S. Department of Defense funded the initial work through an entity known as the Advanced Research Projects Agency (ARPA). The ARPA Network (ARPANET) was designed to be a decentralized system. Some state that the decentralization was the result of an intent to produce a system with the ability to re-route communications in the event of an attack on an individual section of the network. Others believe that the decentralization was simply a necessary concomitant of the decision to use the inherently more efficient packet-switching technology described below.

In the 1980s, the National Science Foundation, the scientific and technical agency of the federal government, expanded ARPANET to connect computers around the world. The Internet, which included electronic mail, exhibited slow but steady growth until 1994, when the World Wide Web was introduced. The World Wide Web, or “the web,” which is the graphical user interface to the Internet, prompted the phenomenal growth in both the size and use of the Internet. The use of the web expanded to business and residential users and stands as the future of commerce by introducing, among other things, a more user-friendly “click and drag” approach to the navigation of the Internet.

The Internet operates by taking data, breaking it up into separate parts called packets, and sending the packets along available routes to a destination computer. Unlike a telephone line, which monopolizes a continuous open wire (through many intermediate locations) throughout the duration of a telephone call, the packet-switched network uses available wire space for only fragments of a second as it transfers a digital message in one direction. The data might be an e-mail message, a web page, a sound clip, a video stream, or a document.

Each packet contains the data, its origin, destination, and the sequence of information needed to reassemble the data once it is received at the destination. These packets can and do travel very different routes on their way to the destination. For example, the first packet of an e-mail

41. Id.
43. Id.
44. Id.
message sent from New Jersey may travel across the telephone line, over thousands of miles of wire, through different countries, or even into space through a satellite, on its way to a destination in Florida, while the second packet may travel directly along the coastline over a fiber-optic cable arriving at the Florida destination before the first packet. Both transmissions take place in a matter of nano-seconds.

To connect to the Internet, businesses and individuals purchase access from Internet Service Providers (ISPs) or Online Service Providers (OSPs). ISPs deliver access to the network in various ways. Some ISPs are integrated with large telecommunications companies like AT&T and MCI. Other national ISPs, like Netcom and PSINet, exist along with local ISPs and cable television companies like ComCast. OSPs deliver access to the net and provide proprietary content organized in an easy to use format. Some OSPs include America Online, Prodigy, and MSN. All of these ISPs and OSPs own or lease a connection to the network.

Today the most common way for individuals to connect to the Internet is through dial-up telephone service. But the speed and clarity of traditional telephone lines, using traditional signals, are limited. To provide faster and better access, individuals and businesses can connect using digital subscriber lines (DSL), Integrated Service Digital Network (ISDN) lines, dedicated T1 or T3 leased lines, or cable modem access. Each of these transfer mediums provides different levels of speed and data capacity known as "bandwidth." They also vary significantly in cost. The greater the bandwidth, the faster large amounts of information can be retrieved and sent. As bandwidth increases, more and more opportunities to transact business online will become available.

Once connected, the users need to be able to find the content they are looking for and the content providers need to find ways to get content to the users. To do this, network users follow a common set of rules known as Internetworking Protocol (IP). Simply put, IP assigns every computer on the Internet an address made up of a series of four numbers between 0 and 255 (i.e. 255.255.100.1). Using these numbers, one computer can contact and communicate with any other computer on the Internet and share data.

IP numbers or addresses enable a computer host to locate a remote computer. Assignment of IP addresses to users was the responsibility of the Internet Assigned Numbers Authority (IANA), a private entity with ties to international standard-setting bodies. IANA delegated the administration of IP address applications and registrations to both government and private commercial bodies.

Now, the Internet Corporation for Assigned Names and Numbers (ICANN) is the non-profit corporation which administers the IP address space appropriation, protocol parameter assignment, Domain Name System (DNS) management, and root server system functions formerly ful-
filled under U.S. government contract by IANA and other entities.\textsuperscript{45} Part of ICANN's responsibility is to address conflicts between domain names and trademarks.

The international addressing of networked computers on the Internet is made possible through a hierarchy of databases, known collectively as the DNS, that associates IP addresses with easily remembered alphanumeric. These designations, known as "domain names," are typically based upon a four-level naming system consisting of a top-level domain, a second-level domain, a third-level domain, and a fourth-level domain. The top-level domain consists of either a two-letter international country code or a generic top-level domain consisting of a three-letter code: COM, ORG, NET, EDU, MIL, or GOV. Second-level domains consist of up to 22-character words, which can include a single symbol, and refer to specific organizations like McDonalds in "mcdonalds.com." Third-level and fourth-level domains refer to a local network computer within an organization's Internet server. Third and fourth level domains are often replaced with "www" to indicate a World Wide Web server.

The seven generic international top-level domains were originally intended to represent differentiated market segments.\textsuperscript{46} Currently, the .COM domain is the most widely used generic top-level domain in the DNS. Until recently, only Network Solutions, Inc. (NSI) carried out the registration and administration of the DNS for the .COM, .ORG and .NET generic international top-level names.\textsuperscript{47} Today, ICANN has opened the domain name registration market to worldwide competition employing one shared database which is managed by NSI.

With a system of Internet addressing in place, software was created to make the Internet easier to use by building in a graphical user interface. This model, developed by Tim Berners-Lee, an Englishman then working in Switzerland, has now become the basis for the web. The web uses a system of linking or "hyperlinking" to allow a user to move quickly from one document or web site to another, regardless of whether the documents

\textsuperscript{45} The Internet Corporation for Assigned Names and Numbers (visited June 3, 2000) <http://www.icann.org/general/abouticann.htm>.

\textsuperscript{46} The .COM domain was intended for use by commercial businesses, .NET was focused specifically for network or Internet service providers, .ORG was meant for non-commercial organizations, .EDU was designated for four-year degree granting educational institutions, .MIL was for the military, .GOV was reserved for government entities.

\textsuperscript{47} Network Solutions, Inc. is a private company which performs the function of registering Internet domain names.

It is currently under contract with the National Science Foundation \ldots and is the leading registrar of domain names. It is the only organization which is permitted to register domain names ending in "\textunderscore \text{com}\textunderscore \text{com}, \"\text_{org}\textunderscore \text{org}, \"\text_{net}\textunderscore \text{net}, \"\text{edu}\textunderscore \text{edu}" or "\text{gov}\textunderscore \text{gov}." It registers over 100,000 new domain names each month—approximately one every 20 seconds.

are located on the same computer, on different computers, or in different countries. A web page is a “hypertext” document that is contained on a computer connected to the Internet known as a “web server.” This document may contain text, graphics, video, sound, or links to other documents.

Web pages are created using Hypertext Markup Language (HTML), which is a set of special instructions called “tags” or “markups” that lay out how the page is displayed and specify links to other documents. HTML allows web page developers to incorporate graphics, animation, audio, video, databases, and plug-in or helper applications. HTML also allows for hidden commenting known as “metatags.” Metatags were designed to allow web page designers to describe the programmed code or list hidden instructions to facilitate later changes. This concept is borrowed from traditional computer programming.

While the reader may now have a better understanding of what the Internet is, he or she may not understand how to navigate (or “surf”) it. Once a connection is made, the user must communicate with the web server to download web pages and view them. Web browser software (browser) interprets and displays web pages and enables the user to hyperlink to other web pages. Common browsers include Netscape Navigator and Microsoft Internet Explorer.

Browsers retrieve web pages by using an Uniform Resource Locator (URL). An URL is an address that points to a specific resource on the Internet. All web page URLs begin with “http://” which stands for “hypertext transfer protocol,” the communications standard used to transfer documents on the web.

Web browsers keep track of web pages viewed through the use of a history list, bookmark list, or Internet “cookie.” Unlike a history list or bookmark, which are designed to assist the user, a cookie is used to assist the web servers and content providers by giving them information about the user. A cookie is a file on the user’s computer that can be and is accessed by web sites that a user visits. With each visit, the web server deposits information in the cookie file about that visit and that information can later be used to personalize information for the user. Web servers now have the ability to customize web site content on a person by person basis and gain valuable information about its users. Although a browser cannot, alone, provide the hosting web site with personal information, the cookie will reveal that the surfer had previously visited the site, and will reveal the web pages the surfer viewed. If, and only if, the user provides the site with personal information, by answering questions or filling out a form, does the site acquire personal information. A valuable marketing research

48. A history list records the web pages a user has viewed during his or her time online.
49. A bookmark consists of the title of a web page and the URL and is stored for the purpose of helping the user find his or her favorite web sites at a later time.
asset is created when this personal information is coupled with the surfer’s viewing habits, obtained from cookies.

Such information allows the vendor to reduce delays during site visits and eliminates the need to re-enter personal data on successive pages or in successive visits. Personal data may be necessary to authenticate the identity of a customer, process electronic payments, extend credit online, or to allow the consumer to track product delivery or verify account activity. Stored personal data may also be used to provide appropriate after-sale service, such as responding to technical questions, furnishing warranty service, and providing information about product upgrades or alerts. Analysis of individual transactions and preferences allows vendors to fine-tune their product offerings and advertising and to target their direct marketing to the elusive “market of one.” Not surprisingly, consumer data has become a prime asset in electronic commerce.

One of the keys to navigating the web is the use of “search engines” and “web portals.” Search engines and portals provide services to web surfers in an attempt to attract masses to their web sites. The concept of a search engine or portal is that individuals use these sites as a starting point to navigate the vast information available online. Common portals currently operated from the United States include www.aol.com, www.lycos.com, www.altavista.com, www.yahoo.com, www.netscape.com, www.msn.com, and www.excite.com. These web sites not only provide news and information about content on the web, but also allow their visitors to search a directory or database of internal information as well as external links to other web sites indexed by keywords and topics.

When searching the Internet for content, search engines review and often analyze the HTML code of each web site to develop a profile of searchable keywords that they later index. By using metatags, web site creators can specify the keywords that they would like indexed by the search engine. Metatags may include multiple listings of the selected keyword. For example, a pornography site may use a metatag such as “sex, sex, sex, sex, Y,” while a software distributor may use a metatag listing the trademarks “Microsoft,” “Adobe,” “Netscape,” “Windows,” etc.

As technology improves, security issues become increasingly important. An unsecured corporate network increases the risk that hackers and other intruders may break into and steal company and client information that may be posted on an intranet or in databases. Security technologies such as firewalls, anti-virus software, and encryption technology help to shield this information from thieves and authors of malicious code and also allow sensitive messages and files to travel, for the most part, securely and safely across the Internet.

The term “firewall” comes from the world of real space in which walls are constructed to shield a room from a fire started in an adjoining room. A network firewall is a combination of hardware and software configured to prevent outsiders from accessing and using a computer network and any other resources connected to that network.
Encryption technology is software that is used to encode data so that, even if accessed by an intruder, it cannot be read or viewed by anyone other than those with the keys to decode the message. These technologies are the means of protecting information as users move to, from, and on the Internet. As discussed above, businesses have a need to protect information online. While there should be little fear that content or messages will be intercepted while en route, information remains vulnerable at both the source and at the destination. The use of encryption should help to ease the fears of those not comfortable with conducting business on the Internet.

“Digital signatures” are a specific use of encryption that allows one party access to an e-communication or e-commerce transaction to verify the accuracy and authenticity of an electronic transmission. A digital signature is essentially an electronic substitute for a manual signature. This digital signature, however, is nothing like a handwritten signature in that it is not a graphic of a handwritten signature or a typed signature. Digital signatures are used to verify that the item or communication received was the item or communication sent. All of this technology is combined on the Internet to allow users and businesses to engage in commercial activity. Electronic commerce involves all of the risks and benefits of traditional commerce complicated by the use of computer and communications technology.

**ORGANIZATION**

The report of the Project (Report) is divided into two primary parts. The overview that follows 1) sets out jurisdictional solutions to puzzles posed by the technology briefly described above for global consideration; 2) describes the changes in jurisdictional paradigms which support those solutions; and 3) provides the doctrinal framework that has and is continuing to emerge which, in turn, supports the described changes. Following the overview are brief reports of the working groups discussing the changed jurisdictional landscape through each substantive law prism.

**OVERVIEW**

**SOLUTIONS FOR GLOBAL CONSIDERATION**

The goals of the Report were to create a global summary of the law of jurisdiction and to explore the issues, uncertainties, and conflicts created by the proliferation of electronic commerce. The completion of this task was far more difficult than was originally envisioned.

The Internet, unlike earlier forms of electronic communication, created a non-linear network where data moves in a widely diffused fashion; this, and other technological changes, raise questions about what laws should apply. The reduction of legal uncertainty is critical to the development of an efficient and effective system to promote electronic commerce. But,
much like the very nature of the Internet, this Report suggests that the resolution of these legal uncertainties is a function of the reconciliation of a wide variety of factors and national and state interests.

During this two-year Project, possible solutions emerged which the Steering Committee and the Working Groups found it impracticable to ignore. The Cyberspace Jurisdiction Project has, therefore, included in this Report, as summarized below, criteria that it hopes governments, interested organizations, businesses, legislatures, and courts will consider as they deal with jurisdictional principles in electronic network environments. By no means are these meant to comprise an exclusive list of immutable dogma. They are merely points we believe others should consider in the establishment of rules, standards, and polices to govern electronic commerce globally. This Project underscores the limited ability that any one state or nation may have in bringing greater certainty to this area. In that regard, we believe that the nature of this subject suggests the establishment of a global commission to test the feasibility of global consensus in this area. Toward that end, we offer the following to assist in the development of an agenda for that process.

Section 1 contains some of the default rules that would form the foundation of a fair system of jurisdictional jurisprudence for commerce in Cyberspace. Section 2 considers the ability of parties to agree upon jurisdiction as a matter of contract. Section 3 considers the use of hybrid solutions that may avoid conflicts that will inevitably need rules of jurisdiction for resolution. Section 4 contains suggestions for the agenda that should be considered in the future.

1.1 Jurisdictional Default Rules

1.1.1. Every Internet party should be subject to personal and prescriptive jurisdiction somewhere. In reasonable circumstances, more than one state may be able to assert both personal and prescriptive jurisdiction in electronic commerce transactions, as they have historically in physical transactions.

1.1.2. Personal or prescriptive jurisdiction should not be asserted based solely on the accessibility in the state of a passive web site that does not target the state.

1.1.3. Both personal and prescriptive jurisdiction should be assertable over a web site content provider (sponsor) in a state, assuming there is no enforceable contractual choice of law and forum, if:

50. Jurisdictional rules, of course, never define the substance of the law that may be applied by a state; they only define what state may exercise jurisdiction over a defendant or regulate its conduct.

51. For purposes of this Report, a "state" is a nation-state (country), a confederation of nation-states, or a separate governmental entity within a nation-state that constitutes a forum which may apply or enforce laws and/or adjudicate disputes.
1.1.3. (a) the sponsor is a habitual resident of that state or has its principal place of business in that state;
1.1.3. (b) the sponsor targets that state and the claim arises out of the content of the site; or
1.1.3. (c) a dispute arises out of a transaction generated through a web site or service that does not target any specific state, but is interactive and can be fairly considered knowingly to engage in business transactions there.

1.1.4. Good faith efforts to prevent access by users to a site or service through the use of disclosures, disclaimers, software, and other technological blocking or screening mechanisms should insulate the sponsor from assertions of jurisdiction.

1.1.4. (a) Users (purchasers) and sponsors (sellers) should be encouraged to identify, with adequate prominence and specificity, the state in which they habitually reside.

1.1.4. (b) Sponsors should be encouraged to indicate the jurisdictional target(s) of their sites and services, either by: (a) defining the express content of the site or service, or listing destinations targeted or not targeted; or (b) by deciding whether or not to engage in transactions with those who access the site or service.

1.1.5. Rules of tax jurisdiction should be more closely related to other rules of prescriptive jurisdiction than has generally been the case.

1.1.5. (a) Jurisdiction for the purpose of requiring assistance in the collection and/or enforcement of taxes that are imposed on residents of the taxing state (tax assistance jurisdiction) should be governed by the same principles as prescriptive jurisdiction in other disciplines.

1.1.5. (b) Jurisdiction for the purpose of imposing a direct tax burden should not be assumed in all cases to be as broad as tax assistance jurisdiction.

1.1.6. Personal and/or prescriptive and/or tax jurisdiction should not be exercised merely because it is permissible under principles of international law. Rather, assertions of such jurisdiction should take into account:

1.1.6. (a) the interests of other states in the application of their law and the extent to which laws are in conflict;

1.1.6. (b) the degree to which application of a state’s own law will impede the free flow of electronic commerce;⁵³

⁵² What constitutes targeting needs to be agreed upon globally. Generically, targeting should cover technological practices that sponsors use to purposefully avail themselves of the commercial benefits of the targeted states. See Parts 2.2 and 3.1.2.(b), infra.

⁵³ In this regard, consider the implications of an international “dormant commerce clause,” a gloss on Section 403 of the Restatement (Third) of Foreign Relations Law.
1.1.6.(c). whether the regulatory or tax benefits to be gained through the assertion of jurisdiction are sufficiently material to warrant the additional burden on global commerce that it will impose; and

1.1.6.(d). principles recognized under national abstention doctrines, such as forum non conveniens, where the interests of justice or convenience of the parties and witnesses point to a different place as the most appropriate one for the resolution of a dispute.

1.2. **Contractual Choice of Law and Forum**

1.2.1. Absent fraud or related abuses, forum selection, and choice of law contract provisions should be enforced in business-to-business electronic commerce transactions.

1.2.2. In business-to-consumer contracts, courts should enforce mandatory, non-binding arbitration clauses, where sponsors have opted to use them, and permit the development of a “law merchant,” in exchange for:

1.2.2.(a). the sponsor’s agreement to permit enforcement of any resulting final award or judgment against it in a state where it has sufficient assets to satisfy that award or judgment; and

1.2.2.(b). the user’s acceptance of an adequately disclosed choice of forum and choice of law clauses.

1.2.3. Jurisdictional choices should be enforced where the consumer demonstrably bargained with the seller.

1.2.4. Jurisdictional choices should also be enforced if the choice of the consumer to enter into the contract was based on the use of a programmed, intelligent agent or Bot\(^5^4\) deployed by or on behalf of the consumer and whose programming included such terms as the nature of the protections sought, the extent to which such protections are enforceable, and other factors that could determine whether the user should enter into the contract.

1.2.5. An Internet vendor subject to tax assistance jurisdiction in a particular state should have the option and ability to contract with other Internet or financial service providers to reallocate the burden of the required tax assistance. The taxing state would, of course, have a right to regulate the qualifications of those to whom the tax assistance burden will be shifted.

1.3. **Hybrid Alternative**

Safe harbor agreements, such as the one negotiated between the United States and the European Union in the context of personal data protection, are good models for the resolution of jurisdictional conflicts in Cyberspace to the extent that they include a public law framework of minimum stan-

---

54. A consumer’s Bot should be defined as one to which no criteria were applied except those explicitly specified by the consumer, *i.e.* a “fiduciary” Bot.
dards, back-up governmental enforcement, and the opportunity for a multiplicity of private, self-regulatory regimes that can establish their own distinctive dispute resolution and enforcement rules.

1.4. The Future Global Agenda to Address Jurisdiction in Cyberspace

A multinational Global Online Standards Commission (GOSC) should be empanelled to study jurisdiction issues and develop uniform principles and global protocol standards by a specific sunset date, working in conjunction with other international bodies considering similar issues. In considering the conclusions listed above as well as others, the GOSC should take into account the following:

1.4.1. In the interests of encouraging the growth of electronic commerce on a fair, universal, and efficient basis, governmental entities should be cautious about imposing jurisdictional oversight or protections that can have negative extra-territorial implications in Cyberspace.

1.4.2. Technological solutions, such as universal protocol standards, employed by intelligent electronic agents may be developed so that users and sponsors may electronically communicate jurisdiction information and rules (including rules relating to taxation), enabling such preprogrammed agents to facilitate the user’s or sponsor’s automated decision to do business with each other.

1.4.3. In the interests of fairness, jurisdictional rules should be developed by and/or only after full consideration of the views of those who must abide by them and/or those substantially impacted by them.

1.4.4. The creation of responsible, private sector, contract-based regimes to which local governments may defer can reduce jurisdictional uncertainty and be more readily adapted to the needs of electronic commerce.

1.4.5. Global regulatory authorities of highly regulated industries, such as banking and securities, should either reach agreement regarding either the uniform application of laws, rules, and regulations to the provision of such products and services or develop rules as to whose laws will be applied in an electronic environment.

55. For example, the Global Business Dialogue, the Hague Conference on Private International Law, the Internet Law and Policy Forum, the International Chamber of Commerce, the United Nations Commission on International Trade Laws, the World Intellectual Property Organization, the World Trade Organization, and others are studying jurisdiction issues in Cyberspace. We note that the Committee of Experts on Crime in Cyberspace of the Council of Europe released a draft treaty that would require all participating nations to adopt new laws requiring government access to encrypted information, expanding copyright and criminalizing possession of common security tools (<http://conventions.coe.int/trevy/en/projects/cybercrime.htm>). The Global Internet Project has issued recommendations for businesses and organizations to follow and measures for governments to consider regarding cybercrimes (<http://www.gip.org/gipwp0500.htm>).
1.4.6. Any use of intermediaries (choke points) in the flow of electronic information, commerce and money, such as Internet Service Providers and payments systems, to regulate commercial behavior and to enforce jurisdictional principles impose significant, new legal burdens on those private entities and should require very careful exploration before being proposed for adoption.\(^{56}\)

1.4.7. Cyberspace may need new forms of dispute resolution—to reduce transaction costs for small value disputes and to erect structures that work well across nation boundaries. Voluntary industry councils and cyber-tribunals should be encouraged by governmental regimes to continue developing private sector mechanisms to resolve electronic commerce disputes. Government-sponsored online cross-border dispute resolution systems may also be useful to complement these private sector approaches. The disputes resolution machinery established under ICANN rules to resolve trademark/domain name disputes is a promising example. Credit card charge backs are another good example, which deserve elaboration for Internet e-commerce.

1.4.8. The global benefits of reciprocal enforcement of judgments should be explored.

1.4.9. Self-regulatory regimes that can forge workable codes of conduct, rules, and standards among a broad spectrum of electronic commerce participants may provide an efficient and cost effective jurisdictional model that governments can adopt and embrace.

IN SUPPORT OF THE SOLUTIONS: HOW TECHNOLOGY HAS CHANGED JURISDICTIONAL PARADIGMS

2.1 Jurisdictional Principles

Jurisdictional principles, both personal and prescriptive, originally derived from an assumption about the absoluteness of boundaries and sovereign power within them. Every nation (or, in a federation, every state) was thought to have complete authority to control persons and things within its borders and to lack any authority to control persons and things outside them. The latter rule was a corollary of the first; outside a nation-state’s borders was another nation with complete authority over its own

\(^{56}\) For example, tax authorities may attempt to increase their efforts to create, on a global basis, uniform rules for requiring tax assistance from non-resident providers of goods and services over the Internet, including efforts to encourage large and sophisticated providers of financial, credit, or similar services to discharge a greater part of the burden of tax assistance. Requiring such assistance is controversial. The E.U. recently proposed requiring foreign sellers of services delivered over the Internet to E.U. customers to charge value-added taxes; the United States immediately protested. See CNN Financial Network, EU Proposed Web Tax (last modified June 8, 2000) <http://cnnfn.com/2000/06/08/europe/eu_vat/>.
territory, foreclosing the exercise of jurisdiction by any other state.\textsuperscript{57} Within its borders, the state could exercise its power, defining characteristic of sovereignty; outside of them, an attempt to do so would lead to war. The jurisdictional assumptions, then, were grounded in political practicality. Such a system makes critical the physical location of a defendant at the moment the state attempts to assert its authority, \textit{i.e.} at the moment the defendant is served with process. If she is served within the borders of the state, its jurisdiction over her person is clear;\textsuperscript{58} although jurisdiction to regulate her conduct might be questionable under today's understanding.\textsuperscript{59} A territorial system can only work, however, if few legal disputes involve multiple states. As changes in the economy and technology made cross-border contact common, therefore, jurisdictional assumptions changed to acknowledge the authority of a sovereign under identified circumstances to assert jurisdiction over persons not physically within its boundaries and to regulate conduct that occurred, at least in part, outside those boundaries. Mutual sovereign acknowledgment of the circumstances under which its citizens and domiciliaries could be subject to the authority of another state permitted the international system to tolerate multiple sovereign authority over persons and conduct, but always with the understanding that assertions of such authority demanded justification. Not only did they in some sense dilute the absolute sovereignty of each nation; they also, of course, implicated the rights of individual defendants. One central tenet of liberty is the right to choose with which government one wishes to associate; to what degree the right to remain unconnected is maintained,

\textsuperscript{57} One early exception to this absolute rule, though perhaps not clearly perceived as such, was the recognition of a nation's jurisdiction over its citizens even in their absence. See Pennoyer v. Neff, 95 U.S. 714, 723-24 (1877). As the story of King Henry II and Thomas Becket demonstrates, such an exception was not always accepted; the Archbishop fled to France precisely because, while on French territory, the English crown had no jurisdiction to penalize his prior conduct in England.

\textsuperscript{58} In the United States, a state may still constitutionally exercise jurisdiction on this basis. See Burnham v. Superior Court, 495 U.S. 604 (1990). Australia also recognizes such jurisdiction on a nation-wide basis. See Comments-Australia, submitted by Mallesons Stephens Jaques, available in <http://www.kentlaw.edu/cyberlaw/docs/foreign/> [hereinafter Mallesons] at 2.2 and 2.6. On the other hand, the Brussels Convention, supra note 33, tit. II, § 1, art. 3, disallows jurisdiction based solely on service in the forum. And, the Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters proposed by the Hague Conference on Private International Law (May 5, 1992) [hereinafter draft Hague Convention] also bars this basis of jurisdiction. Article 18(2)(f)(2)(a) of the same draft also precludes the exercise of jurisdiction based on the seizure of property within the state unrelated to the claim, a position with which the United States is now in agreement. See generally Shaffer v. Heitner, 433 U.S. 186 (1977).

\textsuperscript{59} In fact, when jurisdiction was based on this kind of physical power over the person of the defendant, the court inevitably applied its own law or dismissed the case; it did not apply the law of another sovereign. See A.E. ANTON & P.R. BEAUMONT, PRIVATE INTERNATIONAL LAW 18 (2d ed. 1990).
and when, how, and to what degree it is renounced, drives much of the
law of jurisdiction.60

2.2. The Relevance of Physical Location61

The starting point—historically, in the recent pre-Internet world, and
today—is the physical location of the parties. That location is easily
determined if the critical moment is that at which process is served on a
defendant. It may be easily determined if the critical moment is when an
act took place. But if an activity occurs in Cyberspace, it is impossible to
ascribe it to any specific physical space. Nevertheless, it remains true—and
critical—that parties themselves always exist in real, not virtual, space.

In determining under what circumstances such extraterritorial jurisdic-
tional assertions are proper, courts and legislatures focused in the last half
of the twentieth century, as they had previously, on physical location but
at a different temporal point. Most frequently, the focus was on where
certain activities that gave rise to the plaintiff’s claim had occurred. Where
a negligent act took place, where the injury was suffered, where a contract
was entered into62 or was to be performed,63 where a service was per-
formed, a security offered for sale, or a trademark infringed became the

60. While jurisdictional jurisprudence in the United States specifically focuses on the de-
defendant, many other countries assert jurisdiction based on the place of harm (see Brussels
Convention, supra note 33, art. 5(3)) or the existence of an action brought against defendant
A, served within the jurisdiction, to which defendant B is a “necessary and proper party.”
Id. art. 6(1). Nonetheless, although the defendants’ acts are certainly less than would be
required under U.S. law, in all situations the defendant did choose to do something—manu-
ufacture a product, enter into a relationship with another party—that contradicts its desire
to remain completely isolated. Still, clearly the U.S. concern with choice does not consciously
drive all jurisdictional analysis.

61. The five themes discussed in Sections 2.1 to 2.5 were presented in a speech by Thomas
P. Vartanian. See Thomas P. Vartanian, E-Commerce & Internet Regulation, 1999 BNA
PUBLIC POLICY FORUM ON E-COMMERCE & INTERNET REGULATION (November 15, 1999)
<http://internetconference.pf.com> (on file with The Business Lawyer; University of Maryland
School of Law).

62. Countries gave much thought to the rules regulating contract formation, presumably
at least in part to guarantee perceived desirable jurisdictional results. In Australia, for ex-
ample, a contract is formed at the time and place its acceptance is received by the offeror.
The consumer is the offeror, so the typical consumer contract is “formed” when and where
the consumer receives the seller’s acceptance. See Mallesons, supra note 58, at 3.76-3.82.
Brazil, Columbia, and Romania also look to the residence of the offeror, although in Brazil
a contractual choice of a different law will be upheld if it is not in violation of public policy.
See Written Remarks, submitted by Nestor Nestor Kingston & Petersen, available in <http://

In Canada, proposed legislation would fix the address of the consumer as the place in
which an online contract was formed. See Canadian Law on Jurisdiction in Cyberspace, submitted
by Arlan Gates, Paul Tackaberry and Adam Balinsky, available in <http://www.kentlaw.edu/
cyberlaw/docs/foreign/> [hereinafter Gates].

63. The Brussels Convention permits domiciliaries of contracting states to be sued in the
courts of another contracting state where the contractual obligation in question is to be
performed. Brussels Convention, supra note 33, tit. II, § 2, art. 5.
touchstones of both personal and prescriptive jurisdictional inquiries. As long as such an act occurred within the state’s boundaries, its assertion of both personal and prescriptive jurisdiction was proper. As long as activities continue to occur in “real” space, the place of such occurrences remains relevant.\(^{64}\)

Technology, however, reduces and frequently may eliminate the need for physical contact in the creation of legally significant relationships between parties or between an actor and the state acting as regulator. The legal system must then decide what relationship is necessary between the forum and either the conduct occurring outside the forum or the parties. It is the tie between a party and a forum, not necessarily a physical connection between the forum and the conduct of that party, that is critical. If the remote party (\textit{i.e.} the party never physically in the forum) knows that the proximate party is in (or is a habitual resident of) the forum when the remote party interacts with the proximate party, the remote party has created a tie between itself and the forum state. Now it is the remote-party/forum relationship at the time of interaction,\(^{65}\) not at the time process is served, that matters. Whether such a tie is sufficient to enable the forum to assert personal and prescriptive jurisdiction depends on an analysis of additional factors (such as whether the remote party targeted the forum, discussed below), but its existence is necessary to such assertions. For example, if a doctor in Wyoming, using detailed verbal and visual information supplied to her electronically by a patient living in Illinois, diagnoses the patient and prescribes a course of treatment, the doctor has created a tie between herself and Illinois, whether or not that tie is ultimately sufficient to permit Illinois to assert jurisdiction.

\textbf{2.3. Targeting}

Today, entities seeking a relationship with residents of a foreign forum need not themselves maintain a physical presence in the forum. A forum can be “targeted” by those outside it and desirous of benefiting from a connection with it via the Internet (assuming, of course, that the foreign actor is willing to confine its target to those with access to technology, a growing but still not universal subset of any forum’s population). Such a chosen relationship will subject the foreign actor to both personal and

\(^{64}\) Of course, not all assertions of jurisdiction were based on this kind of conduct-based inquiry. For example, as described \textit{infra}, states continue to assert jurisdiction over their citizens with respect to claims that arise outside of the state and to regulate conduct that occurs elsewhere which is intended to and does cause substantial effects in the state. Nonetheless, a concern with where relevant acts took place is central to many, if not most, decisions.

\(^{65}\) In some contexts some countries have already implicitly recognized this in the specific context of electronic commerce. Australia’s Electronic Transactions Act 1999 (Cth) provides default rules for the place of dispatch and receipt of electronic communications (including the place of an offer or acceptance of a contract) based on the party’s place of business or ordinary residence. \textit{See} Mallesons, \textit{supra} note 58, at 3.5-3.13.
prescriptive jurisdiction, so a clear understanding of what constitutes targeting is critical.

Maintenance of a web site, by itself, should not constitute targeting the world. There is no legal or practical reason why it should. At the other extreme, designing a web site whose only, or at least primary, relevance is to the population of a single forum clearly does target that forum. A site in French, offering to sell securities at prices quoted in francs and supplying French tax information, is certainly targeted at least to France. At issue is whether it might also be considered to target, for instance, French-speaking Morocco, where it is also accessible.

In light of fundamental jurisdictional principles, based on the premise that individuals should be able to choose whether or not they wish to become connected to any given sovereign, the critical issues are the intent of the web site sponsor and what constitutes sufficient evidence of that intent. The site itself provides the first evidence of that intent. It may contain a list of fora it intends to target and filters to block participants from other states. It may contain a list of fora it does not intend to target. But filters may be by-passed, and stated intent may not reveal reality. When transactions are involved, the best evidence of intent is the willingness to deal with persons in the forum state. If securities are knowingly sold to Moroccan citizens, Morocco is a target of the site that promoted them. It must be possible, however, to rely on information concerning location provided by the other party. An e-mail address frequently gives no evidence of where the respondent lives; if an offer of sale is limited to those who are citizens of France living in France, and a purchaser provides a statement of citizenship and a French address, the seller cannot be said to have targeted Morocco if that is, in fact, the home of the purchaser. On the other hand, if an individual wishes to remain unconnected to a state, she

66. It is generally believed that generic disclaimers alone are not sufficient to determine that a site does not target a specific forum. “Offer void where prohibited by law,” for example, says nothing about the actual intent of the offeror.

67. Thus, the Wyoming doctor who diagnosed and prescribed a course of treatment for an Illinois patient performed a regulated service in Illinois.

68. Various countries which have considered when their regulatory laws apply to offshore offerings of securities have all indicated that such targeting is, indeed, the critical inquiry. See generally Richard Cameron Blake, Advising Clients on Using the Internet to Make Offers of Securities in Offshore Offerings, 55 BUS. LAW. 177 (1999).

There is, however, some question as to what a court will determine is necessary to constitute a good faith effort by a web site sponsor to block access to the site by forum residents. In People v. World Interactive Gaming Corp., No. 98-404428, 1999 WL 591995, at *4-*6 (N.Y. Sup. Ct. July 22, 1999), the court found that it was not enough to request a party who wished to gamble to specify his location; if an individual from New York was denied access, all that would be necessary would be to enter another state as his location without physically leaving New York. On the other hand, those wishing to gamble needed to wire money to open a bank account in Antigua, which might have provided another clue to the bettor’s location. And in any event, the requirement of “good faith” implies that even an imperfect filter may succeed if it is a reasonable choice.
must act on that wish. Ignorance of the location of the other party should not be available as an excuse; if the offeror is willing to and does sell its securities in any country in the world, it may well need to comply with the registration requirements of each country.

2.4. Power Parameters

Many jurisdictional rules as they are applied to commercial transactions reflect presumed power imbalances between buyers and sellers. Traditionally, sellers are ordinarily thought to seek out buyers (manifesting their desire to benefit from a connection with the buyers' forum) and to set the terms of the purchase contract. Those presumptions may well be subject to challenge, if not today, in the very near future.

The Internet empowers consumers vis-à-vis sellers. Power in a commercial relationship depends upon knowledge and choice. Electronic commerce in the worldwide marketplace represented by the Internet inherently expands consumer choice because it opens up every market to every buyer regardless of where the seller is located.69 A priori, therefore, electronic commerce strengthens buyers with respect to sellers because it opens up more possibilities for the buyer. Thus, the implied concern that buyers will be taken advantage of by sellers to whom they are tied by geographic or other limitations is less appropriate.

Moreover, the Internet's inherently lower economic barriers to entry already have resulted in smaller sellers transacting business beyond a single geographic location. While this trend is not entirely different from catalogue and telephone businesses, the scale that can be achieved on the Internet with lower costs presents an entirely new phenomenon. This phenomenon expands consumer choice and undermines the assumption that most sellers are more powerful than most buyers. In e-commerce, many transactions may occur between very small enterprises and individuals. This suggests that the consumer law's concern with an imbalance in bargaining power may be less significant for Internet-based commerce. Technology has substantially affected the leverage between buyer and seller.

The Internet also enables more buyers to purchase goods directly from the manufacturer. In the past, intermediaries almost inevitably intervened between the manufacturer and consumers, adding cost to the transaction for sometimes unclear added value. The Internet makes market pricing transparent and may substantially reduce the role of the merchant-intermediary.

On the other hand, the explosion in numbers of sellers may result in a kind of information overload for buyers, negating the improved leverage they have gained in this new market structure. In addition, the same powerful database technologies that increase consumer choice also provide

69. Legal regulation may block some sellers from some markets.
potent tools in the hands of sellers for more precisely targeted marketing, which among other things enables a seller to trade on the fact of simple convenience. But technology may address these problems also.

Cyber-robots, or "Bots," are an increasingly feasible technology that puts the buyer in charge of the buying decision. Such cyberagents with computerized artificial intelligence can be programmed with enormous amounts of information about the goods, preferences, attitudes, and capabilities of their human "principals." They can roam in virtual space without human intervention, endowed with such information, and apply their artificial intelligence to conduct all manner of commercial, social, and intellectual transactions with other Bots. In turn, they can appoint sub-agents, capable of speaking in multiple languages or ultimately communicating through a universal "computer-speak." An individual buyer still may not be able to negotiate the terms of sale, but the ability to find all available terms and prices for a product or service anywhere on the globe empowers the buyer in ways that may surpass the benefits of negotiation. Absent the maintenance by the seller of an interactive site programmed to accept offers in compliance with its terms from any buyer, it is difficult to conclude that, by merely agreeing to sell something to a buyer located elsewhere, the seller ought to be subject to jurisdiction at the buyer's home. Indeed, it is at least arguable that the buyer has "targeted" the seller and ought to be answerable (for nonpayment, for instance) at the seller's home.\footnote{70}

The Internet not only empowers consumers; it also may reduce a seller's power to define its market. In traditional commerce, a seller defines its

\footnote{70. The concern that a mere contractual tie to a forum party would permit an assertion of personal jurisdiction over the non-present party was noted and rejected by the Court in \textit{Burger King Corp. v. Rudzewicz}, 471 U.S. 462, 478 (1985). The Court's opinion makes it clear that among the relevant jurisdictional factors is the extent to which the relationship was actively sought out by the nonpresent party.}

The change may also affect at least default rules respecting applicable law. In Switzerland, for example, a contract is subject to the law of the state with which it is most closely connected, presumed to be the ordinary residence of the party called upon to provide the characteristic performance, i.e. the seller. But to the extent that the buyer defines its purchase, activates delivery, etc., its control may surpass that of the seller, resulting in the use of the law of the buyer's residence. This assumes, of course, that the buyer utilizing a Bot is still seen as the buyer; a Bot might lack legal standing. See Meyer, Müller, Eckert, \textit{ABA Cyberspace Jurisdiction Project} (Dec. 20, 1999), available in <http://www.kentlaw.edu/cyberlaw/docs/foreign/> [hereinafter Meyer], at A and D. The Rome Convention on the Law Applicable to Contractual Obligations, June 19, 1980, 80/934/EEC, 1980 O.J. (L 266) 2, art. 4 [hereinafter Rome Convention] also mandates use of the law of the country with which the contract is most closely connected, presumed to be the habitual residence of the party who is to effect the performance characteristic of the contract.

Such Bots might also be seen as trespassing on third-party web sites. The disruption such a result would cause is severe, because search tools in common use rely on accessing deep links. \textit{See Automated Queries to Ebay Site Preliminarily Enjoined as Likely Trespass}, 68 U.S.L.W. 1734 (June 6, 2000).
market, almost always far narrower than global, by its advertising strategy and budget, its investment in distribution channels, the physical locations of its goods or service-delivery points, and by its processes for taking orders. Electronic commerce on the Internet changes all of that. Unless a seller takes substantial measures, every web site is world wide. The default market is now global. Now, the buyer is as likely to search out a relatively passive seller, as is an active seller to search out a passive customer.

### 2.5. Contractual Choice

Many disputes involving electronic commerce arise between parties who are bound by a contract determining the terms and conditions upon which they have agreed to interact. Frequently, the contract itself may provide that any dispute concerning it is to be heard in the courts of a specified state ("choice of forum" clause or "forum selection" clause) and is to be determined under the substantive law of a specified state ("choice of law" clause).71

If parties to the contract are presumed to have equal bargaining power and, therefore, an equal ability to accept or reject such clauses, the clauses are generally uncontroversial and enforced. When one party to the contract is a consumer, however, equality between buyer and seller has not been presumed. The seller is assumed to define its market and to set the terms of the contract for its own benefit. The buyer is assumed to be confronted with a stark option: accept the terms imposed by one of a limited number of sellers serving her market or forego the purchase. In an attempt to protect the consumer from disadvantageous choice of forum and law clauses, the E.U. will enforce them only if they favor the consumer;72 although in the United States they are enforced unless they are "unreasonable."73

---

71. Contract terms themselves, of course, also supply a set of substantive rules to govern the transaction, which will be used by a court unless they violate the public policy of the forum.

72. Italy, for example, provides that the choice of any forum other than the consumer's domicile is deemed unfair and, therefore, unenforceable unless the seller can demonstrate the existence of dealings over that clause with the consumer. Similarly, the choice of the law of a non-E.U. country is void if the chosen law is less favorable to the consumer and the contract's closest connection is to an E.U. country. See Emilio Tosi, Consumer Protection under Italian Law (Nov. 30, 1999), available in <http://www.kentlaw.edu/cyberlaw/docs/foreign/> [hereinafter Tosi].

For an excellent discussion of these clauses and their treatment in Europe, see Gabrielle Kaufmann-Kohler, Choice of Court and Choice of Law Clauses in Electronic Commerce, in ASPECTS JURIDIQUES DU COMMERCE ELECTRONIQUE (Vincent Jeanneret, dir., 2000).

73. Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585, 593 (1991). However, individual states, when their law is applicable (Carnival Cruise Lines was an admiralty case, so federal law controlled), may as a matter of public policy refuse to enforce such clause. See, e.g., Jones v. GNC Franchising, Inc., 211 F.3d 495 (9th Cir. 2000) (refusing to enforce Pennsylvania choice of forum clause against a California franchisee).
To the extent that the Internet is both limiting the ability of a seller to confine its market and, consequently, dramatically widening the options available to buyers, the presumption of inequality in business-to-consumer transactions is called into question and, therefore, the policy reasons for refusing to enforce contractual choice of forum and law clauses in that context are correspondingly weakened.

### 2.6. The Intersection Between Jurisdiction and Substantive Liability for Intermediaries

If exercises of personal and prescriptive jurisdiction are seen as problematic absent physical contact between the defendant-actor and the forum, states may well be tempted to create new rules of substantive liability for third parties who do have a physical presence in the state's territory. For example, a state unable to compel a nonresident merchant to collect sales tax on sales to its residents might insist that a resident financial institution collect that tax if credit cards issued by it are used by the resident. Today, many controls under the substantive laws of various jurisdictions on international money-laundering are imposed on entities within those jurisdictions that are essentially intermediaries. This is done for the very reason that parties whose money is being laundered are all "off-shore."

Historically, however, it has been changes in substantive law that have driven changes in jurisdictional rules rather than the reverse. In the United States, for example, when privity of contract was required in order for a consumer to sue a manufacturer, manufacturers were ordinarily not liable to consumers. Instead, the consumer's only recourse was against the retail seller, even though the manufacturer was the principle responsible party. No jurisdictional construct was necessary to enable a consumer to sue those manufacturers conveniently, *i.e.* at the consumer's home. After the privity requirement was abandoned, the manufacturer's liability was theoretical rather than real until the law developed the notion of a "stream of commerce" which permitted the manufacturer, under certain circumstances, to be sued in the forum in which the final product was sold to and injured a consumer. An appreciation, however, of the ability of states to assert jurisdiction over non-present parties will generally make it unnecessary to expand liability.

On the other hand, certain traditional kinds of intermediary liability may need to be reconsidered. In the United States, section 230 of the

---

74. For an argument that liability ought to fall on the party best able to manage the risk rather than automatically being assigned to the party "at fault," see Hal R. Varian, *Economic Scene*, N.Y. Times, June 1, 2000, at C2.

75. See *infra*, notes 98-107 and accompanying text.

76. Recognition and enforcement of judgments as distinct jurisdictional issues are discussed in more detail in the doctrinal section, *infra* Part 3.3.
Communications Decency Act\textsuperscript{77} shields ISPs from tort liability for third party content appearing on their sites, in recognition of the practical impossibility of exercising the kind of editorial control over those postings that a newspaper may exercise over articles it publishes.\textsuperscript{78} Additionally, the Digital Millennium Copyright Act\textsuperscript{79} modifies the liability of ISPs with respect to third party copyright violations on their sites. Australia’s proposed Copyright Amendment (Digital Agenda) Bill 1999 (Cth) takes a similar approach. In Britain, however, a server notified by an individual that she considers a posted message to be defamatory may be liable for damages if it does not remove the message when requested.\textsuperscript{80} And at the other end of the spectrum, at least one German court recently held AOL Europe liable for damages resulting from the downloading of copyrighted music by a subscriber, although AOL Europe argued it had made a good faith effort to discourage such violations.\textsuperscript{81}

**THE DOCTRINAL FRAMEWORK**

Courts assert jurisdiction over defendants when the defendants are compelled to appear and defend the claims brought against them or suffer the entry of enforceable default judgments. Legislatures and regulatory agencies acting pursuant to legislative authorization assert jurisdiction over actors when the actors are compelled to comply with regulations covering their activities or suffer penalties specified by the legislation. The executive exercises enforcement jurisdiction when its personnel seize property belonging to a defendant to pay a judgment to the plaintiff, something which no executive will do absent a court order of its own sovereign. Both personal and prescriptive jurisdictional assertions are limited by principles of international law\textsuperscript{82} as well as by a nation’s basic law. While frequently a system with the authority to exercise one kind of jurisdiction will also have authority to exercise the other, and while the factors relevant to each kind


\textsuperscript{81} Ruling Threatens German Internet, FIN. TIMES, Apr. 14, 2000 available in <http://www.ft.com>. Similarly, in 1998, a German court had found the head of CompuServe in Germany guilty of failing to block access to child pornography; the ruling was reversed. Id.

\textsuperscript{82} Pennoyer v. Neff, 95 U.S. 714 (1877), determined that international law constrained states’ assertions of personal jurisdiction prior to the adoption of the 14th Amendment. Subsequent to its adoption, the definitions of the restraints imposed by due process and that imposed by international law have developed in tandem. While Congress may violate international law in exercising prescriptive jurisdiction, it is strongly presumed not to have done so. Murray v. Schooner Charming Betsy, 6 U.S. 64 (1804).
of determination are frequently similar, the issues are analytically separate, the case and statutory law and treaties different, and identical outcomes not inevitable. Personal and regulatory jurisdiction, will, therefore, be addressed individually. Because both are constrained by international law, the approach of the United States mirrors in many ways the approaches taken by other countries heavily involved in electronic commerce. Furthermore, it appears that, because in the United States jurisdictional issues are ordinarily resolved in court, there is more available U.S. law in this area. There are, of course, some significant differences which are discussed. A brief description of enforcement jurisdiction will conclude this section of the report.

3.1. Personal Jurisdiction

Issues of personal jurisdiction are resolved by different methods in common law and civil law countries. Thus, in the United States, jurisdictional principles are developed in case law and focus on broad concepts applied to specific fact patterns. In the European Union and Japan, by contrast, the basic jurisdictional law is statutory and is frequently thought to be more predictable as a result. In many instances, as will become clear in the following pages, the results in both systems are the same. The fluidity of the common law approach, however, does allow jurisdictional assertions by analogy and, therefore, has responded more directly to issues in the context of electronic commerce.

3.1.1. Classic Jurisdiction

Assertions of jurisdiction over the person of the defendant by courts of the United States and of the states must comport with due process in order to be enforceable either by the court rendering the judgment or by other state or federal courts. Since 1945, the constitutional jurisdictional in-

83. See, e.g., Adventure Communications, Inc. v. Kentucky Registry of Election Fin., 191 F.3d 429 (4th Cir. 1999) (discussing whether Kentucky could insist that West Virginia broadcasters, who accepted advertisements from Kentucky gubernatorial candidates broadcast into Kentucky, comply with Kentucky disclosure laws).

84. The discomfort of many civil law countries with the U.S. doctrine of “minimum contacts” is reflected in the current debate regarding article 9 of the draft Hague Convention, supra note 58, which provides for jurisdiction over a defendant where it has a branch, agency, or other establishment and the claim relates directly to the activities of that branch, agency, or establishment. The U.S. delegation wishes also to provide for jurisdiction in a forum where the defendant has carried on related regular commercial activity in the absence of a permanent presence, a provision which many other delegations find troubling because of the definitional issue regarding “regular commercial activities.”

85. Any deprivation of property by the United States, pursuant to the Fifth Amendment to the U.S. Constitution, or by a state, pursuant to the Fourteenth Amendment, must comport with due process; either the extinguishing of a claim by an unsuccessful plaintiff or the award of damages to a successful one constitutes such a deprivation. Courts of each state are
quiry has focused on the contacts between the defendant, the forum, and the litigation. The defendant must have such "minimum contacts" with the forum that the assertion of jurisdiction by it does not offend "traditional notions of fair play and substantial justice." Whether the contacts are sufficient to satisfy the constitutional standard depends upon the "quality and nature" of the defendant's acts in the forum "in relation to the fair and orderly administration of the laws which it was the purpose of the due process clause to insure." This formula focuses on two inquiries: the degree to which the defendant acted in the state and the relationship between those acts and the claim brought against her. An 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" is always necessary. Such an act may be a single occurrence, such as performing a single service in the state; it may be the continuous

required to give full faith and credit to judgments of other states, U.S. CONST. art. IV, § 1, only if those judgments also satisfy the constitutional requirement. See Pennoyer v. Neff, 95 U.S. 714 (1877).


87. International Shoe Co. v. Washington, 326 U.S. 310 (1945). Prior to the Shoe decision, the Court's focus had been on the power of the state rendering the judgment to enforce it. In accordance with then-current understanding of public (international) law, the Pennoyer Court had identified the situations in which such power existed: 1) the defendant had been personally served with process while physically present in the state (the state could theoretically imprison the defendant until the litigation was resolved and, if ordered to do so, the judgment paid; in exchange for the state's willingness to permit the defendant to leave the jurisdiction, other states acknowledged the "power" of the judgment-rendering state and agreed to enforce its decisions); 2) property belonging to the defendant in the forum state was seized at the commencement of the lawsuit (thus providing a fund from which to pay the successful plaintiff); 3) the defendant was a citizen (or domiciliary or resident) of the forum (international law was thought to acknowledge the right of each state to assert jurisdiction over its own nationals even in their absence); 4) the defendant consented to the assertion of jurisdiction (thus obviating any issue of the actual power to enforce the judgment); or 5) the lawsuit involved the status of the defendant under the domestic law of the forum (for example, an absent defendant's marital status vis-à-vis a citizen of the forum). However, as society became more mobile and as the Court's appreciation of the full faith and credit clause grew, it became apparent that the Pennoyer Court's understanding was both unworkably narrow and unnecessary.

88. 326 U.S. at 316 (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)).
89. Id. at 319.
90. Hanson v. Denckla, 357 U.S. 235, 253 (1958). This focus on the defendant's purposeful choice is not found in all other countries. See supra note 60. And outside the constraints imposed by the Brussels Convention, supra note 33, France, for example, will assert jurisdiction whenever the plaintiff is a French national. Code Civil [C. Civ.] art. 14 (Fr.). See Kevin M. Clermont, Jurisdictional Salvation and the Hague Treaty, 85 CORNELL L. REV. 89, 91-95 (1999) [hereinafter Jurisdictional Salvation].
presence of the defendant in the state as a citizen or domiciliary; it may be (and frequently is) something in between. But any time a defendant is by choice physically present in a state, she has benefitted from its legal protections; *Hanson* is satisfied, a prerequisite of the assertion of jurisdiction though not sufficient to sustain it. It remains necessary to consider whether the claim brought against the defendant "arose out of" the defendant’s activities in the state, was completely unrelated to those activities, or was in some way related to them even though the in-state activity is not an element of the plaintiff’s prima facie case.

Although this jurisdictional approach has remained constant, the Court has quietly changed the precise word formula it uses to describe the requirements of due process. "Minimum contacts" is now equated with the *Hanson* requirement that the defendant act purposefully to connect herself to the forum state; *Shoe’s* concern with the "fair and orderly administration of the laws" is now said to require that the assertion of jurisdiction be "reasonable."91 But the two variables remain the same and are at the heart of inquiry.

Both *Shoe* and *Hanson* assumed that a defendant had at some time been physically present in the forum state. The difficulty both cases were attempting to overcome was the traditionally perceived lack of authority to insist a defendant not "caught" within the state return to it to defend a lawsuit arising out of her past presence. The single, past, negligent performance of a contracted for service in the state provides the perfect example; indeed, *Shoe* is frequently praised as an honest statement of jurisdictional concerns previously hidden by rhetoric forced into the *Pennover* framework.92

Under the Brussels Convention,93 specified acts by a domiciliary of a contracting state subject the actor to jurisdiction.94 In many instances, these actions parallel those upon which a U.S. court would rely to find purposeful availing: performance in the state of a contractual obligation

---

92. See, for example, Hess v. Pavloski, 274 U.S. 352 (1927), in which a state's jurisdiction over a nonresident motorist was justified because, according to a Massachusetts statute, the motorist had "consented" to the appointment of a state official as his agent for service of process when he drove into the state. Id. at 356-57. Such consent, of course, is totally fictional and hardly is what the *Pennover* Court rightly thought obviated the need for state power to enforce its judgment. Other state laws also equated doing business in the state with either consent or presence, in an attempt to fit the then-current reality within the *Pennover* linguistics. See generally Richard L. Marcus, Martin H. Redish & Edward T. Sherman, Civil Procedure: A Modern Approach 682-86 (2d ed. 1995).
93. See supra note 33.
94. The Convention applies only to claims brought against domiciliaries of contracting states; if the defendant is domiciled elsewhere, the national law of the forum determines the propriety of a jurisdictional assertion. In the United States, on the other hand, the same due process considerations apply no matter where the defendant is domiciled.
or the occurrence of a tortious event there. Japan’s Code of Civil Procedure similarly provides for jurisdiction where a contractual obligation is to be performed or where a tortious act took place. Both systems make specific and similar rules for cases involving insurance, admiralty, proceedings involving real estate, etc. At least when the identified act in fact took place in the forum (failure to provide conforming goods to a plaintiff in the forum, for example), the resulting assertion of jurisdiction is recognized as proper in the United States, Europe, and Japan.

3.1.2. Jurisdiction Over Defendants Never Physically Present in the Forum

Assertions of jurisdiction based on this kind of past physical presence, of course, are not implicated by changed technology. Cases arising in the context of electronic commerce, however, for the most part do not fit within this simplest part of the Shoe paradigm. Defendants whose forum “presence” is manifested by a website accessible in the forum are the featured players in the new jurisdictional disputes. Still, prior case law has dealt with variations of the same problem and provides at least analogies to guide the emerging jurisprudence. In three different situations, the U.S. Supreme Court has previously found that jurisdiction is constitutionally permissible, even though the defendant did not literally “purposely avail itself of the privilege of conducting activities in the state,” i.e. the defendant had never been physically present in the forum. Acts outside the state, the Court reasoned, which in one way or another could be said to target residents of the state, did invoke the benefits and protections of state law, thus satisfying the Hanson requirement and permitting the assertion of jurisdiction if such an assertion would otherwise be reasonable.

3.1.2. (a). Jurisdiction Based on Indirect Economic Benefit

The most common scenario in which a defendant never physically present in the forum may nonetheless constitutionally be subject to jurisdiction there involves a doctrine known as the “stream of commerce.” Initially formulated by the Illinois Supreme Court in Gray v. American Radiator &

95. Brussels Convention, supra note 33, tit. II, § 2, art. 5.
97. Obviously parties can interact with each other electronically in legally significant ways without the use of a website. When they do, however, each knows from the outset the identity of the others, and jurisdictional resolutions developed in the context of other long distance commercial relationships are easily applied.
Standard Sanitary Corp., the doctrine permits jurisdiction to be asserted over a component parts manufacturer when a good containing its part is purchased in the forum by a consumer who is later injured there by an alleged malfunction of the part. The court reasoned that without the sale to the Illinois consumer of the completed product, the parts manufacturer would have had no market for its part; therefore, the laws of Illinois that protect and facilitate commerce within the state benefit and protect the defendant, whose true, although indirect, source of economic benefit is Illinois. The United States Supreme Court appeared to accept the Gray logic in World-wide Volkswagen Corp. v. Woodson, although it held that the doctrine would not sustain jurisdiction on the fact pattern there before it. In World-wide, the objecting defendants were a New York car retail dealer and its regional distributor. The plaintiffs had purchased a car in New York and, when injured in an accident in Oklahoma, attempted to sue the defendants, as well as the car manufacturer and importer, in Oklahoma. The Court held that whatever “stream of commerce” the car had entered, it left that stream at the point of its purchase, i.e., in New York. The later unilateral decision of the purchasers to remove the car from New York could not provide a basis of jurisdiction over the retailer and distributor, who had had no voice in the decision and procured no benefit from it.

More recently, at least some members of the Court have expressed concern at the breadth of jurisdiction made possible by the doctrine. In Asahi Metal Industry Co. v. Superior Court, the Court was unanimous in its opinion that the assertion of jurisdiction by a California court over a Japanese company being sued as a third party by a Taiwanese component parts manufacturer seeking contract indemnification would be unreasonable and, therefore, unconstitutional. The Court split, however, on the question of whether the Japanese defendant’s use of the stream of commerce was sufficient to constitute “purposeful availing” and thus provide the requisite “minimum contacts.” Writing for herself and three others, Justice O’Connor argued that it was not. The defendant manufactured tube valve assemblies, which it sold to the Taiwanese company that manufactured the tube used in a tire sold to Honda which burst while the plaintiff was riding a Honda motorcycle in California. The plaintiff’s suit had settled, leaving only the claim between the two foreign companies. Accepting that the Japanese defendant was aware that its product might well be used in a motorcycle purchased in California, Justice O’Connor

98. 176 N.E.2d 761 (Ill. 1961).
100. In dissent, Justices Marshall and Brennan argued that the defendants did indeed benefit from the existence of Audi dealerships and repair facilities throughout the United States, including Oklahoma, and that such indirect benefit, like that identified in Gray, ought suffice, at least in light of the fact that cars are intended to be driven from one place to another. Id. at 313-17 (Marshall, J., dissenting).
found that “mere awareness” was insufficient to satisfy *Hanson*; it was necessary that the defendant in some fashion purposefully direct its action toward the forum state.\textsuperscript{102} Her examples included designing a product for a market, advertising, establishing channels for advice to customers in the forum, or using a distributor as a sales agent in the state.\textsuperscript{103} Intuitively, it would seem unlikely that many parts manufacturers would engage in such conduct, however. Four of the remaining justices thought that the “regular and anticipated flow of products from manufacture to distribution to retail sale” in a forum was sufficient to satisfy *Hanson*,\textsuperscript{104} while Justice Stevens thought the inquiry depended upon “the volume, the value, and the hazardous character of the components.”\textsuperscript{105}

Given recent changes in the composition of the Court, it is hard to predict whether the kind of directed activity thought necessary by Justice O’Connor will be required by a majority. Her argument, however, leaves open another question: if a manufacturer does direct its activity toward a particular forum, is that conduct alone sufficient to constitute “minimum contacts,” even if the manufacturer does not utilize a stream of commerce that crosses state lines. Advertising is the obvious example; a seller may advertise in a market in which its products are not sold, intending to reap economic benefit from consumers in that market when they purchase the product at the seller’s home.\textsuperscript{106} On the one hand, the seller has targeted the advertising forum, connecting itself to that forum in a way that is at

\textsuperscript{102} Id. at 112. Many courts have latched onto this language to conclude that when such purposeful direction, or targeting, is shown, both personal and prescriptive jurisdiction may be asserted by the targeted forum. See supra Part 2.2.

\textsuperscript{103} Id.

\textsuperscript{104} Id. at 117.

\textsuperscript{105} Id. at 122 (Stevens, J., concurring).

\textsuperscript{106} In *Shoppers Food Warehouse v. Moreno*, 746 A.2d 320 (D.C. 2000), advertising in D.C. was held sufficient to subject the defendant to jurisdiction in the District of Columbia where a District plaintiff slipped and fell in the defendant’s Maryland store, although the court did note that 1) the claim was only “related” to the advertising and 2) the jurisdictional result might have been different had the advertising been on the Internet, even though the greater metropolitan D.C. area, including the pertinent parts of Maryland and some of Virginia, can be considered a “unified legal and commercial community.” Id. at 332.

The court’s caveat about Internet advertising is interesting in light of *Butler v. Beer Across America*, 83 F. Supp. 2d 1261 (N.D. Ala. 2000). An Alabama law permitted parents to sue those who sold alcohol to their minor children; from his home in Alabama, the plaintiff’s son ordered beer from the Illinois defendant which was shipped to him in Alabama. Finding that an assertion of jurisdiction would violate due process, the court focused on the fact that the sale occurred “in” Illinois, because that is where title to the beer passed (a nice example of courts’ traditional fixation with physicality) and that each state regulates sales of liquor within its borders (which is in fact a concern with the scope of Alabama’s regulatory jurisdiction). The personal jurisdiction issue can be seen as resolved correctly only if the defendant is conceived of as a local, Illinois entity not reaching into Alabama to solicit customers—a questionable conclusion here, given not only its use of the web but also its name, failure to attempt to limit access to those everywhere over the age of legal majority, and its undisputed knowledge of the residence of the purchaser.
least marginally related to any claim caused by the purchase of the advertised product. On the other hand, the liability of the seller for defects in its product is in no way dependent upon the advertising, as would be a claim, for example, for false advertising. In addition, no economic benefit, direct or indirect, accrues to the seller in the forum where the advertising occurred; the benefit accrues when the product is purchased at the seller’s home. Nonetheless, it is generally assumed by buyers, sellers and courts that such conduct, at least when the buyer has not physically traveled to the seller’s home, does give rise to jurisdiction over the seller in the buyer’s home forum with respect to a claim based on the sale. The justification for this result, however, is best considered in the context of a different rationale, that of targeting a forum, discussed below, at 3.1.2.(b).

Despite the superficial appeal of the stream of commerce doctrine to determine the jurisdictional relevance of Internet commerce, it does not withstand close scrutiny. Like the stream, a web site reaches many different fora; also like the stream, the defendant has no control over where the site “ends up” or is accessed. Indeed, the Internet now provides a means for two blues clubs 1500 miles apart to argue about the ownership of a club name. In Bensusan Restaurant Corp. v. King, for example, a judge in the Southern District of New York held that a defendant’s mere operation of a web site, without more, was insufficient to confer jurisdiction. In so holding, the court focused on the situs of the web site (which the district court concluded was either in Missouri, where the defendant resided, or Cyberspace) and the nature, purpose, and intended audience of the site, which was directed almost exclusively to residents of Missouri. None of the information on the web site was targeted to residents of New York, although, given the nature of the Internet, New York residents could access the site as easily as Missouri residents, and may in fact have done so. But it is doubtful that a New York blues lover would travel to Missouri merely to take advantage of the club she saw advertised on the Internet. The district court, citing Asahi Metal Industry Co. v. Superior Court, analogized the operation of a web site in dicta to the placement of a product into the stream of commerce, concluding that even though a web site may be accessed from anywhere in the world, without more, the operation of a web site is not an act purposefully directed toward the forum state. Similarly, in

107. Jurisdiction over the buyer at the seller’s home, for nonpayment for example, is not assumed, however. Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985); Jamik, Inc. v. Days Inn of Mount Laurel, 1999 WL 109200 (N.D. Ill. 1999).
111. The case turned on an interpretation of New York’s long-arm statute.
CompuServe, Inc. v. Patterson,\textsuperscript{112} the court, while finding jurisdiction proper on other grounds, noted that the stream of commerce would have not been a sufficient basis for its assertion.

The difficulty with the application of the stream of commerce doctrine in Cyberspace is that the theory is designed to deal with jurisdictional issues in a very particularized context, claims of injury caused by the negligence of a parts manufacturer. It depends on the Gray court's insight that the defendant received (indirect) economic benefit when the sale was consummated in the forum to the consumer and thus benefited from the forum's laws in a way related to the claim brought there against it. It certainly may imply that when the defendant sells a product directly to the plaintiff, the defendant has satisfied the requirement of purposeful availing, but it is not necessary to that conclusion. The theory also is not relevant when, as in Bensusan, the claim is that the defendant infringed the plaintiff's trademark, a claim analogous to the commission of an intentional tort from which the defendant derives no economic benefit.

By contrast, the Brussels Convention and Japan's Code of Civil Procedure both permit assertions of jurisdiction over a defendant if conduct outside the forum resulted in tortious injury to the plaintiff within it.\textsuperscript{113} Apparently, this is true even if the presence in the forum of the product that caused injury cannot be attributed to any act of the defendant. While civil law countries are, as previously noted, frequently concerned about the breadth of potential jurisdiction made possible by the U.S. doctrine of "minimum contacts," this difference in approach permits European and Japanese assertions of jurisdiction in situations that would constitute a violation of due process.\textsuperscript{114} In the context of the Internet, jurisdiction in Bensusan would have been proper in New York and anywhere else the site was accessed, although only for the damages caused to the plaintiff in the forum.\textsuperscript{115}

3.1.2.(b). Jurisdiction Based on Intentional Causation of Effect

The second situation identified by the U.S. Supreme Court in which a defendant never physically present in the forum nonetheless may be subject

\textsuperscript{112} 89 F.3d 1257 (6th Cir. 1996).

\textsuperscript{113} Brussels Convention, supra note 33, tit. II, §2, art. 5. Financial damage alone is insufficient to trigger this provision, however, and if damage is suffered in more than one jurisdiction (for example, in a claim for libel), each jurisdiction may only assess damages for the harm caused there; the plaintiff may obtain complete relief only from the forum in which the wrongful conduct occurred. See James A. Graham, Comment to the Draft Final ABA Report § II (visited July 3, 2000) <http://www.kentlaw.edu/cyberlaw/docs/foreign/> [hereinafter Graham]. With respect to the interpretation of the Japanese Code, see Oda, supra note 96, at 395-96, and Kitagawa, id., § 1.02.

\textsuperscript{114} According to James A. Graham, this reflects a basic principle of European tort law, not shared by the United States, that only the victim/plaintiff needs protection. James A. Graham, IR: Comments to the Proposed ABA's Draft (visited July 3, 2000) <http://www.kentlaw.edu/cyberlaw/docs/foreign/>.

\textsuperscript{115} Id.
to jurisdiction there does provide a workable analogy for Internet commerce cases. If the defendant intends to and does cause damage in the forum, it is subject to the forum’s jurisdiction. The classic international law example involves a defendant standing in the United States shooting an individual standing a few feet away in Canada. The Court’s acceptance of the constitutionality of jurisdiction on this fact pattern is exemplified in *Calder v. Jones.* The plaintiff alleged that two individual defendants, a newspaper editor and reporter, as well as the newspaper itself, had libeled her. Jurisdiction over the paper was not challenged; it sold copies of the paper in California, the forum state. The individual defendants, however, had never been in California in any jurisdictionally significant way. Nonetheless, jurisdiction over them was constitutionally asserted. The Court focused on two sets of facts: first, everything relevant to the claim other than the actual writing and editing of the story focused on California. The plaintiff and her career were there; the alleged acts took place there; the sources were there. Second, every aspect of the defendants’ activities was intentional (rather than negligent): writing is an intentional act, libel is an intentional tort, and the causation of damage in California was intentional (given that the defendants knew the location of the plaintiff and her business). Many cases can be explained (and the results accurately predicted) by *Calder,* including most of those involving intellectual property.

The clearest use of the analogy is *Pannavis Int’l, L.P. v. Toeppen.* There, the Ninth Circuit held that jurisdiction was proper in California over an Illinois defendant, where the defendant, an alleged domain name hijacker—or cyber-squatter—had intentionally registered the California plaintiff’s trademarks as his domain names. Toeppen registered *panavision.com* and used it as the address for a web site that displayed aerial views of Pana, Illinois (literally a vision of Pana). Lawyers for Pannavision In-

---


117. No matter how slight the actual activity of the defendant in the state is, jurisdiction is constitutionally proper if the claim arises directly out of that activity, as libel arises out of the sale of the paper in the state. *Kecton v. Hustler Magazine, Inc.,* 465 U.S. 770, 773-75 (1984).


119. 938 F. Supp. 616 (C.D. Cal. 1996), aff’d, 141 F.3d 1316 (9th Cir. 1998).
ternational L.P., which owned the “Panavision” trademark, sent Toeppen a letter so advising him and demanding that he stop using that trademark or the panavision.com domain name. Toeppen then wrote Panavision offering to sell it the domain name for $13,000 (and promising that if it paid this sum it would not “acquire any other Internet addresses which are alleged by Panavision Corporation to be its property.”). When Panavision refused, Toeppen registered panaflex.com (Panavision also owned the “Panaflex” trademark), which he used for a website that simply displayed the word “Hello.” Panavision sued in California, alleging that by registering these domain names, Toeppen prevented it from using them and that his sole purpose for doing so was to extract money.

The district court found jurisdiction appropriate under Calder because the defendant intentionally directed his conduct towards California, knowing that the effect of his actions—in registering plaintiff’s trademarks as his domain names—would be felt in that state.

The Ninth Circuit agreed, analogizing cyber-squatting to an international tort and noting that Toeppen “purposely registered Panavision’s trademarks as his domain names on the Internet to force Panavision to pay him money.”120

The brunt of the harm to Panavision was felt in California. Toeppen knew Panavision would likely suffer harm there because, although at all relevant times Panavision was a Delaware limited partnership, its principal place of business was in California, and the heart of the theatrical motion picture and television industry is located there.121

Another case, Blumenthal v. Drudge,122 makes clear that the most obvious

120. 141 F.3d 1316, 1321 (9th Cir. 1998).
121. Id. An alternative approach might have avoided reliance on Calder, assuming that Panavision only wanted to prevent the use of the domain name by Toeppen. The name is property; the state where it is located, i.e. the state with jurisdiction over the entity who controls it (Network Solutions, Inc. in Virginia) may seize it; because the claim arises directly out of the use of the property, there are minimum contacts between the defendant Toeppen and the state where it is located and due process is satisfied. See Thomas R. Lee, In Rem Jurisdiction in Cyberspace, 75 WASH. L. REV. 97 (2000).


In turn, an alternative to in rem jurisdiction is provided by the new arbitration procedures of the ICANN. By registering a domain name, registrants agree to arbitrate the transfer and recovery of domain names, provided by dispute resolution services including the World Intellectual Property Organization. The advantage, of course, is speed. See John Caher, New Domain Arbitration Rules Get Results (visited July 3, 2000) <http://www.lawnewsnetwork.com/stories/A18566-2000Mar13.htm>.

analogy can be obscured by the advent of new technology. The plaintiff was a White House employee whose connection with the District of Columbia paralleled that of Jones to California. The Drudge Report containing the alleged libel was circulated in the District, albeit on the Internet, and, given its political and gossip content, was designed for an audience likely to live there. The column, while posted on the defendant’s web site, was also sent to subscribers via e-mail. Had the Internet not been involved, a one line cite to *Calder* would have sufficed. Instead, the court focused on the interactive nature of the web site, a fixation of many lower courts deciding these kinds of cases which will be addressed below.

A somewhat similar case, the only reported case involving the Internet as yet decided in Australia, came out differently. In *Macquarie Bank & Anor v. Berg*, 123 the bank sued a former employee, alleging he had defamed it on a web site located outside Australia; the employee himself was also outside Australia at the time the claim arose. A single member of the New South Wales Supreme Court refused to enjoin the site, focusing on the inability to confine the requested order to dissemination of the defamatory in New South Wales and the difficulty of enforcing any injunction against an absent defendant. The decision, thankfully, made no mention of the passive nature of the web site, but neither did it take into account the extent to which the site targeted a local bank. Any injunction against a site sponsor will inevitably deny access to the site globally; that cannot mean that no such regulation may ever issue.

The critical fact in *Calder*, the directing by the defendant of his activities to the forum state, sustains jurisdiction over claims other than libel or cyber-squatting, however. It provides the better U.S. constitutional justification for assertions of jurisdiction over sellers who advertise in the forum and ship their goods to buyers there: 124 the advertisements “target” the forum and, even if the seller did not intend to breach its contract or provide a negligently made product, it did intend to connect itself to residents of the forum.

Results under the Brussels Convention are the same. As already noted, 125 jurisdiction in tort claims is proper where the injury occurred. Section 4, articles 13 and 14, of Title II of the Brussels Convention expressly provide for jurisdiction in breach of contract claims at the domicile of the consumer 126 when the seller has advertised in the buyer’s domicile and the buyer took the steps necessary for the conclusion of the contract

123. [1999] NSW SC 526. See Mallesons, supra note 58, at 3.23-3.31, from which this paragraph is drawn.
124. See supra notes 106-07 and accompanying text.
125. See supra note 113 and accompanying text.
126. Article 13 defines a consumer as a person who enters into a contract “for a purpose which can be regarded as being outside his trade or profession.” Non-consumer contracts are best analyzed under *Burger King Corp. v. Ruizes*, 471 U.S. 462 (1985) and the Brussels Convention, supra note 33, tit. II, § 2, art. 5.
there. The consumer may only be sued for breach in her domicile, a result parallel to that generally presumed in the United States. 127

3.1.2.(c). Jurisdiction Based on Intentional Affiliation

Finally, the third situation in which a defendant, never physically present in the forum, may still be subject to jurisdiction there is that reflected by _Burger King Corp. v. Rudzewicz._ 128 Other Supreme Court adjudicatory jurisdiction cases had involved claims of tortious injury; _Burger King_ was at least the modern Court’s first attempt to resolve jurisdictional issues in the context of a claim for breach of contract. The defendant franchisee, a Michigan businessman, had allegedly breached his contract with Burger King, a Florida corporation. While the defendant had not been present in Florida in any way the Court considered jurisdictionally significant, and although he argued strongly that his contacts had been with the Michigan district office, the Court found that he had intentionally affiliated himself with a Florida entity in a way that satisfied _Hanson’s_ requirement. Determinative was a combination of factors: the defendant was seen as a sophisticated businessman who not only had solicited the franchise arrangement but also had actively negotiated its terms with Burger King’s Miami headquarters; the resulting franchise agreement was of high value, long-term, and closely supervised; the contract called for the use of Florida law to determine claims arising under it; and payments were to be made to the Miami headquarters. The failure to make those payments was the basis of the plaintiff’s claim.

The _Burger King_ Court specifically rejected what it termed “any talismanic jurisdictional formula[,]” 129 noting that its decision did not justify an assertion of jurisdiction over any party to a contract in the other party’s home state. 130 The fact that _Burger King_ involved a claim for breach of contract rather than damages caused by negligence in the end seems insignificant. The requirement of _Hanson_, that the defendant purposefully avail itself of the privilege of conducting activities in the state, thus invoking the benefits and protections of state law, must be satisfied; it may be satisfied by a non-present defendant; once it is satisfied, the propriety of an assertion of jurisdiction depends upon its reasonableness, _i.e._ upon the relationship between the defendant’s contacts with the state and the claim brought against her.

Just as the _Blumenthal_ court struggled with the _Calder_ analogy, the court in _CompuServe, Inc. v. Patterson_ 131 struggled with an obvious analogy to _Burger_

127. See supra note 107.
129. Id. at 485-86.
130. See, e.g., VCS Samoa Packing Co. v. Blue Continent Products (PTY) Ltd., 83 F. Supp. 2d 1151 (S.D. Cal. 1998) (contract between California plaintiff, who initiated the contact, and South African defendant for purchase of tuna to be delivered to plaintiff’s cannery in American Samoa insufficient to subject defendant to jurisdiction in California).
131. 89 F.3d 1257 (6th Cir. 1996).
King. CompuServe, a computer information service headquartered in Columbus, Ohio, sued defendant Richard Patterson, a resident of Houston, Texas who claimed never to have visited Ohio. In addition to being an attorney, Patterson did business as defendant FlashPoint Development, and in that capacity, marketed shareware.\textsuperscript{132} Patterson was both an individual subscriber to CompuServe and had entered into a “Shareware Registration Agreement” (SRA) with CompuServe. The SRA purported to create an independent contractor relationship between Patterson and CompuServe, whereby Patterson could place his software on the CompuServe system. The SRA incorporated by reference two other documents: the CompuServe Service Agreement (Service Agreement) and the Rules of Operation. Both the SRA and the Service Agreement expressly provided that they were entered into in Ohio.\textsuperscript{133} The Service Agreement further provided that it was to “be governed by and construed in accordance with” Ohio law.\textsuperscript{134} Although both documents were standardized agreements prepared entirely by CompuServe, the SRA specifically asked shareware providers like Patterson to type “AGREE” at various points in the document, “in recognition of your on line agreement to all the above terms and conditions.”\textsuperscript{135}

Between 1991 and 1994, Patterson electronically transmitted 32 master software files to CompuServe. These files were stored in CompuServe’s system in Ohio and were displayed in different services for CompuServe subscribers, who could download them and pay for them if they later decided to retain the programs. Patterson also advertised his software on the CompuServe system, noting the price term in at least one of his advertisements. Patterson alleged that he sold less than $650 worth of his software, to only twelve Ohio residents, via CompuServe.

One of the shareware programs Patterson marketed over CompuServe was intended to allow people to navigate around the Internet. CompuServe subsequently began to market a similar product. Patterson notified CompuServe by email that the terms “WinNav,” “Windows Navigator” and “FlashPoint Windows Navigator” were common law trademarks which he and his company owned. Patterson alleged trademark infringement and deceptive trade practices. CompuServe changed the name of its program, but Patterson continued to complain. Consequently, CompuServe filed suit in Ohio for a declaratory judgment that CompuServe had not infringed defendants’ trade names or otherwise engaged in unfair competition.

\textsuperscript{132} Shareware is software provided free of charge on the understanding that if the end user decides to retain the program after trying it out, the user will remit a predetermined (usually low) fee to the owner of the program.

\textsuperscript{133} The inclusion of this clause is a nice example of courts’ (and, therefore, parties’) preoccupation with where certain events take place.

\textsuperscript{134} 89 F3d at 1260.

\textsuperscript{135} Id. at 1261.
The Sixth Circuit held that CompuServe had made a prima facie showing that defendant’s contacts with Ohio were sufficient to support the exercise of personal jurisdiction. The court found that defendant purposely availed himself of the privilege of acting in Ohio or causing a consequence in that state, that the cause of action arose from the defendant’s activities in Ohio, and that the acts of the defendant or consequences of acts by him had a substantial enough connection with the forum to make the exercise of jurisdiction reasonable. Specifically, the Sixth Circuit found that “Patterson has knowingly made an effort—and, in fact, purposefully contracted—to market a product in other states, with Ohio-based CompuServe operating, in effect, as his distribution center.”

The Sixth Circuit concluded that Patterson himself took actions that created a connection to Ohio:

He subscribed to CompuServe, and then he entered into the Shareware Registration Agreement when he loaded his software onto the CompuServe system for others to use and, perhaps, purchase. Once Patterson had done those two things, he was on notice that he had made contracts, to be governed by Ohio law, with an Ohio-based company. Then, he repeatedly sent his computer software, via electronic links, to the CompuServe system in Ohio, and he advertised that software on the CompuServe system. Moreover, he initiated the events that led to the filing of this suit by making demands of CompuServe via electronic and regular mail messages.

The Sixth Circuit emphasized that Patterson had entered into a written contract with CompuServe which provided for the application of Ohio law, and he then purposefully perpetuated the relationship with CompuServe via repeated communications with its system in Ohio. The Sixth Circuit criticized the district court, which had dismissed the case for lack of personal jurisdiction, for focusing on Patterson’s status as a CompuServe subscriber (or purchaser of services), because his relationship with CompuServe was more complex; “he was a third-party provider of software who used CompuServe, which is located in Columbus, to market his wares in Ohio and elsewhere . . . . [T]his is Patterson’s relationship with CompuServe as a software provider and marketer that is crucial to this case.”

The Sixth Circuit wrote that the district court disregarded “the most salient facts of that relationship: that Patterson chose to transmit his software from Texas to CompuServe’s system in Ohio, that myriad others gained access to Patterson’s software via that system, and that Patterson advertised and sold his product through that system.” It also found

136. Id. at 1263.
137. Id. at 1264.
138. Id.
139. Id.
significant the fact that Patterson’s relationship with CompuServe was intended to be on-going, and not a “one shot affair.”

Echoing the U.S. Supreme Court, the Sixth Circuit emphasized that merely entering into a contract with CompuServe, without more, would not have been sufficient to establish specific jurisdiction over Patterson in Ohio. Because, however, Patterson had both entered into a contract with CompuServe and marketed his software through CompuServe and, because of the other factors in the case, the minimum contacts test was satisfied. The Sixth Circuit wrote that CompuServe, in effect, acted as Patterson’s distributor, “albeit electronically and not physically.” A single citation to Burger King would have justified the decision.

Under the Brussels Convention, the assertion of jurisdiction in Burger King would have been supported by Title II, section 2, article 5, which allows jurisdiction over a defendant in “the place of performance of the obligation in question”; the claim was a failure to pay monies owed to the Florida plaintiff, an obligation to be performed by the defendant in Florida. The result on the facts of CompuServe is difficult to determine but may not have paralleled the U.S. holding. Again, the civil law focus is not on contacts but on the locale of specified acts. Here the injury caused by Patterson’s attempt to prevent CompuServe from marketing its product could arguably have been felt in Ohio. On the other hand, the true injury could be seen as the alleged trademark infringement; jurisdiction would then be proper wherever the injury was felt. But in that view, the choice of forum would belong to Patterson; the fact that he was injured in Ohio would not serve to make him subject to jurisdiction there. In fact, the use of a declaratory judgment remedy by a traditional defendant does not fit well into the “Special Jurisdiction” category of the Convention. The Convention’s focus on the nature of the claim, tort or contract, makes it hard to apply to such suits.

3.1.3. Jurisdiction and the Internet

In part, the lack of clarity in lower court opinions in the United States simply reflects the lack of clarity in a doctrine that is highly fact specific, the key European criticism. In part, it may also result from the first re-

140. Id. at 1265 (quoting Southern Mach. Co. v. Mohasco Indus., 401 F.2d 374, 381 (6th Cir. 1968)).
141. Id.
142. Id.
143. The Tenth Circuit in Intercor, Inc. v. Bell Atlantic Internet Solutions, Inc., 205 F.3d 1244 (10th Cir. 2000), had less trouble drawing an analogy to CompuServe itself in holding that the continued, knowing, and unauthorized use of the plaintiff’s Internet access service by defendant was sufficient to sustain personal jurisdiction over it at the plaintiff’s home. The more obvious analogy, however, would have been to Calder.
144. Brussels Convention, supra note 33, tit. II, § 2, art. 5. Articles 13 and 14 of the Brussels Convention preclude use of similar logic when the defendant is a consumer.
ported decision involving the jurisdictional significance of an out-of-state web site accessible to forum residents, Inset Systems, Inc. v. Instruction Set, Inc.\textsuperscript{145} The decision was wrong, and is not now widely followed, but it left its mark. The defendant, Instruction Set, Inc. (ISI), was a Massachusetts corporation with its principal place of business in Massachusetts. ISI provided computer technology and support to thousands of organizations throughout the world, but it did not have any employees or offices in Connecticut or conduct any business on a regular basis in that state. Inset argued, however, that jurisdiction could be obtained over ISI under Connecticut’s long arm statute because “ISI has repeatedly solicited business within Connecticut via its Internet advertisement and the availability of its toll-free number.”\textsuperscript{146}

Inset had registered the federal trademark “INSET.” Thereafter, ISI obtained the inset.com domain name. ISI also used the telephone number “1-800-US-INSET,” which the court characterized as intending “to further advertise its goods and services.” Inset first learned of ISI’s registration of the inset.com domain name when it attempted to register the same domain name.

The court considered whether the assertion of jurisdiction over ISI would be consistent with due process. The plaintiff argued that the defendant had the minimum required contacts with Connecticut because it used the Internet, as well as its toll-free number, to try to conduct business in Connecticut. The court found that ISI’s Internet presence constituted purposeful availment:

In the present case, [ISI] has directed its advertising activities via the Internet and its toll-free number toward not only the state of Connecticut, but to all states. The Internet as well as toll-free numbers are designed to communicate with people and their businesses in every state. Advertisement on the Internet can reach as many as 10,000 Internet users within Connecticut alone. Further, once posted on the Internet, unlike television and radio advertising, the advertisement is available continuously to any Internet user. ISI has therefore, purposefully availed itself of the privilege of doing business within Connecticut.\textsuperscript{147}

Under this analysis, a company that maintained a web site could be subject to jurisdiction anywhere, because the Internet is widely accessible in every U.S. state and many foreign jurisdictions. While the operation of a web site may properly subject a defendant to jurisdiction in a far-flung location in appropriate cases, it did not evidence the defendant’s purposeful availment of the privilege of conducting business in Connecticut in

\textsuperscript{146}  Id. at 164.
\textsuperscript{147}  Id.
this case. There was no evidence presented in this case that the defendant selected the domain name inset.com—a legitimate abbreviation for Instruction Set, Inc.—with any knowledge of plaintiff’s use of the Inset name or trademark in Connecticut, or that the lawsuit—a domain name dispute—was related to any contacts (in the traditional sense) with the forum state. Unlike other domain name disputes, this was not a case where a defendant intentionally registered a plaintiff’s trademark, such that under Calder it could be said that the defendant committed a tort directed at a resident of the forum state.

The Inset analysis of what constitutes solicitation of business in Connecticut is overly simplistic for two reasons. First, while it may have been true that there were 10,000 sites in Connecticut from which the defendant’s web site could have been accessed, this evidence hardly suggests that any Connecticut residents in fact accessed ISI’s site, or, more importantly, that ISI intended specifically to solicit customers in Connecticut. While it is certainly true that information available over the Internet is more accessible, and available for longer periods of time, than traditional newspaper, television, or radio advertising, it is also the case that there is a much higher volume of information available over the Internet, such that the mere existence of a web site does not evidence that the information on the site in fact has been widely viewed. 148 Second, forum residents would have actively had to access the defendant’s out-of-state web site in order to obtain the information made passively available there by the defendant. By contrast, newspaper and television advertising is actively placed by companies intending to target specific customers and passively received by consumers.

Mere maintenance of a web site cannot subject a defendant to global jurisdiction if the new technology is to be capable of meaningful use. If each web site subjected its sponsor to global jurisdiction, many would forego use of the technology for fear of its secondary costs. If these costs were in practice nonexistent because judgments rendered by distant courts were not enforced by courts that could seize the person or assets of the defendant, an evolving and necessary system of internationally accepted jurisdictional principles would be undermined. 149 It, therefore, becomes

148. The extent to which a site is visited can actually be measured (and with the use of web cookies and other devices, the identity of certain users may even be discerned).

149. One decision by the British Columbia Court of Appeals does leave the impression that a web site makes a foreign defendant’s plea of lack of jurisdiction less likely to succeed; the site means the defendant has portrayed itself as an international actor. See Old North State Brewing Co. v. Newlands Services, Inc. [1998] 58 B.C.L.R. (3d) 144, discussed in Gates, supra note 62, at 3-4. The case itself, however, was simplistic and not dependent on Internet advertising; it involved the purchase and installation of equipment in the forum by the defendant, as well as losses suffered there by the plaintiff.

More troubling is another Canadian decision, Alteem v. Informix Corp., [1998] 79 A.C.W.S. (3d) 1157, decided by the Newfoundland Supreme Court. Newfoundland investors sued a California company for misrepresentation; jurisdiction was upheld because investment in-
necessary to determine what more must be found in order to satisfy the Supreme Court's requirement that a defendant invoke the benefits and protections of the forum. In the United States, the analytical framework supplied by *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.* has become the most frequently used by lower courts. In *Zippo*, District Judge McLaughlin, writing in early 1997, summarized earlier lower court opinions and explained that whether jurisdiction could be properly asserted in a case based on a defendant's Internet-related contacts should depend on the nature and quality of commercial activity that an entity conducts over the Internet.

At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise [of] personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.

In this view, jurisdiction cases fall somewhere on a "sliding scale" or "spectrum" where "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet."
The *Zip*po formulation was subsequently adopted by the Ninth Circuit in *Cybersell, Inc. v. Cybersell, Inc.*, a late 1997 decision which was also the first circuit court opinion to evaluate whether jurisdiction could be obtained over a defendant, consistent with due process, based solely on the defendant’s operation of a passive web site. In *Cybersell, Inc.*, the Ninth Circuit held that jurisdiction could not constitutionally be asserted simply because an out-of-state defendant operated a passive web site accessible to residents of the forum state. The site at issue displayed the name, logo, and local (as opposed to toll-free) telephone number of the defendant and included a link that invited visitors to submit their names to obtain additional information.

The court quoted *Zip*po for the proposition that “[c]ourts that have addressed interactive sites have looked to the ‘level of interactivity and commercial nature of the exchange of information that occurs on the Web site’ to determine if sufficient contacts exist to warrant the exercise of jurisdiction.” In finding that the defendant operated “an essentially passive home page on the web,” the Ninth Circuit did not actually focus on the site’s level of interactivity as much as on the more traditional analysis of the contacts between the defendant, the forum state and the underlying cause of action. The court stated “[w]hile there is no question that anyone, anywhere could access that home page and thereby learn about the services offered, we cannot see how from that fact alone it can be inferred that Cybersell FL deliberately directed its merchandizing efforts toward Arizona residents.”

153. 130 F.3d 414 (9th Cir. 1997). The Ninth Circuit did not expressly state that it accepted the *Zip*po court’s analysis, but analyzed the facts before it in terms of the three categories outlined there and expressly quoted *Zip*po’s analysis of interactive web sites.

154. The jurisdictional significance of maintaining a toll free number is questionable. Given the number of different area codes that may exist within a single metropolitan area and the frequency with which people travel on business, it is not unusual for small businesses that operate primarily within a single state (or even county)—such as real estate brokers and mortgage bankers—to maintain toll free numbers for the convenience of existing and potential clients.

155. 130 F.3d at 418.

156. The court wrote that:

*Cybersell FL did nothing to encourage people in Arizona to access its site, and there is no evidence that any part of its business (let alone a continuous part of its business) was sought or achieved in Arizona. To the contrary, it appears to be an operation where business was primarily generated by the personal contacts of one of its founders. While those contacts are not entirely local, they aren’t in Arizona either. No Arizonan except for *Cybersell AZ* ‘hit’ *Cybersell FL*’s web site. There is no evidence that any Arizona resident signed up for *Cybersell FL*’s web construction services. It entered no contracts in Arizona, made no sales in Arizona, received no telephone calls from Arizona, earned no income from Arizona, and sent no messages over the Internet to Arizona.*

*Id.* at 419.

157. *Id.*
“something more’ to indicate that the defendant purposefully (albeit electronically) directed his activity in a substantial way to the forum state” the court could not find jurisdiction proper based on the operation of a passive web site.158 “Otherwise, every complaint arising out of alleged trademark infringement on the Internet would automatically result in personal jurisdiction wherever the plaintiff’s principal place of business is located. That would not comport with traditional notions of what qualifies as purposeful activity invoking the benefits and protections of the forum state.”159 The court also emphasized, however, that in evaluating minimum contacts in Cyberspace, all contacts—including those occurring on terra firma—should be considered.160

Under the Zippo/Cybersell, Inc. guidelines, specific jurisdiction may be found where, in addition to operating a passive web site, a defendant has other contacts with the forum or where its Internet presence allows for some level of commercial interactivity. Mere advertisement on the web, without more, is insufficient to confer jurisdiction under this analysis.

Courts clearly are convinced that the nature of a defendant’s web site is relevant to the jurisdictional issue, but a failure to articulate why it is relevant makes it difficult to determine where the jurisdictional line should be drawn in cases that fall between Zippo’s two extremes. A recent opinion by Chief Judge Harry Edwards of the D.C. Circuit Court of Appeals provides a glimmer of guidance. GTE New Media Services, Inc. v. BellSouth Corp.161 involved the application of the District’s long arm statute, which required that, before asserting jurisdiction over a defendant whose activities outside the District had caused harm to a plaintiff there, the defendant either regularly do or solicit business there, engage in another persistent course of conduct there, or derive substantial revenue from goods used or consumed, or services rendered, there. The court was clear that merely because an interactive web site of the defendant was available to District residents, the defendant was not, therefore, automatically subject to the District’s jurisdiction. It is not the nature of the site per se that is critical. In certifying its jurisdictional decision for appeal, the district court in GTE had noted that other cases basing jurisdiction on an interactive site had involved defendants with other contacts with the forum related to the cause of action.

To understand why interactivity is relevant, it is necessary to refer back to basic jurisdictional theory. Jurisdiction is about chosen contacts between the defendant and the forum. This is the premise of World-wide Volkswagen. Of course, the seller of an automobile could reasonably foresee that the vehicle would be driven in a state other than the one in which it was sold

158. Id. at 418.
159. Id. at 420.
160. Id. at 419.
161. 199 F.3d 1343 (D.C. Cir. 2000).
and that, therefore, injury arising from its negligent preparation could occur elsewhere. The seller, however, had no control over where the vehicle was taken by the owner and thus no way to prevent his “contact” with the forum. In much the same way, the sponsor of a passive web site has no way to control which fora she is “connected to” by the site. On the other hand, the site sponsor who does business electronically knows or can take reasonable steps to discover the location of the party with whom she is interacting. The provision of an interactive site, alone, may express the sponsor’s willingness to become connected to all fora in which the site is accessible (assuming it does not contain any disclaimers etc.) but it does not constitute that connection.\(^{162}\) Nor, of course, does the mere accessing of the site by forum residents.\(^{163}\) Once the interactive site is engaged, the defendant can no longer argue persuasively that he did not choose to become connected to the forum of the other party. He may not have intended whatever consequences the plaintiff alleges flowed from that connection, but while that may defeat certain substantive claims against him (libel and trademark infringement, for example) it does not defeat the jurisdictional relevance of the connection.

Reliance, then, on the nature of the web site alone is misplaced. If an interactive site is not targeted to a specific forum,\(^{164}\) courts should focus on how the site is actually used. Knowing and willing use of it by a non-present party to enter into dealings with persons or businesses in the forum demonstrates a chosen contact with the forum, provides the forum with an interest in the relationships thus created, and makes it less likely that

\(^{162}\) This was the insight of the court in *Millennium Enterprises, Inc. v. Millennium Music LP*, which refused to conflate the potential of doing business on an interactive site with citizens of the state with actually doing such business. 33 F. Supp. 2d 907 (D. Or. 1999). See also Rothschild Berry Farm v. Serendipity Group LLC, 84 F. Supp. 2d 904 (S.D. Ohio 1999) (interactive site not utilized by forum residents (in fact, after motion to dismiss for lack of personal jurisdiction was filed, the defendant did receive one apparently unrelated request for sale, which it refused to fill) insufficient to sustain an assertion of personal jurisdiction in a trademark infringement claim).

\(^{163}\) Following the opinion in *Insot*, the court in *Maritz, Inc. v. CyberGold, Inc.*, found relevant the number of “hits” on the defendant’s site by forum residents. 947 F. Supp. 1328 (E.D. Mo. 1996). The case involved trademark infringement, so the number of Missouri residents who saw the site, and thus the injury to the plaintiff in Missouri, was important. However, there are two problems. In the first place, there was no indication that the defendant intentionally sought to infringe the trademark, the issue the *Benswan* court found dispositive. Second, the numbers are unreliable and ultimately unhelpful. Not all addresses (which is how those who come to the site are identified) are geographically located; not all those who visit a site do so from their own address; not all addresses may belong to different visitors. Finally, the number of visitors from a given forum, even if known, really doesn’t say anything about the importance of that forum to the site sponsor. In *CyberGold*, the court was swayed by 131 hits from Missouri. The significance of the number is unclear.

\(^{164}\) If a site is so targeted, the forum may assert jurisdiction over its author and its contact, pursuant to *Asahi* and *Calder*. 
multiple fora with different applicable laws will attempt to regulate the site and assert jurisdiction over its sponsor.

To date, apparently no other country has focused on the degree of a site's interactivity in assessing jurisdiction. In part, this may reflect the relative lack of case law outside the United States dealing with electronic commerce. But in part its irrelevance may be systemic; if the central issue is where acts occurred rather than what choices a defendant has made, interactivity would be relevant only in determining whether, for example, a transfer of digital property was “performed” at the seller’s or buyer’s terminal.165

3.1.4. General Jurisdiction

All the situations discussed thus far involve assertions of what is called “specific” or “special” jurisdiction. The contacts the defendant has with the forum or certain acts there are sufficient to permit jurisdiction to be asserted with respect to related claims but are presumptively insufficient to permit jurisdiction to be asserted with respect to claims that have no relationship to those contacts or acts.166 “General” jurisdiction, on the other hand, describes jurisdictional assertions which are proper no matter what the claim brought against the defendant is because of the substantiality and nature of the defendant’s contacts with the forum. The easiest example is that of a state asserting jurisdiction over one of its own domiciliaries. If a domiciliary of Illinois contracts with a domiciliary of Indiana for the provision of services in California, the Indiana plaintiff could institute suit in California, where the services were to be performed, but for convenience might well prefer to bring suit closer to her home. Jurisdiction over the Illinois domiciliary in Indiana would not be proper, because the defendant has no contacts with that forum and the contractual perfor-

165. The difficulty in sensibly “locating” acts in Cyberspace was at the center of one of the seminal articles on jurisdictional issues in this new era. David R. Johnson & David Post, Law and Borders—The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367 (1996).

166. There is a difference between claims that are related to a defendant’s contacts with the forum and those that arise from the contacts. In the latter instance, the contact is itself an element of the claim; jurisdiction is then clear. A good example is Keeton v. Hustler Magazine, Inc., a libel suit in which the defendant argued that the plaintiff’s close-to-total lack of contact with the forum and its own negligible sales there ought defeat jurisdiction. 465 U.S. 770 (1984). The Court, however, held that the claim arose out of the sale of magazines in the state and jurisdiction was, therefore, proper. By contrast, when the defendant’s contact with the forum state is via the stream of commerce, a claim for tortious injury there caused by the product is related to but does not arise out of the forum contact. Without the defendant’s use of the stream of commerce, the final product would not have been purchased by the plaintiff in the state; however, it is an alleged negligent act elsewhere that allegedly makes the defendant liable to the plaintiff for damages. In this fact pattern, jurisdiction might be defeated if other factors make the forum a less “reasonable” one, for example if the injury occurred outside the state, so that witnesses and evidence were not easily available in the state in which the purchase had taken place.
mance was not to occur there, but an assertion of jurisdiction by Illinois would be consistent with due process.\textsuperscript{167}

In the United States, whether general jurisdiction is proper when the defendant has “continuous and systematic” contact with the state but is not a citizen of the state is a matter of debate. The Supreme Court since 1945 has decided two cases which it believed raised the issue. The first, \textit{Perkins v. Benguet Consolidated Mining Co.},\textsuperscript{168} permitted Ohio to exercise jurisdiction over a Philippine mining company that had its (sole) U.S. office in that state in a cryptic opinion that merely concluded that the assertion was “reasonable and just,” although the claim did not relate to the activities in Ohio. At the time suit was brought, however, the Philippines were occupied by Japan, which was at war with the United States. Therefore, if jurisdiction in Ohio was not proper, there would literally be no forum in which the plaintiff could proceed.

More recently, in \textit{Helicopteros Nacionales de Colombia, S.A. v. Hall},\textsuperscript{169} the Court found that Texas could not constitutionally assert jurisdiction over a Colombian corporation in a claim arising out of a Peruvian helicopter crash. Although Justice Brennan dissented, the majority of the Court agreed that the claim was not relevantly related to the contacts between the defendant and Texas.\textsuperscript{170} Those contacts included negotiating the contract pursuant to which the defendant provided the transportation service being used at the time of the crash, the purchase of the helicopter involved (as well as eighty percent of the defendant’s entire fleet of helicopters) from a Texas corporation, and the training of the defendant’s pilots in Texas. The majority held, however, that “mere purchases, even if occurring at regular intervals”\textsuperscript{171} were insufficient to support the assertion of

\textsuperscript{167} See, e.g., Blackmer v. United States, 284 U.S. 421 (1932) (absent citizen of the United States subject to the jurisdiction of courts of the United States); Milliken v. Meyer, 311 U.S. 457 (1940) (absent citizen of a state subject to the exercise of personal jurisdiction by courts of the state). See also Brussels Convention, supra note 33, tit. II, § 1, art. 2; ODA, supra note 96, at 395.

There are some technical differences between the United States, the E.U., and Japan, however. In the United States, citizenship is a sufficient basis of jurisdiction even if the defendant is domiciled elsewhere; under article 18 of the draft Hague Convention, supra note 58, nationality of a defendant is a prohibited ground of jurisdiction. Furthermore, both Europe and Japan apparently equate domicile and habitual residence; in the United States an individual “habitually resident” in one state may retain her domicile in another state if she intends to return there. No Supreme Court case has found jurisdiction proper in that situation, but domicile combined with U.S. citizenship is the generally accepted test for state citizenship.

\textsuperscript{168} 342 U.S. 437 (1952).
\textsuperscript{169} 466 U.S. 408 (1984).
\textsuperscript{170} \textit{Id.} at 416.
\textsuperscript{171} \textit{Id.} at 418. In support of its holding, the majority cited \textit{Rosenberg Bros. & Co. v. Curtis Brown Co.}, 260 U.S. 516 (1922), a pre-\textit{Shoe} case involving an attempted assertion of personal jurisdiction by New York over an Oklahoma retail purchaser of men’s clothing. The Court specifically noted that it was not determining whether, on similar facts today, an exercise of
general jurisdiction. The activity described in the case is quite clearly continuous and systematic, so presumably the difficulty lies in its "substantiality and nature." The majority pointed out that the defendant did not have a place of business in the state, nor was it licensed to do business there. The latter point would seem of greater relevance to an argument that the defendant had previously consented to the assertion by Texas of jurisdiction; a license to do business says nothing at all about the business actually done in the state. On the other hand, the lack of any actual place of business in the state means that the defendant cannot be characterized as a "resident" of Texas.

A resident of a state, unlike one who simply has continuous dealings with others in the state, has entered into a permanent relationship with the forum. The "nature" of that relationship is distinct. It may be inferred from *Helicopteros* that general jurisdiction requires such permanence, as it is difficult to imagine a business relationship absent residence stronger than that which bound the defendant to Texas. Assuming, however, that residency or at least a permanent presence in the state is necessary before general jurisdiction may be asserted, it is not clear that is all that is necessary. New York, for instance, assumes that it is; Maryland assumes it is not. Arguably, *Shoe* supports the need for further inquiry. That case, after all, referred to not only the nature but also the substantiality of the continuous and systematic contact necessary to support jurisdiction when the claim is not related to the activity.

In addition, New York's position results in nation-wide general jurisdiction with respect to large national corporations with offices in every state. There seems to be no policy justification for that result; why should a California plaintiff alleging a breach of contract claim against State Farm entered into and to be performed in California be able to sue in Idaho? The burden on the defendant is also a heavy one, because witnesses, evidence, applicable law etc. are all likely to be in the state where the claim arose. If the suit is brought in the defendant's state of citizenship, the practical inconveniences are thought to be outweighed by the generic con-

specific jurisdiction over the defendant would be permissible; the *Rosenberg* holding was that the defendant was not "present" in New York by virtue of its purchases, so as to subject it to jurisdiction there under the logic of *Pennoyer*.

172. Ownership of real property in the state, for instance, may not be the equivalent of residency; residency is possible without ownership, and ownership need not include use of the property. However, it too provides a permanent connection to the state; arguably the jurisdictional implications of that connection are best considered here rather than as an analogy to the holding of the Court in *Burnham* regarding jurisdiction based on the personal service of process on a defendant present in the forum.


venience of being sued "at home;" also, given the complexities of the law of personal jurisdiction, it seems appropriate that there be one forum in which a plaintiff can be assured that the defendant is amenable to service of process. But one such state is sufficient.

This issue is not subject to debate under the Brussels Convention or in Japan, although its resolution pursuant to those laws is different. Article 5(5) of the Brussels Convention makes it clear that only disputes arising out of the operations of a branch, agency, or other establishment, i.e., of a residence as opposed to principal place of business, can be brought in the forum. Japan, on the other hand, requires foreign companies that conduct business there on a continuous basis to register a place of business and a representative; because the company’s principal place of business is outside Japan, this residence suffices for an assertion of general jurisdiction.

For the most part, courts are in agreement that the maintenance of a web site outside the forum, even when coupled with sales into the forum, is insufficient to sustain an assertion of general jurisdiction. In light of the Court’s decision in Helicopteros, this conclusion must be correct. Apparently, only one case has found an assertion of general jurisdiction over a non-resident defendant to be properly based, in part, on its Internet contacts with the forum. In Mieczkowski v. Masco Corp., the court asserted jurisdiction over a North Carolina manufacturer of a children’s bed, although the bed which had allegedly caused the death of the plaintiff’s son had been sold by the defendant to a third party in Washington, D.C., who thereafter sold it to the plaintiff in Virginia. The defendant had, however, apparently sold the same product to Texas residents and maintained a web

175. While courts generally assume that a corporation is a citizen of both its state of incorporation and the state of its principal place of business for purposes of general jurisdiction (these being the states of corporate citizenship for purposes of diversity jurisdiction under 28 U.S.C. § 1332), this convenience argument might logically be used to defeat jurisdiction based solely on state of incorporation. While many corporations are incorporated in Delaware, that frequently is their only contact with the state and, at least with respect to claims unconnected to Delaware law (for example, a California breach of contract claim), Delaware does not seem intuitively to be a “reasonable” forum.

176. The harshness of the assertions of general jurisdiction over a defendant in multiple fora based on its multiple residences may, of course, be reduced through use of the doctrine of forum non conveniens. Indeed, the doctrine’s most frequent use is in situations in which the claim brought against the defendant is totally unrelated to its activities in the forum. However, there are significant differences between a constitutional protection and a discretionary one. See generally Margaret G. Stewart, Forum Non Conveniens: A Doctrine in Search of a Role, 74 CAL. L. REV. 1259 (1986).

177. ODA, supra note 96, at 395. See also Joseph W.S. Davis, Dispute Resolution in Japan, Kluwer Law International (1996) [hereinafter Davis], at 195-201. Australia also permits such assertions. Mallesons, supra note 58, § 2.6.


site from which its products could be ordered. While the plaintiff’s claim clearly had nothing to do with those contacts, clearly also an identical claim could have arisen from the sale of a bed to a Texas resident; the court’s jurisdiction over that claim would have been unquestioned. Given that the burden of defending the plaintiff’s suit was no different than the burden of defending a suit arising from the sale of a bed in Texas which the defendant had already assumed, arguably due process was not offended by the assertion of general jurisdiction. In one sense, this is not “true” general jurisdiction, but a limited variety of it which is justified by the similarity between the actual claim and the specific jurisdiction which could be asserted.\textsuperscript{180}

In one other situation in the United States, jurisdiction may be asserted against a defendant who lacks contacts with the forum relevant to the claim. In 1990, a unanimous Supreme Court held in \textit{Burnham v. Superior Court}\textsuperscript{181} that jurisdiction was proper when the defendant was personally served with process while in the forum (so-called “tag” jurisdiction), although why that was so fractured the Court. Writing for himself and three others, Justice Scalia held that \textit{Shoe} was meant to expand, not contract, the availability of jurisdiction and was directed to the propriety of jurisdictional assertions over nonpresent defendants. In his view, the acceptance of personal service in the forum as a basis of jurisdiction at the time of the adoption of the Fourteenth Amendment and its continuing acceptance today made it obvious that the assertion of such jurisdiction comported with the “traditional notions of fair play and substantial justice” at the heart of the \textit{Shoe} opinion.\textsuperscript{182} Four other justices believed that minimum contacts analysis was required but that the defendant had such contacts with the forum because his presence there constituted purposeful availing of the benefits and protections of the state’s laws, the burden of defending there was slight, and the defendant could anticipate the assertion of jurisdiction.\textsuperscript{183} Justice Stevens said, “this is, indeed, a very easy case.”\textsuperscript{184} In any event, this basis of jurisdiction is unchanged by technol-

\begin{footnotesize}
\begin{enumerate}
\item See Buckeye Boiler Co. v. Superior Court, 458 P.2d 57 (Cal. 1969).
\item 495 U.S. 604 (1990)
\item Although seizure of property located in the forum at the commencement of the lawsuit had also been a traditional basis of jurisdiction, the Court had previously rejected its continuing validity in \textit{Shaffer v. Heiner}, 433 U.S. 186 (1977), requiring an analysis under \textit{Shoe} of the relationship between the contact exemplified by the presence of the property and the plaintiff’s claim. This, Justice Scalia argued, didn’t negate the validity of jurisdiction based on service in the forum; minimum contacts are required for all nonpresent defendants. 495 U.S. at 620-21.
\item Justice Scalia was unimpressed. He noted that the first two prongs of the argument would hold true whether or not the defendant had been personally served while in the forum and that the third is simply another way of stating Scalia’s own reliance on tradition. \textit{Id.} at 622.
\item \textit{Id.} at 640 (Brennan, J., concurring).
\end{enumerate}
\end{footnotesize}
ogy; the requirement is personal service on the real, not virtual, person of the defendant in the forum.

Under the Brussels Convention, tag jurisdiction is prohibited by article 3. That article itself, however, reveals that the national laws of many of the contracting states do permit its assertion.\(^{185}\)

### 3.1.5. Contractual Choice of Forum

Finally, the complexities of the law of personal jurisdiction in cases involving electronic commerce may, in some instances, be obviated by prior agreement between the parties, just as they have been historically. Such agreements may simply express a party's consent to be sued in a specific forum (usually the home of the other party),\(^{186}\) or it may identify the only forum in which litigation concerning the contract shall be filed.\(^{187}\) In either instance, there may be difficulty with respect to the validity of the agreement under the applicable law of contract, but if contractually valid they govern the location of the litigation. In business-to-business contracts, choice of forum clauses are generally enforced in the United States,\(^{188}\) the E.U.,\(^{189}\) and Japan.\(^{190}\) Their validity, however, may be problematic when one party is a consumer.

Many contracts between consumers and vendors (both off-line and on-line) are not negotiable and are drafted by the vendor. Consumer advocates and consumer protection agencies will want to ensure that, to the extent online contracts are premised on unequal bargaining power and pressure to buy (or violate fundamental public policy), provisions of these contracts can be overridden by local law.

Under U.S. law, "adhesion contracts" (unilaterally-drafted form agreements) are enforceable absent a finding of "unfairness" or "unconscionability." Both of these latter terms are susceptible to many meanings. "Unfairness" often means that the weaker party is not in a position to shop around for better terms, or that the weaker party is so bereft of bargaining power that he or she has no real choice. "Unconscionability" often means that terms that are grossly unreasonable in light of the mores and business practices of the time. A finding that a given contract is a contract of adhesion is the beginning of the analysis, not the end, and courts try to distinguish enforceable adhesion contracts from unenforceable ones.

\(^{185}\) See generally Jurisdictional Salvation, supra note 90.


\(^{189}\) Brussels Convention, supra note 33, art. 17.

\(^{190}\) Davis, supra note 177, at 197.
As previously noted, such clauses are not enforced in European countries in business-to-consumer transactions unless they favor the consumer. Australia also is more reluctant to enforce such clauses against consumers than it is when the objecting party is a business, particularly in the international context when, absent such a clause, Australian consumer protection laws would apply.

Japan, on the other hand, will enforce such clauses unless they are “too unreasonable and contrary to public policy.”

The U.S. Supreme Court opinion upholding such a contractual clause, Carnival Cruise Lines, Inc. v. Shute, involved Washington passengers on a cruise that departed from California; the contract (found on the back of the ticket) chose Florida as the exclusive location for litigation and was upheld. Interestingly, however, the Court did not simply rely on a prior case upholding such a clause in an international contract between two businesses. Instead, it noted, but distinguished, the Bremen's recognition that “the serious inconvenience of the contractual forum to one or both of the parties might carry greater weight in determining the reasonableness of the forum clause.” While the U.S. home forum of a seller may be presumptively reasonable in a dispute with a U.S. consumer (although in Carnival Cruise Lines, the reasonableness of Florida was enhanced because the accident that gave rise to the lawsuit occurred off the coast of Mexico), its reasonableness may not be as apparent if the consumer is domiciled abroad; similarly, U.S. courts might be reluctant to find the choice of a

191. See supra note 72 and accompanying text. See also Tosi, supra note 72.

Brazil, Colombia and Uruguay also limit the enforceability of contractual choice clauses. In Brazil, if the defendant is domiciled in the country, if the contractual obligation is to be performed there, or if the dispute arises from matters occurring or practiced there, Brazilian courts will assert jurisdiction. See Noronha Advogados, A Brazilian Perspective § 5.1.2 [hereinafter Advogados] <http://www.kentlaw.edu/cyberlaw/docs/foreign/>. Colombia will not enforce such a clause if the contract is to be executed there, unless the choice falls under the New York Arbitration Convention. See Luisa Gamboa, Colombian Comments [hereinafter Gamboa] <http://www.kentlaw.edu/cyberlaw/docs/foreign/>. Uruguay simply does not recognize such clauses at all. See Guyer & Regules, Answers to the Requested Questions: Uruguay <http://www.kentlaw.edu/cyberlaw/docs/foreign/>. Neither does the national law of France in cases involving consumers (applicable when the dispute is not subject to the Brussels Convention). See James A. Graham, Comments to the Proposed Draft by the ABA <http://www.kentlaw.edu/cyberlaw/docs/foreign/>.

192. See Mallesons, supra note 58, at 3.58-3.60.

193. Davis, supra note 177, at 197.


196. The M/S Bremen v. Zapata Off-Shore Co., 407 U.S. 1 (1972) (enforcing a contractual choice of the London Court of Justice with respect to a suit between an American and a German Company concerning the towing of a drilling rig from Louisiana to Italy).

197. 499 U.S. at 594 (quoting M/S Bremen v. Zapata Off-Shore Co., 407 U.S. 1, 17 (1972)).
foreign seller’s home reasonable in a contract featuring a U.S. consumer. It is at least possible that, in the international context, the positions of the United States and other countries are not as far apart as they presume.

3.2. Prescriptive Jurisdiction

3.2.1. Constitutional and Other Local Restraints

Prescriptive jurisdiction is the authority of a state to apply its own law to regulate conduct. Clearly, this is critical to the global nature of electronic commerce and the protection of consumers, but it is particularly germane to industries such as banking and securities which are highly regulated. When such jurisdiction is asserted, entities (juridical persons) subject to that law are compelled to comply with it; failure to do so leads to litigation, enforcement or incarceration, which may involve a dispute about the jurisdiction itself.

While frequently a court capable of asserting personal jurisdiction over a defendant will also properly be able to apply local law to the dispute, there are situations in which such conjunction does not exist, either because the basis of personal jurisdiction is unrelated to activities in the forum related to the claim or because another state has a manifestly greater interest in the dispute recognized by the forum.

In the United States, two constitutional provisions are frequently thought to be relevant to the question of whether a state may exercise prescriptive jurisdiction: due process and the full faith and credit clause. In fact, only the former restrains a state’s choice to apply its own law. Full faith and credit does require the courts of one state to recognize and apply the substantive law of another state when the forum state has no law of its own to apply. It does not appear, as a matter of U. S. constitutional law, that either the due process clause or the full faith and credit clause prohibits a state from preferring its own law to that of a sister state when the forum state has both prescriptive jurisdiction and substantive law to apply. Any other reading would prevent a state from using its own law whenever that of another state could constitutionally apply, an irrational result that the Supreme Court has never required. If forum state


199. U.S. CONST. art. IV, § 1. “Full Faith and Credit shall be given in each State to the public Acts, Records, and judicial Proceedings of every other State.” This clause is most familiar to U.S. lawyers because of its requirement that one state enforce a valid judgment of another state, but by its terms it also defines the recognition one state must give to another’s laws.

200. The precepts of international law, according to section 403 of the Restatement (Third) of Foreign Relations Law of the United States, may require one state to abstain from applying its own law when another state has a stronger claim to the application of its law, as explained later in this section of the Report. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES Report 403 (1986) [hereinafter RESTATEMENT (THIRD)]
law is not applicable, however, whether because its choice is constitutionally precluded by the due process clause or because the law on its own terms is not applicable, the full faith and credit clause does prevent a state from refusing to accept otherwise proper adjudicative jurisdiction merely because the claim is to be decided under the law of another state.\textsuperscript{201}

The restriction imposed on a state’s assertion of prescriptive jurisdiction by due process is easily met. There must be a reasonable connection between the state and the transaction.\textsuperscript{202} Rarely is such a connection lacking; indeed, the Supreme Court’s jurisprudence with respect to this due process limitation is conspicuously undeveloped in comparison with its complex personal jurisdiction matrix.\textsuperscript{203} In \textit{Allstate Insurance Co. v. Hague},\textsuperscript{204} for example, Allstate had insured a Wisconsin citizen killed in a Wisconsin car accident; the deceased’s widow moved to Minnesota after the accident, was appointed there as his personal representative, and sued there for a declaratory judgment of the defendant’s liability on the policy, which had been issued in Wisconsin. Minnesota was permitted to apply Minnesota law to determine liability. Relevant contacts included the fact that the deceased had worked in Minnesota, Allstate was doing business in the state, its alleged obligation was to a current resident of Minnesota, and Allstate could not legitimately have expected only Wisconsin law to apply to the policy (had the accident occurred outside of Wisconsin or had the

\textsuperscript{201} Hughes v. Fetter, 341 U.S. 609 (1951). This case neatly demonstrates the disjunction between subject matter jurisdiction and prescriptive jurisdiction, a line recently blurred by a majority of the Supreme Court in \textit{Hartford Fire Insurance Co. v. California}, 509 U.S. 764 (1993). State courts are presumed to have subject matter jurisdiction over private transitory (versus purely local) claims; federal courts have similar jurisdiction in diversity cases. Whether the state law of the state in which the court sits may be used or not does not affect the existence of that jurisdiction. If either a private or public nonfrivolous claim is brought in federal court because the plaintiff alleges it arises out of federal law, and the court determines that law is inapplicable, the case should be dismissed for failure to state a claim upon which relief may be granted, not for lack of subject matter jurisdiction.

\textsuperscript{202} Home Ins. Co. v. Dick, 281 U.S. 397 (1930). The case involved an attempt by Texas to use its statute of limitations in deciding an insurance claim between Mexican parties based on a policy issued in Mexico covering a vessel in Mexican waters. The attempt was held to violate the defendant’s right to due process by increasing its obligation to the plaintiff under a law that had no connection to the claim. (The plaintiff was a Texas citizen who had been assigned the claim against the insurance company.) \textit{See also} Phillips Petroleum Co. v. Shutts, 472 U.S. 797 (1985).

\textsuperscript{203} The Court’s apparent reluctance to impose meaningful restraints on a state’s assertion of prescriptive jurisdiction may have contributed to the strictness with which it reviews assertions of personal jurisdiction. In \textit{Hanson v. Denckla}, 357 U.S. 235 (1958), had the court of Florida been able to obtain jurisdiction over the Delaware trustee it would have utilized Florida law to find that the trust agreement, entered into by a then-citizen of Pennsylvania and the Delaware bank, was invalid under Florida law (it had been “republished” there when the grantor had exercised her power of appointment under the trust agreement). Clearly, use of Florida law to determine the validity of an agreement entered into in Delaware is not intuitively logical, but it is constitutional.

\textsuperscript{204} 449 U.S. 302 (1981).
deceased moved from Wisconsin prior to his death another state’s law could obviously have applied. Just why these contacts were relevant to anything other than the convenience of the plaintiff is unclear; in dissent, Justice Powell argued that to be sufficient the contacts must form a link between the litigation and state policy.\textsuperscript{205} 

One other constitutional doctrine provides an additional, Court-imposed restraint on a state’s exercise of prescriptive jurisdiction in the context of taxation. The so-called “dormant” commerce clause prevents a state from unduly impeding the free flow of commerce across state lines by extending its law unreasonably to out-of-state conduct.\textsuperscript{206} 

Given the wide variety of conduct over which a state may constitutionally exercise control, it is frequently necessary for a state to determine whether its law or that of another state is applicable. The doctrine utilized to make such a determination is known as choice of law. Choice of law rules, however, are themselves informed by international law restraints. While a state court, for example, would not ordinarily determine whether its local law violated international restraints, the law-giver presumably would.

Although Joseph Story treated conflict of laws as a subject of international law\textsuperscript{207} and today the subject is often referred to as “private international law,” it is local or—as international lawyers say, “municipal”—in an important respect. The choice of law rule that determines whether the substantive law of another sovereign is applied to a particular controversy is the law of the forum. The analysis used depends on the choice of law doctrine of the sovereign in which the court deciding the case sits. When two states may legitimately exercise prescriptive jurisdiction over the same transaction or conduct, and the contents of the laws emanating from the two sovereigns differ, a tribunal deciding a dispute related to the transaction or conduct must choose which law to apply. If another sovereign purports to apply its substantive law to aspects of a controversy, and that application exceeds the extent of prescriptive jurisdiction permitted by international law, a second sovereign is unlikely to recognize the first sovereign’s law as regulating the controversy.

Finally, before turning to a discussion of those international restraints and their reflection in various conflicts of laws doctrine, it must be noted that the terminology used in much conflict of laws writing can be confusing. Conflicts writers usually talk about the jurisdiction of “courts,” and

\textsuperscript{205} Id. at 334.

\textsuperscript{206} See Hunt-Wesson, Inc. v. Franchise Tax Bd. of Cal., 120 S. Ct. 1022 (2000). This clause operates primarily as a restriction on a state’s ability to impose a sales tax on an out-of-state seller. Before it may do so, the sale must have, \textit{inter alia}, a “substantial nexus” with the state, Complete Auto Transit, Inc. v. Brady, 430 U.S. 274 (1977), which in turn requires a physical presence of the vendor in the state. National Bellas Hess, Inc. v. Department of Revenue, 386 U.S. 753 (1967). Canada also requires a fixed physical base. See Gates, supra note 62, at 5.

\textsuperscript{207} \textbf{JOSEPH STORY, CONFLICTS OF LAWS} 1 (8th ed. 1883) [hereinafter \textit{STORY}].
assess the relationship between “parties” and states. The practices of many lawyers, and many jurisdiction problems, involve not the regular courts, but administrative agencies, and not parties in the sense of corporations or individuals, but regulators. It is important to understand that all of the analysis in this report relating to the jurisdiction of courts also applies to administrative agencies, and that parties include agencies and government officers as well as private citizens and corporations.

Few agency decisions refer explicitly either to personal jurisdiction or to choice of law. When jurisdictional problems arise, they typically are addressed as “subject matter jurisdiction” problems. Nevertheless, there is an important linkage between jurisdiction and choice of law in the judicial context and agency decision making.

First, the subject matter jurisdiction of administrative agencies often is defined by statute in terms of geography. When that is the case, an

208. Rare exceptions in the communications field are In the matter of Western Union Telegraph Co., 75 F.C.C.2d 461 ¶ 18, 1979 WL 43964 (1979) (finding “personal jurisdiction” over Western Union’s implementation of new services through facilities outside geographic confines of United States because commission had jurisdiction over Western Union as a carrier); In the matter of Metropolitan Theatres Corp., 85 F.C.C.2d 1004 ¶ 6, F.C.C. 81-132 (1981) (using choice of law principles to apply state law to question of corporate law); and in the labor field Davis Electrical Constructors, Inc. v North Carolina State Building and Construction Trades Council, 291 NLRB No. 17, 291 NLRB 115, 1988 WL 214147, **31 (finding no personal jurisdiction over non party to permit requested remedy); Alexander Milburn Co. v United Electrical, Radio & Machine Workers, 78 NLRB 747, 1948 WL 7782 (1947) (adjudicating claimed lack of personal jurisdiction because of faulty service); West India Fruit & Steamship Co. v Seafarers International, 130 NLRB 343, 353, 1961 WL 15253, Case No. 15-CA-1454 (1961) (applying choice of law concepts from Lauritzen v. Larsen, 345 U.S. 571 (1953), to determine effect of foreign registry).

Securities decisions are an exception. A Westlaw search on 30 January 2000 of the FSCC-ADMIN database found 598 documents using the phrase “personal jurisdiction.” A search of the same database for the phrase “choice of law” identified 40 documents.

209. But see supra note 201.

210. The term “commerce” means trade, traffic, commerce, transportation, or communication among the several States, or between the District of Columbia or any Territory of the United States and any State or other Territory, or between any foreign country and any State, Territory, or the District of Columbia, or within the District of Columbia or any Territory, or between points in the same State but through any other State or any Territory or the District of Columbia or any foreign country.


The provisions of this Act shall apply to all interstate and foreign communication by wire or radio and all interstate and foreign transmission of energy by radio, which originates and/or is received within the United States, and to all persons engaged within the United States in such communication or such transmission of energy by radio, and to the licensing and regulating of all radio stations as hereinafter provided.

47 U.S.C. § 152(a) (1994) (Federal Communications Act);

‘Commerce’ means commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such
assessment of subject matter jurisdiction often becomes an assessment of
the scope of application of the agency’s substantive law, a subset of pre-
scriptive jurisdiction or choice of law analysis.

Second, as to personal jurisdiction, agencies cannot use coercive means
of enforcement on their own, except in the limited set of cases involving
license revocation or termination of governmental benefits. In all other
situations, agencies must go to court to seek coercive means of enforce-
ment. When they go to court, personal jurisdiction questions may arise.
So although the agency itself may not consider personal jurisdiction ques-
tions, those will arise later, in the context of judicial litigation.

3.2.2. The Restraint of International Law

While the U.S. Supreme Court has never held that the Constitution
precludes an assertion of jurisdiction in violation of international law,\(^{211}\) it has long held that congressional legislation is presumed to be enacted
in accordance with that law and will be interpreted in violation of it only
if no other recourse is open to the court.\(^{212}\) A second canon of statutory
construction, reflecting an original principle of international law, is that
congressional enactments are presumed to apply only to conduct under-
taken within the territory of the United States.\(^{213}\) Instances in which this
second presumption are overcome exceed those in which the first is turned
aside, presumably in large measure because international law itself has
come to acknowledge the propriety of certain assertions of jurisdiction
beyond the territory of the regulating sovereign.\(^{214}\)

Territory and another, or between any such Territory and any State or foreign nation,
or between the District of Columbia and any State or Territory or foreign nation.


211. Similarly, the Australian constitution does not itself limit the extraterritorial reach
of the Australian parliament, although Australia does utilize its principles of private inter-
national law to determine the law applicable to a dispute. See Mallesons, supra note 58, §§ 2.13,
2.18.

212. Murray v. the Schooner Charming Betsy, 6 U.S. 64 (1804).


214. The territoriality principle was the foundation of prescriptive jurisdiction, and
expansions of the doctrine may be seen as exceptions to this basic principle. Thus, one hundred
seventy years ago, Joseph Story in the first treatise on Conflict of Laws, observed that the
starting point for the subject is the territorial limits of law.

It is plain that the laws of one country can have no intrinsic force, proprio vigore, except
within the territorial limits and jurisdiction of that country . . . No other nation, or its
subjects, are bound to yield the slightest obedience to those laws. Whatever extraterritor-
orial force they are to have, is the result, not of any original power to extend them
abroad, but of that respect, which from motives of public policy other nations are
disposed to yield to them, giving them a . . . with a wise and liberal regard to common
convenience and mutual benefits and necessities.

Story, supra note 207, at 8.
International law requires a basis for the exercise of prescriptive jurisdiction. The five currently acknowledged are set out in the Restatement (Third) of Foreign Relations Law (Restatement (Third)): conduct within a nation’s territory, nationality, effects within a nation’s territory, “protective” jurisdiction (jurisdiction of any state to punish a limited number of offenses directed against the security or integrity of a state), and universal jurisdiction (over piracy, for example). By far the most controversial of these bases is that based on the effects conduct undertaken outside a state has within the state asserting jurisdiction. The Restatement (Third), however, in section 403 precludes assertion of jurisdiction on any basis if its exercise would be “unreasonable,” and lists a nonexhaustive list of factors to be considered in reaching that conclusion. The approach


216. Restatement (Third), supra note 200, at § 404. In United States v. Martinez-Hidalgo, 993 F.2d 1052 (3d Cir. 1993), for example, the U.S. Maritime Drug Enforcement Act, 46 U.S.C. app. § 1903 (1994), was interpreted to apply to a stateless vessel’s nonresident crew found carrying drugs in international waters with no nexus to the United States (i.e. no evidence that the drugs were intended to reach the United States). The court interpreted international law as not requiring such a nexus (a position it might have taken but did not, bolstered by reference to Restatement (Third) section 404) but also noted that, even if international law was to the contrary, congressional intent was clear and governed.

217. The basis is accepted in international law, even though its use in certain circumstances by the United States has been criticized. See generally John A. Trenor, Jurisdiction and the Extraterritorial Application of Antitrust Laws After Hartford Fire, 62 U. Chi. L. Rev. 1583, 1601 (1995). Another controversial basis, not generally accepted, is based on the local citizenship of the plaintiff, “passive personality” jurisdiction.

218. Section 403(2) states:

(a) the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory;

(b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect;

(c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted;

(d) the existence of justified expectations that might be protected or hurt by the regulation;

(e) the importance of the regulation to the international political, legal, or economic system;

(f) the extent to which the regulation is consistent with the traditions of the international system;

(g) the extent to which another state may have an interest in regulation the activity; and

(h) the likelihood of conflict with regulation by another state.

Restatement (Third), supra note 200, at § 403(2).
parallels that which first surfaced in *Lauritzen v. Larsen*\textsuperscript{219} and which was adopted by numerous lower courts following *Timberlane Lumber Co. v. Bank of America*.\textsuperscript{220} The Supreme Court's most recent foray into the area, however, apparently rejects the notion that such a balancing test, which takes into account the interests of various nations in the litigation and very much resembles the domestic conflict of laws approach, is required.

In *Hartford Fire Insurance Co. v. California*,\textsuperscript{221} the Sherman Act, previously held to apply to conduct occurring outside the United States that was intended to and did produce substantial effects in the United States,\textsuperscript{222} was held by the majority to apply to such conduct whether or not the interests of another country (in this instance Britain, where the conduct complained of occurred and where it was apparently in accordance with national policy) could be considered to outweigh those of the United States. Writing for five members of the Court, Justice Souter held that international comity would argue against the assertion of jurisdiction only when there was a "true conflict" between the laws of the relevant nations and that such a conflict exists only if compliance with both laws is impossible.\textsuperscript{223}

Of course, because an effect in the United States would quite clearly satisfy the constitutional requirements of due process, and because courts construing the extraterritorial reach of U.S. law are attempting to ascertain the intent of Congress which is only presumed not to desire to violate international law, the fact that effects in the United States may be sufficient in the eyes of the Court does not necessarily mean that they satisfy international law. At least, however, some support for this basis of jurisdiction can be found in Europe,\textsuperscript{224} and the need for (as well as the wisdom of) interest balancing is debatable.

On the other hand, even though Congress could intend the broadest possible reach for U.S. law, it obviously need not. For example, Title VII of the Civil Rights Act of 1964\textsuperscript{225} was interpreted by the Court not to extend its protection to U.S. employees employed abroad by U.S. employers,\textsuperscript{226} though under the nationality principle such jurisdiction would

\textsuperscript{219} 345 U.S. 571 (1953).
\textsuperscript{220} 549 F.2d 597 (9th Cir. 1976).
\textsuperscript{221} 509 U.S. 764 (1993).
\textsuperscript{223} 509 U.S. at 769. In dissent, Justice Scalia maintained that a conflict exists whenever states provide different substantive rules of decision and that the majority had misread Section 403(3) of the Restatement (Third). *Id.* at 798-99 (Scalia, J., dissenting). It does indeed command deference only when compliance with both laws is impossible, but it presupposes that the interest balancing mandated by Section 403(2) has already taken place.
\textsuperscript{224} See *supra* note 217.
clearly be proper. Similarly, although a nation clearly may regulate conduct that occurs on its territory, not all such conduct is in fact subject to U.S. law.227

Effects within the sovereign territory presumably were the basis for a recent assertion of prescriptive jurisdiction by France in a case involving the online auction by Yahoo! Inc. of Nazi-related items on its yahoo.com (as opposed to yahoo.fr) web site. There was no question that the site was accessible in France, but the .fr site did not offer the items. Clearly, the perceived ability to assert prescriptive jurisdiction does not determine whether it will be asserted.

If a court determines that a dispute is within the prescriptive jurisdiction of more than one sovereign, the court then must determine whether more than one sovereign has expressed the intent that its substantive law extend to the disputed transaction or conduct. If the answer is yes, the court then returns to an assessment of the same kinds of interests that figure in prescriptive jurisdiction analysis, in determining what law to apply pursuant to the forum's choice of law rules.

3.2.3. American and European Approaches to Choice of Law

Choice of law doctrine has followed very different paths in the United States and Europe. In the United States, formal approaches exemplified by the law of the place of the wrong, lex locus delicti, for torts, the law of the place of contracting, lex locus contractu, for contracts, and the law of the situs of property, lex locus sitae rei, for property disputes, has largely been replaced by more flexible approaches that analyze contacts between the dispute and contending sovereigns, supplemented by an interest approach that examines the interests of competing sovereigns in having their own law applied to particular issues in controversy.228 Thus, section 6 of the Restatement (Second) of Conflicts (American Restatement), followed by most states, directs a court's attention, absent a statutory directive, to concerns similar to those found in section 403 of the Restatement (Third).229

227. See, e.g., Europe and Overseas Commodity Traders, S.A. v. Banque Paribas London, 147 F.3d 118 (2d Cir. 1998) (U.S. securities laws not applicable to sale of foreign securities made in Florida by a foreign corporation to another foreign entity's president). For a discussion of the varying approaches of circuit courts to the reach of the securities laws, see Kauthar SDN BHD v. Sternberg, 149 F.3d 659 (7th Cir. 1998).

228. The formal American approach is associated with the First Restatement of Conflict of Laws and Joseph Henry Beale, its reporter. The newer approach is identified with Brainerd Currie and the Second Restatement of Conflict of Laws.

229. (a) the needs of the interstate and international systems,
(b) the relevant policies of the forum,
(c) the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue,
(d) the protection of justified expectations,
(e) the basic policies underlying the particular field of law,
(f) certainty, predictability and uniformity of result, and
There is much debate among American conflict of law scholars as to what should be done to clarify a set of doctrines that is perceived as being unsatisfactory because it is so unpredictable. Europe, especially Germany, still adheres to a more formal approach that resembles in its basic rules the formal approach of the American Restatement (First) of Conflict of Laws. So too does Japan, where the place of the relevant act, without consideration of "various nexuses," governs. Thus, for example, in tort cases, the applicable law is that of the place where the facts giving rise to the claim arose, and in contract cases, absent party choice, the law of the place where the offer was dispatched governs.

3.2.4. Torts

The American approach for torts is summarized in section 145 of the American Restatement. The law of the state with the most significant relationship to the occurrence and the parties is to be applied, taking into account such factors as where the injury occurred, where the conduct causing the injury occurred, the home of parties, and the place where any relationship between the parties is centered.

The differences between this approach and the European are more theoretical than real, however. In fact, the substantive law that gets applied under modern contacts or interests analysis in the United States most often is the same law that would get applied under lex loci delicti. Moreover, during the era when lex loci delicti was the norm, a variety of avoidance mechanisms were used to make the formal rule more flexible, including characterization of some issues as procedural and therefore always subject to the law of the forum, as opposed to substantive and thus within the

(g) ease in the determination and application of the law to be applied.


*d. Needs of the interstate and international systems. Probably the most important function of choice-of-law rules is to make the interstate and international systems work well. Choice-of-law rules, among other things, should seek to further harmonious relations between states and to facilitate commercial intercourse between them. In formulating rules of choice of law, a state should have regard for the needs and policies of other states and of the community of states. Rules of choice of law formulated with regard for such needs and policies are likely to commend themselves to other states and to be adopted by these states. Adoption of the same choice-of-law rules by many states will further the needs of the interstate and international systems and likewise the values of certainty, predictability and uniformity of result.

AMERICAN RESTATEMENT § 6 cmt. d.

230. ODA, supra note 96, at 443-44.
232. AMERICAN RESTATEMENT, supra note 229, at § 145.
scope of the *lex locus delicti* rule. As another example, the doctrine of Renvoi was used to change the outcome. Under the purportedly formal European approach, questions regularly arise as to the where the harm occurred, for application of the tort choice of law rule.

3.2.5. Contracts

The American approach for contracts is summarized in sections 186-188 of the American Restatement.\(^{233}\) Contractual choice of law clauses govern absolutely if the issue could have been resolved by an explicit contract provision; with respect to other issues, the clause governs unless the chosen state has no substantial relationship to the parties or transaction and is not otherwise reasonable, or use of the chosen law would violate a fundamental policy of a state with a materially greater interest in the issue than the chosen state and whose law would have been used under section 188 of the American Restatement had there not been a contractual choice.

Compare the regime created by the Rome Convention.\(^{234}\) Contractual choice of law clauses are enforceable, although if the contract is entered into by a consumer or if only one country is connected to the issues raised by the dispute, the clause does not preclude the use of that country’s mandatory rules.\(^{235}\)

Japan also generally enforces contractual choice of law clauses, although they can be overcome by mandatory protective laws when necessary to the maintenance of that regime.\(^{236}\) Thus, for example, the employment by a U.S. firm in Japan of a Japanese is subject to Japanese law; the employment of a Japanese in the United States is not.\(^{237}\)

Both approaches embrace party autonomy as the basic rule, allowing contract parties to choose the law to be applied to contract disputes, but both approaches allow significant exceptions: public policy or absence of contact with the chosen law, in the case of the American Restatement, and mandatory rules of the state of the consumer or the one with most significant contact, in the case of the Rome Convention and Japan.

When the parties have not expressly chosen the law to be applied to contract disputes, the American Restatement section 188 again provides that the law of the state with the most significant relationship to the issue should apply, taking into account where the contract was negotiated, entered into and to be performed, where the subject matter of the contract is, and where the parties live.\(^{238}\)

\(^{233}\) *American Restatement*, supra note 229, at §§ 186-88.

\(^{234}\) See supra note 70.

\(^{235}\) A mandatory rule is defined as one that cannot be derogated from by contract.

\(^{236}\) ODA, supra note 96, at 443.

\(^{237}\) Id. at 443-44.

\(^{238}\) *American Restatement*, supra note 229, at § 188. If the place of negotiating the contract and the place of performance are in the same state, the local law of this state will usually be applied, except as otherwise provided in §§ 189-199 and 203.
Corresponding provisions of article 4 of the Rome Convention provide that, absent contractual choice, the applicable law shall be that of the country with which the contract is most closely connected,\(^{239}\) which is presumed to be the habitual residence or principal place of business of the party who is to effect the performance characteristic of the contract. The article also presumes that if the contract involves immovable property, the country where the property is located has the closest connection to it and that with respect to the carriage of goods, the most closely connected country is the carrier's principal place of business if it is also where the goods are loaded or discharged or the principal place of business of the consignor.

3.2.6. Consumer Contracts

The tension between Europeans and Americans with respect to choice of law is most dramatic when consumer disputes are involved. The principal difference arises from the contrast between articles 5 and 7 of the Rome Convention regarding consumer contracts and mandatory rules, and the doctrine of *Carnival Cruise Lines*,\(^{240}\) which permits the enforcement against consumers of reasonable choice of forum clauses even in a contract of adhesion. Article 5 of the Rome Convention does not enforce the waiver by consumers\(^{241}\) of mandatory laws of their habitual residence designed for their protection, although a choice of law clause may apply different law to other aspects of the contract and dispute.\(^{242}\) Furthermore, absent a choice of law clause, article 5 provides that the law to be applied is that of the consumer's habitual residence unless the contract is for carriage (other than an inclusive contract for travel and accommodation) or the provision of services exclusively in another forum.

Most reviews of American choice of law assert that this special rule for consumer contracts sharply distinguishes European doctrine from American doctrine. That is not necessarily so. For example, in *State ex rel Meier-henry v. Spiegel Inc.*,\(^{243}\) the attorney general of South Dakota sued to recover excessive interest charged by an out of state seller in violation of South Dakota law.

\(^{239}\) Rome Convention, *supra* note 70, at art. 4. Australia operates under a similar rule, choosing (in the absence of an enforceable contractual choice clause) the law of the state with which the contract has "the closest and most real connection." Mallesons, *supra* note 58, at § 2.19.


\(^{241}\) 241. Rome Convention, *supra* note 70, at art. 5. Covered consumers are those who were solicited, either individually or through advertising, in their forum and who there completed steps necessary by them for the formation of the contract and those who traveled elsewhere to place an order for goods at the arrangement of the seller for that purpose.

\(^{242}\) *See* Graham, *supra* note 113, at § I.A.

\(^{243}\) 277 N.W.2d 298 (S.D. 1979).
Dakota law. The defendant was an Illinois-based mail-order enterprise, which offered credit sales via catalogues available in South Dakota. Credit agreements provided that they were to be governed by Illinois law. The trial court granted summary judgment for the defendant, finding that Illinois law, rather than South Dakota law, applied to determine the permissible rate of interest. The state supreme court accepted the general rule that parties to a contract may effectuate their own choice of law but nevertheless reversed. It found that the choice of law provision in the credit agreement was void as against the public policy expressed in the South Dakota usury statute.

Other American choice of law cases recognize the possibility that the public policy of one state may override a choice of law provision in a contract but avoid invalidating the contract because of similarity of the competing substantive laws.244

3.2.7. The Internet and International Law

It is not simply a matter of reconciling sharply contrasting European and American approaches to choice of law; the question is whether characteristics of Internet transactions necessitate new approaches to choice of law, which have not been adopted under the pressure of earlier forms of commerce. As Spiegel and other cases illustrate,245 the possibility of economic burdens arising from differing requirements imposed by multiple jurisdictions is not new. The Internet does, however, complicate matters. The typical facts of a political or a commercial Internet transaction support competing inferences as to localization of activity (where is a web page located? where it is viewed, on a client computer, or where the server transmitting the code is located?) and as to when a transaction is completed (when the server transmits a web page, or when a client transmits the URL that automatically causes the page to be transmitted from a remote server?). Much of this difficulty is encompassed by the argument over whether the law of the place origin or the law of the place of the consumer should be applied to e-commerce disputes involving consumers.

It also can be argued, as with respect to personal jurisdiction, that the Internet’s inherently global reach justifies special efforts to reduce uncertainty with respect to choice of law. Pre-Internet modes of doing business make it relatively easy to limit business only to those states where the seller

244. Demitropoulos v. Bank One Milwaukee, N.A., 915 F. Supp. 1399, 1414 (N.D. Ill. 1996) (upholding choice of law provision) suggests that similarity of an Illinois consumer protection law and the Wisconsin law selected by the choice of law clause vitiated a public policy argument that the Illinois law should be applied notwithstanding the clause.

245. See, e.g., Aldens, Inc. v. Miller, 610 F.2d 538 (8th Cir. 1979) (rejecting claim by interstate mail order vendor that mandatory provisions of Iowa Consumer Credit Code violated Commerce Clause because they imposed burden on operations of vendor; citing cases from the Third, Seventh and Tenth Circuits reaching same conclusion).
is willing to comply with the local law protecting consumers in that state. An Internet seller must undertake extraordinary steps to limit the reach of its solicitation of customers and receipt of customer orders; the Internet does not naturally associate either sellers or buyers with physical places. Technology, however, may be used to redress the jurisdictional issues raised by the technological efficiencies and global reach of the Internet. The existence and continuing development of intelligent electronic agents, which can be deployed by sellers and purchasers to evaluate the relative product, price and jurisdictional terms of the potential relationship, provide a basis for a global standard, as long as the underlying legal “code” can be agreed upon.

3.2.8. Choice of Law and Personal Jurisdiction

Finally, choice of law and personal jurisdiction interact. Whether a court gets the chance to apply its own choice of law rule depends on whether that court has personal jurisdiction. If it adjudicates the case and its choice of law rule rejects application of the substantive law of another sovereign and causes substantive law of the forum sovereign to be applied, the efficacy of that decision depends on whether the court had personal jurisdiction. If the judgment debtor (usually the defendant) has no assets within the forum sovereign state, the judgment must be enforced in a sovereign state where the judgment debtor does have assets. The courts of that sovereign are entitled to reassess the question of personal jurisdiction in deciding whether to recognize and then to enforce the first judgment. If the courts in the second sovereign determine that the first court lacked personal jurisdiction, the choice of law made by the first court is defeated.

3.3. Enforcement Jurisdiction

A judgment generally can be enforced only in a forum in which assets belonging to the defendant can be found and seized by the executive arm of government, pursuant to a court order of that forum, sold, and the proceeds turned over to the plaintiff in satisfaction of the judgment.\textsuperscript{246} As jurisdiction is exercised more frequently over defendants not physically present in the state rendering the initial judgment, the need to involve other states in the enforcement of judgments increases.\textsuperscript{247}

\textsuperscript{246} Exceptions to this include situations where regulatory agencies seek to enforce a judgment issued or obtained against an entity not currently in the forum through the prohibition of its activities in the forum.

\textsuperscript{247} Typically, though not necessarily, the forum asked to enforce a foreign judgment is the defendant’s home state, where he is clearly subject to personal jurisdiction and where his assets are likely to be found. Other fora, however, in which his assets are located may also be asked to enforce the judgment. Jurisdiction there is satisfied because the property in the state constitutes a purposeful contact with it and the claim is, even after \textit{Shaffer v. Heiner}, 433
Enforcement of a judgment rendered by another forum requires its recognition by courts of the forum requested to enforce it. If the judgment is that of a court of a state of the United States, the full faith and credit clause of the Constitution requires that it be recognized and enforced by the courts of all other states if it has been rendered in accordance with due process, if, in other words, the court rendering it had personal jurisdiction over the defendant. A defendant who has defaulted may argue to the enforcing court that the rendering court lacked such jurisdiction; if she so convinces the court, the judgment will not be enforced. If the defendant has argued in the first forum, however, that it lacks personal jurisdiction and lost, he may not relitigate the issue in the court from which enforcement is sought; his only recourse is to appeal the first court’s decision in the courts of that forum.

When the judgment for which recognition is sought has been rendered by a foreign court, its recognition in the United States depends upon local statutory law or comity. Basically, these sources of law require recognition unless the party opposing it can show violations of procedural due process.

U.S. 186 (1977), sufficiently related to the property to make an exercise of jurisdiction reasonable. Shafter, while questioning quasi in rem jurisdiction as a basis for hearing a case in the first instance, explicitly distinguished enforcement jurisdiction, suggesting that the presence of property supports jurisdiction to enforce a judgment even if the underlying litigation was unrelated to the property. Id. at 217.

248. Supra note 199.

249. Pennoyer v. Neff, 95 U.S. 714 (1877). If, however, she loses her jurisdictional argument, the judgment will be enforced; she may not litigate the merits of the claim underlying the default judgment.


Of course, the degree of procedural difficulty may vary widely, even if underlying principles are similar. Both Brazil and Columbia, for example, have quite elaborate statutory requirements for recognition. See Noronha Advogados, supra note 191, at § 5.4.1, and Gamboa, supra note 191.

253. See, e.g., Bridgeway Corp. v. Citibank, 201 F.3d 134 (2d Cir. 2000) (refusing to enforce a final judgment of the Supreme Court of Liberia rendered during a period in which the Liberian judicial system was described by the U.S. State Department as corrupt and incompetent).
lack of personal jurisdiction by the rendering court, 254 or, in rare instances, violations of public policy in the recognition state. 255

Not all nations rely solely on international law notions of comity to determine under what circumstances judgments of foreign courts will be enforced. In Australia, for example, the common law permits recognition and enforcement of foreign money judgments if the defendant either resided in the forum whose courts rendered the judgment or submitted to that court’s jurisdiction. Otherwise, final and conclusive foreign judgments are recognized and enforced pursuant to section 7 of the Foreign Judgments Act 1991 (Cth), which specifies courts and countries covered by it and which is dependent upon reciprocal recognition and enforcement of Australian judgments. 256

National procedures required for recognition and enforcement of judgments vary widely both in detail and complexity. Whether reciprocal recognition is required and what that requirement entails differ from country to country. Some countries will not recognize a default judgment, others will. 257 One of the most beneficial potentials of the draft Hague Convention is its dual nature: judgments rendered by a contracting state in accordance with its jurisdictional rules are enforceable in all contracting states. 258

Because in all instances enforcement of foreign judgments depends upon the existence of personal jurisdiction in the rendering state, agreement between nation-states in particular as to what that jurisdiction necessitates is critical to effective judicial dispute resolution involving parties from different states.

REPORTS OF THE WORKING GROUPS

ADVERTISING/CONSUMER PROTECTION

Traditional aspects of jurisdiction over consumer protection and advertising practice are difficult to apply to the Internet. The primary reason is that countries throughout the world have in place numerous different regimes to protect their consumers based on the “old world” presumption that consumers will shop in proximity to where they live and will not give

254. While one state is bound by another’s determination of its own jurisdiction, fora asked to enforce foreign judgments typically will feel free to reconsider the existence of jurisdiction in the rendering state.


256. Mallesons, supra note 58, at 2.20-2.22.


258. Draft Hague Convention, supra note 58, art. 2.
up their sovereignty in applying these laws. Merchants cannot comply simultaneously with the laws of all of the local jurisdictions throughout the world regardless of whether they are actually directing or doing business with consumers in the local jurisdictions. Moreover, even if it were possible to comply with all of the differing laws, the cost of compliance, particularly for small companies, creates a barrier to entry. Of course, however, it is important to recognize when measuring the costs of compliance that the Internet creates inexpensive access to a worldwide customer base that is otherwise unimaginable. The Internet can also reduce compliance costs by making information about legal regimes more available. In addition to legal predictability for merchants, consumers need effective protection and predictable and consistent standards to have confidence in their transactions. A global dialogue between regulators, consumers, and businesses is underway to create a coherent, functional, and predictable framework for consumer protection.²⁵⁹

One of the difficulties in attempting to define a workable framework for consumer protection on the Internet is that the scope of “consumer protection” is too broad to be governed by any one approach. To evaluate better an appropriate framework and to identify how jurisdictional concerns impact this area of the law, dividing the subject of consumer protection into three categories is useful: (1) fraud and deception, (2) transactional, and (3) content/otherwise regulated industries.

Local authorities will likely continue to maintain and exercise jurisdiction over deceptive fraudulent Internet activities against their citizens. Even if the remediation differs, basic principles outlawing fraud and deception should be universal. As a result, the power of numerous countries to pursue bad actors should be less problematic to the development of the Internet. In fact, the burden of multiple sovereigns exercising their jurisdiction against bad actors could actually serve as a strong deterrent to such behavior, enhancing consumer confidence.

Local authorities will also apparently continue to assert jurisdiction in the content/otherwise regulated industries category. The result is that issues falling within this area generally will be subject to numerous complex, and often conflicting, regulations on the global scale. This category of consumer protection includes transactions that are specially regulated, such as financial services, health care, alcohol, tobacco, firearms, gambling, and other content issues such as hate speech and pornography.

The “transactional” category presents the greatest opportunity to begin to develop a new global jurisdictional framework. Of the three categories,

²⁵⁹. See, e.g., the recent European Commission proposal for the establishment of an alternative dispute “clearinghouse” mechanism to deal with disputes arising from online purchases. Commission launches “e-confidence” on-line forum to promote alternative dispute resolution (last modified April 2000) <http://www.ispo.cec.be/ecommerce/epolicy/2000-04.html#econfidence>.
this one provides the main focus of international discussions attempting to define a new global framework. This category includes marketing and online contract terms and covers disclosures, terms of agreements, and dispute resolution. Advertising fits into this category, as an advertisement is the communication about the offer from the seller to buyer. The lines between marketing, advertising, and performance are increasingly blurred by the technical capabilities of the Internet.

1.1. Power Parameters

The characteristics of the Internet (e.g., personalization, lower barriers to entry, global reach, and asynchronous communication) may reduce risks of “unfairness” and “unconscionability” in consumers’ contracts with vendors. The Internet increases the availability of consumer choice and has the potential to limit the sales pressures that can create unfairness. All Internet users can find alternate sources of goods and services—indeed, the global nature of the medium could reduce the risk that users are ever “stuck” with a single source or a single form contract for a given good or service.

In some ways, however, the Internet may also make consumers less powerful. New challenges to knowing choice exist in this medium. For example, important contract terms can be buried multiple clicks beneath an offer. Moreover, it may be difficult to understand the implication of even clearly disclosed contract terms. Consumers also might be held to contractual terms as a result of an accidental click of the mouse. Consumers cannot physically visit or handle the merchandise on the Internet as they can in the offline environment, so they rely more on merchant disclosures of the quality and description of products.

The Internet provides consumers with easy access to vast amounts of information and facilitates rapid comparison shopping on a global scale. The merchant itself can provide a large amount of information about its products and services. Consumers can look to third-party sources that provide additional information, including product reviews, advice and guidance concerning how to purchase a particular good or service, and reputational information concerning a particular merchant. The Internet provides consumers with up-to-date, easily searchable information about companies’ performance histories, and the ability to communicate their own experiences widely to others, making it even more difficult for unscrupulous companies and individuals to stay in business for long. Third-party consumer protection organizations provide another important and useful resource. All of this information is close at hand and easily accessible.

Of course, however, the seemingly limitless number of choices for consumers available on the Internet may also create new risks to consumers that did not exist in the off-line world. For example, as a result of the
multitude of sites and services available, it may be more difficult for consumers to recognize individually merchants as reputable based on their own familiarity and personal experience with the merchant.

1.2. Contractual Deference

As a result of the change in power parameters, deference to contract could play a major role in determining the standards for transactions between merchants and consumers. One central similarity between off-line and online consumers is that both groups enter into contracts with vendors. Many of these contracts are not negotiable. Under U.S. law, “adhesion contracts” (unilaterally-drafted form agreements) are enforceable absent a finding of “unfairness” or “unconscionability.”260 In the European Union, contractual deference is limited by the Unfair Contract Terms Directive,261 and a variety of national consumer protection laws. The Directive governs contractual terms which have not been individually negotiated, the type that currently comprises the majority of consumer Internet transactions. Such contracts are deemed unfair if they cause a significant imbalance in the parties’ rights and obligations under the contract, to the detriment of the consumer.

Moreover, the nature of a contract between a consumer and a vendor is being positively affected by the technological developments that have created these complex jurisdictional issues. Technology, indeed, can solve many of the problems that it causes. For example, electronic agents and other artificial Bots—resident software programs—can be programmed by consumers to identify the country, laws, protections, standards, and remedial options that the consumers seek while shopping on the Internet. The consumer can thus be given a clear green, red, or yellow light regarding whether she should proceed with a particular transaction. Where the consumer is advised that the location and terms of the site are inconsistent with her preprogrammed preferences, she can make an informed decision to proceed anyway and accept the terms of the transaction. To the extent that nations adopt uniform global protocol standards, such a system of electronic disclosure and decisionmaking can allow consumers to enter only into the contractual arrangements they want to in Cyberspace.

Given the rich diversity of sources for products and services available on the Internet that provide the opportunity for Internet consumers to have access to more information about vendors than they possibly could in the physical world, e-commerce contracts are likely not, as a class, to be inherently unfair or unconscionable either in the United States or the European Union. Individual contracts, however, may still be unfair and/or unconscionable. Nonetheless, choice of law and forum clauses in online

adhesion contracts could potentially be enforced and may provide an option that could increase certainty regarding jurisdiction.

1.3. Relevance of Physical Location

Another approach to addressing jurisdictional issues with regard to Internet transactions, offered by consumer groups as well as various governments, is that jurisdiction resides with the physical location of the consumer for all transactions. This concept attaching jurisdiction to the location of the consumer also is contained in the proposed amendment to the European Union’s Brussels Convention that could be implemented in the coming months. Finding the jurisdiction of the consumer to apply to a transaction could prove unworkable for e-businesses, requiring them to be familiar with and comply with the laws of every jurisdiction in which consumers who transact business with them may reside.

It is also daunting for consumers to be familiar with the laws of the various jurisdictions of merchants, and consumers may have fewer resources to do legal research. In fact, companies may have more leverage to solicit from consumers their locations than consumers can from merchants.

Yet in a similar way, knowledge of physical location of merchants may be an important factor for consumers.

This concept requires knowledge of the jurisdiction of the consumer, which in certain instances does not currently exist. Companies would, depending on the jurisdiction of the consumer, be required to conduct, either manually or electronically, an analysis to determine the legal obligations within the consumer’s jurisdiction for conducting the transaction. A traditional analysis of the different classes of transactions in varying jurisdictions would be very expensive and could result in increasing the price to the consumer or in limiting the merchant’s offering altogether. An electronic analysis based on disclosures made by the consumer and the vendor pursuant to global protocol standards could affect the practicality and cost of such a process. The analysis also could be provided through a service offered by a separate business or consultant.

Another potential outcome is that merchants will offer their products over the Internet only to consumers in limited jurisdictions. Many companies currently are placing such restrictions on their transactions. Such a result would limit the number of international transactions outside of the United States, thus stunting new markets where much of the future growth is predicted. In some instances, limiting the availability of goods and services may be a positive result. For example, in certain circumstances, limiting the availability of products (such as those that pose health and safety risks) may be desirable.

262. Brussels Convention, supra note 33, tit. 2, § 1, art. 3.
Alternatively, some businesses are suggesting that the jurisdiction of the merchant ("law of origin") govern transactions with consumers. This is the approach currently being set forth by the Global Business Dialogue on Electronic Commerce, the American Advertising Federation (AAF) and the International Chamber of Commerce.\textsuperscript{263} The AAF proposes that advertisements should be governed by the law of the country of origin. Under this approach, the jurisdiction of the merchant and its corresponding consumer protection laws would apply to all transactions. This approach is unlikely to garner the support of consumer advocates or governments outside the United States. Additionally, the jurisdiction of the merchant approach would encourage "shopping" by merchants to locate in jurisdictions with legal frameworks favorable to their businesses. Examples of forum shopping in the Internet context are already seen with regard to issues more focused on content, such as pornography and gambling.

1.4. Targeting

Another possible basis for establishing jurisdiction in the area of consumer protection is that of "targeting." Under this concept, local authorities could assert jurisdiction over online consumer transactions involving merchants from another jurisdiction when the merchant has intentionally targeted the overall offer to consumers found in those jurisdictions.\textsuperscript{264} Some factors that could serve as indications of targeting are advertising, sale of products or services, shipment, language, and monetary currency of the web site. The targeting concept also is mentioned in the Organization for Economic Cooperation and Development’s (OECD) Guidelines on Consumer Protection adopted in December 1999 by the more than 20 member countries of the OECD which states that "[b]usinesses should take into account the global nature of electronic commerce and, wherever possible, should consider the various regulatory characteristics of the markets they target."\textsuperscript{265} This approach may prove difficult because of the difficulties in determining the characteristics that are associated with "targeting," unless nation states are willing to agree on acceptable standards for successful targeting in Cyberspace. In addition, to the extent that "targeting" becomes an accepted means of establishing jurisdiction, the use and effectiveness of software filters and other technological screening de-


\textsuperscript{264} See analysis in Part 2.2 of this report.

vices should also be considered. Given, however, the potential for such an approach, it is one stakeholders need to discuss and evaluate thoroughly.

1.5. Harmonization

Another potential solution is to not apply either the law of the consumer or of the merchant, and instead to apply common principles of consumer protection law that would govern all transactions that occur over the Internet regardless of the location of the consumer or the merchant. Such an approach would harmonize differing laws and establish a uniform law of consumer protection for Internet transactions. Harmonization could occur through formal governmental mechanisms, i.e. treaties or bilateral agreements, or through less formal self-regulatory frameworks. One development toward harmonization is seen in the OECD development of consumer protection guidelines for consumer protection on the Internet. These guidelines represent a first step toward defining harmonized law in the area of consumer protection. While the guidelines do not set out detailed standards for consumer protection, they do provide general guidance to member countries for the substantive consumer protections that they should provide to their citizens. Included are guidelines on advertising and marketing practices, business disclosures, payment, dispute resolution, and redress. As with other guidelines adopted by the OECD, countries will consider these guidelines as they develop and implement online consumer protection standards.

Of course, there always exists the possibility of negotiating a treaty that would harmonize the consumer protection laws of all signatories to the treaty. This approach has been disfavored because treaties generally can take a very long time to negotiate and implement. Such a time frame is not particularly well suited for the rapidly evolving and changing Internet. In addition, treaties in the area of consumer protection in the non-Internet context do not exist, thus further bringing its feasibility into question.

One way to achieve a result similar to that of an international treaty would be a series of bilateral or multilateral agreements in which countries could agree to adhere to specific consumer protection laws. The United States has entered into several agreements with other countries to allow the Internet to continue to develop unfettered by regulation. Bilateral agreements could also agree to defer to self-regulatory frameworks for Internet consumer protection.

The draft Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters presents one possible forum for addressing

the jurisdictional issue. The drafting of this convention began prior to the proliferation of the Internet. The momentum for concluding the Convention appears to have slowed as representatives are considering its implications for e-commerce. Until recently, the Convention had an approach similar to that found in the Brussels Convention in which the law of the habitual residence of the consumer would apply. It is unclear what the outcome of this convention will be. The convention does not address substantive areas of consumer protection.

1.6. Self-Regulation: Private Codes of Practice Supported by Third-Party Seal Program and/or Alternative Dispute Resolution

Another framework with significant potential is industry self-regulation. While self-regulation may offer an attractive alternative to the development of local laws, its success may be thwarted by national and local regulators who are not familiar with concepts of self-regulation, not familiar with the Internet and see it as a dangerous threat to their power, not willing to defer to such a system, and not able to avoid local political pressures that will doom the effort. The sheer number of local and national authorities that would have to "buy into" any system for it to work is staggering. In addition, the concept of First Amendment protection for commercial speech (often a distinctly U.S.-centric concept) makes uniform application of general principles of advertising regulation difficult. Some self-regulatory efforts are perceived as being ineffective. Finally, there is a very real and legitimate concern by business that over-regulation or knee-jerk fear of the Internet may spill over into more traditional forms of marketing, advertising, and consumer transactions.

Nonetheless, codes that set forth the standards for transactions are being developed throughout the world. Various U.S. companies are actively discussing consumer protection and jurisdiction issues that arise in the electronic commerce context, in the hope of developing a code of conduct for online transactions between merchants and consumer. BBBOnline is in the late stages of developing a code of conduct for businesses dealing with consumers. And on June 6, 2000, the Electronic Commerce and Consumer Protection Group\textsuperscript{268} proposed guidelines to protect consumers online. The use of seal programs and third-party dispute resolution are being considered as a means of resolving complaints by consumers. Self-regulatory codes backed by effective enforcement could offer an efficient means of addressing consumer protection for transactions.\textsuperscript{269} But it ap-

\textsuperscript{268} The group is composed of leading Internet companies that address consumer protection issues in electronic commerce. See Electronic Commerce & Consumer Protection Group (visited July 3, 2000) \textlt{http://www.ecommercegroup.org/}.

\textsuperscript{269} Henry H. Perritt, Jr., The Internet is Changing the Public International Legal System, 88 Ky. L.J. 885 (1999-2000).
pears that for such a framework to achieve "buy-in" from regulators, experience needs to demonstrate the effectiveness of such a system.

1.7. Intermediary Liability

The framework that evolves will likely be composed of some combination of the various approaches set forth above. Regardless of the framework, an important question to be resolved will be to what types of entities the legal regime and consumer protection standards apply. The technical underpinnings of the Internet are such that it is possible to impose liability on intermediate providers of services. While extending liability to these services is certainly possible, such extensions may not be good policy. For example, in the United States, Internet service providers are not liable for content supplied by others.270 One problem with intermediary liability is that intermediaries tend to become censors, impeding free expression and innovation. Another problem is that it may be impracticable for intermediaries to screen content. On the other hand, the intermediary frequently is the only "deep pocket" and is close at hand, while the original actor may be hard to identify, hard to find, and judgment proof. The temptation to ameliorate jurisdictional challenges by targeting intermediaries is not likely to disappear.

1.8. Conclusion

Significant progress in the area of establishing standards and regulatory certainty with respect to the transaction component of consumer protection will likely be made in the coming year. Other areas with respect to content and otherwise regulated business will likely evolve more slowly.

DATA PROTECTION

The data protection working group has examined jurisdictional issues as they apply to divergent data protection (or "data privacy") laws that apply to online interactions with individuals, particularly consumers. Specifically, the working group has concentrated on the jurisdictional aspects of laws that establish rights and obligations concerning the collection and use of personally identifiable information for commercial purposes.

2.1. The Proliferation of New Privacy Rules

A glance at the newspapers, television news, webzines, or popular Internet discussion sites quickly reveals a heightened public concern over privacy in the age of networked computers. This has given rise to calls for

greater legal protections against such practices as covert information gathering, identity theft, insecure storage of credit card numbers, compilation of mailing lists for unsolicited advertising, consumer profiling, and information sharing for marketing and other purposes.\footnotemark[271]

Data privacy laws enacted in the 1970s and '80s were designed to prevent abuses of large government and commercial databanks and to curtail adverse consequences stemming from inaccurate or incomplete data in those databases. These statutes include prominently the U.S. federal Fair Credit Reporting Act of 1970 (FCRA)\footnotemark[272] (regulating credit bureaus and their corporate customers) and the Privacy Act of 1974\footnotemark[273] (governing federal databases), the early "omnibus" laws on privacy and data processing systems such as the 1978 French data protection law\footnotemark[274] and the various European national laws based on the 1981 Council of Europe Convention No. 108 on the automated processing of personal data.\footnotemark[275]

Now these laws are being updated or supplemented by measures at state or provincial as well as national levels that cover more activities, in greater detail, and with more extensive provisions for regulatory oversight and remediation. The fifteen Member States of the European Union are in the process of transposing the comprehensive E.U. Data Protection Directive into national law\footnotemark[276] and, at the same time, they are trying to assess how to apply the Directive to cross-border electronic commerce.\footnotemark[277] Most of the other European nations and, indeed, several of the major trading partners of the E.U. in other regions of the world, from Canada to Japan, are debating new laws or supplementing old ones, following to some extent the model of the E.U. Data Protection Directive. In the United States, the

\footnotetext[273]{5 U.S.C. § 552a (1994).}
\footnotetext[275]{Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, ETS No. 108 (Jan. 28, 1981) <http://conventions.coe.int/treaty/EN/cadreprincipal.htm>; see national laws collected in English translation in the BUSINESS GUIDE TO PRIVACY AND DATA PROTECTION LEGISLATION (C. Franklin ed., 1996).}
Federal Trade Commission and several state attorneys general have taken or threatened action against privacy abuses as "unfair or deceptive" trade practices. New federal statutes, elaborated by agency regulations that are scheduled to take effect in 2000, cover, respectively, financial privacy (the Gramm-Leach-Bliley or GLB Act), children's privacy (the Children's Online Privacy Protection Act, or COPPA), and medical privacy (proposed Health and Human Services regulations under HIPAA). Dozens of data privacy bills are being debated by Congress or state legislatures this year, some of them specifically focused on online activities.

There are common themes in these data protection laws and regulations. Data protection laws are typically based on principles of "fair information practices," which the U.S. Federal Trade Commission has summarized, based on seminal U.S. and international texts, as "notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress." These principles are broadly reflected in the U.S. Privacy Act of 1974, the 1980 OECD Guidelines on personal data protection and the free flow of information across borders, Council of Europe Convention No. 108, and the more recent E.U. Data Protection Directive.

But there are substantial differences in scope, detail, and remedies under the various data protection laws, giving rise to potential conflicts when they are applied to actors across national (or indeed sub-national) borders. There is, as yet, little jurisprudence on the application of such laws to foreign parties. The relevance of such laws to purely electronic contacts


in Cyberspace is especially uncertain, for both jurisdictional and practical reasons.

2.2. What Is Different about the Internet?

This Report identifies five issues relevant to jurisdictional analysis that are peculiar to transactions via the Internet. Some have greater relevance than others to questions about the application of data protection laws to online contacts with consumers.

2.2.(a). Localization

Legal protections of data privacy concern the collection and use of information about individuals—and information moves abroad swiftly and automatically on the Internet. Information can even be obtained covertly from a user’s computer, or recorded automatically as she visits a web site or posts comments, and then it may be transferred onward to other parties at other locations, perhaps for other purposes than those contemplated by the user. The parties who obtain and use consumer information may have no physical establishment in, or even regular contacts with, the jurisdiction in which the consumer resides. This raises both practical and legal impediments to the enforcement of local data privacy laws designed to protect that consumer. To the extent that data protection laws focus on acts of information gathering or processing that occur “within” a territory, it may be unclear whether Internet contacts would suffice to trigger coverage under the law. Data processing on a foreign computer, even one that was at some time linked telephonically to a local consumer, is not indisputably an act “within” the consumer’s territory.

2.2.(a)(1). The E.U. Directive

The uncertainty as to how to analyze Internet-only contacts under data privacy laws can be illustrated by the jurisdictional provisions of the E.U. Data Protection Directive, the most comprehensive piece of modern data privacy legislation. The Directive provides that each Member State must apply its national data protection law (based on the Directive, but subject to some degree of local variation) to any “processing” of personal data that is “carried out in the context of the activities of an establishment of the controller on the territory of the Member State.”284 “Processing” is very broadly defined in the Directive and includes collection, recording, storage, transmission, or use of personal data,285 and a “controller” is any party that determines “the purposes and means of the processing of personal data.”286 An “establishment” is not defined in the Directive but generally

285. Id. art. 2(b).
286. Id. art. 2(d).
refers to a legally recognized, physical presence in the territory of a Member State.

Thus, virtually any “processing” in the E.U. by a company established in an E.U. country will trigger the application of that nation’s data protection law. And if the controller of the data is a company that is established in several E.U. member states, the controller is obliged to ensure that “each of these establishments complies with the obligations laid down by the national law applicable.” These are hardly surprising results; local establishments can be expected to comply with local law, and they can be supervised by data protection regulatory authorities located in the E.U.

But the wording of article 4 suggests that “processing” itself is not what must occur “on the territory” of a Member State or States. Processing is covered by the law if it is carried out “in the context of the activities” of an establishment located in a Member State. This might be read to indicate that if a multinational company has established branches or affiliates in the E.U. and also processes personal data at its headquarters in the United States in support of its E.U. operations (perhaps in connection with online orders, for example), the European laws cover the processing in the United States. This reading of article 4 would assert an extraterritorial reach for the national laws implementing the Directive. And article 4 operates in parallel with the better-known but indirect extraterritorial impact of the Directive in obliging Member States to prevent the transfer of personal data to any country where it is not “adequately” protected.

The E.U. Data Protection Directive also attempts to regulate the activities of parties that are not established in the E.U. but that make use of facilities in the E.U. to collect or otherwise “process” personal data. Article 4(1)(c) says that a Member State’s law must apply to a controller that is not established on E.U. territory but “for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory” of the Member State (unless the equipment is used solely for the transit of data through the country). Moreover, such controllers are obliged to “designate a representative” established in that Member State, presumably for purposes of legal or regulatory actions concerning compliance with the country’s data protection laws. Commentators note that article 4(1)(c) could apply, for example, to a web site operator in Florida whose site is visited by a German consumer; the web site operator might be deemed to “make use of” the consumer’s computer and the German telephone network to collect information on the consumer.

287. Id. art. 4(1)(a).
288. Id. art. 25(1).
289. Id. art. 4(2).
so, article 4 may represent an independent ground for asserting jurisdiction over Internet activities without reference to existing jurisdictional doctrines or conventions. And again, the Member States are under an obligation to prevent data from being transferred to a country where the data is not “adequately” protected.291

The application of articles 4 and 25 of the E.U. Directive to Internet-only contacts from abroad is unsettled. But as a practical matter, it would be nearly impossible for European regulators to compel foreign web site operators around the globe that are not associated with established companies in Europe to designate European legal representatives, register or notify their data processing activities under the laws of each European country, and comply with the entire range of European data privacy rules and procedures. The Directive is not without effect on the Internet, but its reach certainly exceeds its grasp.292

2.2. (a)(2). U.S. Laws

U.S. laws and regulators concerned with data privacy have typically been silent about foreign online transactions. The Federal Trade Commission’s annual Internet surveys and enforcement actions to date, based on assertions of “unfair or deceptive” trade practices under FTC Act section 5, appear to be limited to U.S.-based operators of “.com” web sites.293 The GLB Act does not itself define its jurisdictional reach, and the various federal financial regulatory agencies are still developing their approach to financial services advertised or offered online from foreign countries. COPPA is unique in being a federal privacy statute specifically focused on online activity, and it takes an aggressive approach to jurisdiction, seeking to control all web site operators, foreign or domestic, who interact with American children. COPPA establishes parental consent rules for online interactions with children under the age of 13, and its obligations extend to “any person offering products or services for sale through [a] web site or online service, involving commerce—(i) among the several States or with 1 or more foreign nations . . . .”294 The implementation of this statute with respect to foreign web site operators is problematic, just as is the implementation of European data protection law with respect to web site operators outside Europe.

2.2. (a)(3). Extraterritorial Enforcement of Criminal and Administrative Sanctions

Data protection laws typically establish criminal offenses and include criminal penalties, often in addition to establishing a regime of regulatory

supervision. These are particularly difficult to sustain extraterritorially, and there is little if any precedent for applying criminal privacy offenses to foreign contacts with a local consumer purely by Internet.

To enforce privacy-related consumer protection laws (including the proscription against "unfair or deceptive" trade practices, as well as violations under the Fair Credit Reporting Act, GLB Act Title V, and the COPPA), the Federal Trade Commission (FTC) is authorized to issue administrative orders, impose civil penalties, and initiate federal court actions seeking injunctions or compensatory damages for consumers. To date, it has not done so with regard to a foreign web site operator accused of violating announced or mandated privacy policies.

GLB Act Title V relies on enforcement by the "federal functional regulators" (such as the Securities and Exchange Commission and the Office of the Comptroller of the Currency), the FTC, and the state insurance commissions to regulate the financial privacy practices of companies within their respective functional jurisdictions. The consequences of violations could, therefore, include administrative orders, fines, compensation, and the revocation or denial of licenses to offer regulated financial services – sanctions that may be meaningless to a foreign company that does not seek to maintain a licensed financial services business in the United States. Similarly, HIPPA section 264 provides for oversight by the federal Department of Health and Human Services and authorizes civil monetary penalties and criminal sanctions where medical privacy is violated. None of these agencies has experience in policing foreign Internet-based activities apart from a handful of egregious fraud and money-laundering schemes, where international cooperation has been forthcoming, and it is difficult to see how they would attempt to deal with foreign web sites that are not complying with detailed U.S. privacy regulations.

On the other side of the Atlantic, the E.U. Data Protection Directive obliges Member States to "adopt suitable measures," including "sanctions," to ensure compliance with the implementing national laws. Those Member States that have already transposed the Directive into national law have, indeed, included criminal penalties. In addition, the Directive expressly requires each Member State to (a) establish an inde-

---


296. GLB Act, supra note 279, ¶ 505.


298. See, e.g., Data Protection Act 1998 (United Kingdom), §§ 60 (prosecutions and penalties) and 61 (liability of directors, etc.) (visited July 3, 2000) <http://wood.cca.gov.uk/cdp/docs.cfm> Protection of individuals and other subjects with regard to the processing of personal data, Act No. 675 (1996) (Italy), arts. 10, 23 (2), 29 (4), 32 (1), and 39 (administrative penalties), 34 (strict liability for failure to notify, with penalties including fines and imprisonment), 35 (imprisonment for violations with intent to cause loss or for gain) (visited July 3, 2000) <http://www.privacy.it/legge675encoord.html>.
ependent supervisory authority with powers of investigation and intervention, including the ability to issue orders blocking data processing or transfers, to engage in legal proceedings or refer violations to judicial authorities, and to provide individuals with judicial remedies, including compensatory damages. But rather than bringing local prosecutions against foreign data handlers, European data protection officials have attempted to negotiate stronger controls in foreign countries, notably in making arrangements for the U.S.-E.U. “Safe Harbor” discussed further below.

Regulatory bodies have relatively limited abilities to monitor and control foreign activities or to obtain effective remedies without cooperation from courts or regulators in the defendant’s country. Courts may be particularly cautious about the “extraterritorial” application of laws defining criminal offenses, for reasons that are entirely understandable: the sanctions are often more serious and carry more opprobrium than civil or administrative remedies; defendants are less likely to be aware of foreign laws; principles of sovereignty and comity urge respect for other countries’ decisions on how to order their own societies; and international cooperation in enforcement depends on the defendants’ activities being widely viewed as criminal and dangerous.

To illustrate, the Greek statute designed to implement the E.U. Data Protection Directive includes large monetary fines and the possibility of imprisonment for up to three years for any party, even if not established on Greek territory, who violates the law (including its prior licensing and notification requirements) with regard to processing data that “pertains” to a person resident (or “established”) on Greek territory. This seems to be a sweeping assertion of criminal as well as administrative jurisdiction. To date, however, there have been no reported criminal prosecutions of foreign data controllers under the Greek law. It is highly unlikely that the Greek authorities would attempt to fine or imprison, for example, the operators of a website based in California, or that they could effectively do so; the mere attempt would likely provoke international protests.

2.2. (a)(4). Summary

The newer data protection laws have not expressly limited their applicable scope to particular activities of data processing occurring on the

300. Id.
301. Id. arts. 22, 23.
303. Law no. 2472 on the protection of individuals with regard to the processing of personal data (Greece) (official English translation available from the Council of Europe, Project Group on Data Protection [CJ-PD], Strasbourg, France), art. 3(b); administrative sanctions and criminal penalties are found in arts. 19, 21, and 22.
territory of the legislating nation. To the contrary, where they have addressed the issue at all, they assert a wider jurisdiction to control the collection or use of data about individuals who reside in that country. Given the largely criminal and administrative nature of these laws, however, and the fact that they are both new and vary substantially from one country to another, it does not seem likely that courts and regulators abroad will cooperate in enforcing local sanctions. One solution may be that suggested by the U.S.-E.U. “Safe Harbor” arrangement, discussed below: an agreement not to impose local rules to cross-border data processing, so long as companies abide by an agreed set of consensus principles backed by cooperative enforcement procedures.

2.2.(b). Targeting

Some bodies of regulatory law, such as securities solicitation rules in the United States, U.K., and a number of other countries, attempt to distinguish between inadvertent contacts with a resident of the country from abroad (not regulated) and systematic efforts to target consumers in that country (which may be regulated). Existing data protection laws, as noted above, typically are triggered by the act of collecting or using certain kinds of personal data, using at least data processing facilities or communications links in the consumer’s country of residence, without inquiring into whether or not there was a conscious effort to target individuals in that territory. Under European choice of law conventions, targeting is also relevant to the mandatory application of consumer protection laws, as discussed further below.

Can negative targeting avoid responsibilities under local data protection laws? A web site operator might post a disclaimer limiting its commercial offers (or even access to pages of its site) to residents of designated countries, or conversely announce its intent to exclude residents of designated countries. To the extent that these disclaimers are effective in discouraging visitors from countries with data protection laws stricter than the web site operator’s policies, the disclaimers could reduce the operator’s exposure to criminal, civil, or administrative liabilities (and to indirect sanctions such as orders to local ISPs to block access to the site). Combined with software filters and other technological screening devices that can block access to sites, disclaimers may become more practically useful and legally effective. But there is no jurisprudence as yet indicating that disclaimers carry weight with courts or regulators, when information is automatically collected and not effectively filtered out according to the nationality of the site visitor.

Liability under the consumer’s data protection laws may be more effectively avoided by plainly disclosing the web site’s provenance and requiring visitors to signal consent to the site’s announced data practices, because data protection laws usually allow consensual processing for most kinds of personal data.
2.2.(c). Consumer Empowerment

An argument can be made that national data protection laws are doomed to be irrelevant and ineffectual when applied to the fluid and borderless Internet. And perhaps this is not to be lamented, given the evolution of technology that increasingly allows a consumer to remain anonymous on the web (unless she wants to use her credit card), to employ encryption, or to choose, perhaps automatically in the first instance, whether or not to deal with a foreign web site or a site with privacy practices inconsistent with her preferences.\(^{304}\)

It is probably too early in the development of such techniques to judge their effectiveness as a substitute for legal obligations; more likely they will continue to evolve alongside efforts to enact and enforce data privacy laws (or, indeed, to enforce compliance with the web site operator’s announced policies and automated settings). But to the extent that consumer-activated privacy techniques are available and effective, courts and regulators should reconsider the need for aggressive assertions of jurisdiction over foreign web site operators and (as discussed further below) the wisdom of overriding fully disclosed contractual choices of law and forum in cross-border online transactions.

2.2.(d). Contractual Choice of Law and Forum

There are certainly advantages for a web site operator in standardizing its online data practices and reducing its risks of liability under stricter or less-known foreign data protection laws. This might be accomplished by including express choice of law and choice of forum provisions in its contractual terms or posted web site policies. (Presumably, the consumer would not be treated as having consented to these provisions if they were not made available before the relevant collection and use of personal data.)

There might also be advantages for the consumer in establishing the applicable law with greater certainty and in designating a fair, accessible, and efficient forum for handling disputes, which might be accomplished, for example, through a private trust seal program with online mediation or arbitration features.\(^{305}\) Companies have also begun to use electronic agents and Bots to assure consumers that they are dealing only with web


sites that adhere to their desires regarding the collection, use and maintenance of personally identifiable data.

U.S. courts are likely to defer to a contractual choice of law and forum, or alternative dispute resolution, provisions, so long as they are disclosed and not “unconscionable” in the sense of depriving the consumer of any effective remedy. At least, this is true in dealing with competent adults online; the FTC and courts would not likely defer to a contractual choice of non-U.S. law, for example, to avoid the application of COPPA to online transactions with children.

In the European Union, it is possible that Member States would refuse to allow certain elements of data protection to be “waived” by contract. In addition, there is ongoing debate in Europe as to whether mandatory consumer protection laws (possibly including some measures designed to protect privacy) should always apply in business-to-consumer electronic commerce, regardless of contractual provisions to the contrary and regardless of whether the consumer was directly “solicited” or merely accessed a foreign web site.

The OECD has encouraged business and consumer groups to cooperate in designing online standards for cross-border privacy and consumer protection, as well as efficient and preferably online dispute resolution schemes. It might be well to experiment with such contractually-based programs before concluding that the detailed rules of the consumer’s home jurisdiction must always apply, a result that is sure to discourage the growth of transborder business-to-consumer electronic commerce.

The European Commission and the U.S. Department of Commerce recently produced a proposal, still undergoing final review on both sides of the Atlantic at the time of this writing, under which the Member States would allow personal data to be transferred to companies in the United States (which the E.U. does not deem to offer “adequate” protection in domestic law), if the U.S. companies undertake to treat the data in accordance with “Safe Harbor” principles based on the OECD Guidelines and

307. See, e.g., E.U. Data Protection Directive, supra note 276, art. 8(2)(a) (Member States may provide that certain sensitive data may not be processed even with the individual’s consent).
308. Brussels Convention, supra note 33, art. 3 and Rome Convention, supra note 70, art. 3 provide that a contractual choice of forum or of applicable law, respectively, cannot deprive a consumer of the benefit of mandatory consumer protection laws in the consumer’s place of habitual residence, if the consumer was solicited there or entered into the contract there. Those conditions are often difficult to establish in electronic commerce, especially if the consumer simply accessed a vendor’s web site. Hence, the European Commission has recently conducted hearings and solicited comments on the question of establishing a presumption that the consumer’s home laws apply to consumer protection in electronic commerce.
309. See supra note 265, at 7.
subject to agreed interpretive "FAQs" (frequently asked questions) and an exchange of procedural letters. Transfers to companies certifying compliance with these principles and procedures would be presumptively considered adequately protected for purposes of the Directive’s article 25. This novel approach would avoid the conflict of law issues and the ban on data transfers to countries lacking sufficiently similar legal protections. Safe Harbor would be a voluntary program, and at least some data transfers from Europe could be based instead on one of the more limited "derogations" found in article 26 of the Directive itself (chiefly unambiguous consent, transfers necessary for the performance of a contract, or protection by adequate contractual safeguards). The United States and the E.U. have not been able to agree as yet on the question of whether financial data should be deemed "adequately" protected in the United States by the new GLB Act and the amended Fair Credit Reporting Act. In the interim, however, the E.U. Member States have informally agreed not to block data transfers simply because they are destined for the United States, at least until a review scheduled for summer 2001.

Apart from the ongoing discussion over the processing of financial data, the Safe Harbor discussions have not produced agreement on the question of whether European data protection laws apply to American and other foreign web sites. Thus, U.S. web site operators are left to decide whether to certify under Safe Harbor (and voluntarily subject themselves to monitoring and enforcement procedures in Europe or the United States) or to risk the possibility that European authorities will assert jurisdiction over their privacy practices and take hostile steps (such as attempting to block access to their sites through European Internet Service Providers) that could be troublesome even if they cannot effectively impose criminal or administrative sanctions.

2.2.(e). Liability of Intermediaries

Intermediaries such as Internet Service Providers (ISPs) and e-commerce portals or electronic malls may be physically established in the seller’s jurisdiction, the buyer’s, both, or yet another jurisdiction. To the extent that they may be held accountable for, or complicit in, data privacy violations, this adds a party and perhaps another jurisdictional basis to the choice of law and choice of forum analyses.

The trend in both the United States and Europe, however, is to exclude liability for Internet intermediaries where they merely provide access and electronic meeting facilities, as opposed to taking part in the substantive

310. See supra note 266.
commercial transactions and information exchange. In the United States, the effect of section 230 of the Telecommunications Act of 1996 is largely to insulate intermediaries from liability for substantive offenses.\textsuperscript{312} Similarly, the newly adopted E.U. Directive on Electronic Commerce exempts intermediaries from liability where they merely serve as "conduits" for information.\textsuperscript{313} In both cases, greater involvement on the part of the intermediary could, of course, result in their being added as a defendant to a criminal, administrative, or civil action based on alleged violations of data protection laws. But the elimination of intermediaries as parties in most data privacy cases removes a complication from an already vexed jurisdictional question.

2.3 Conclusion

Data protection online, as in off-line commerce, is evolving with both new laws and self-regulatory programs. On the Internet, however, the proliferation of privacy laws with different specific requirements threatens confusion and jurisdictional conflict, especially because the most recent laws tend to assert a far-reaching jurisdiction to control activities involving data about local consumers. This may result in consumers avoiding foreign sites with unfamiliar privacy rules, and vendors avoiding foreign customers for the same reason.

In the interest of developing predictable standards and pragmatic remedies for consumers in an increasingly global form of commerce, the most encouraging developments are:

- the emergence of industry codes of conduct, drafted with consumer participation, including online dispute resolution features;\textsuperscript{314}
- movement toward harmonization of legal requirements, especially in Europe;
- convergence in the substantive principles applied to cross-border data transfers, as in the U.S.-E.U. Safe Harbor arrangement.

These trends hold the promise of rendering jurisdictional conflicts largely moot and encouraging both consumers and businesses to take advantage of new opportunities to trade across borders.


INTELLECTUAL PROPERTY

3.1. Introduction

Perhaps the most ubiquitous jurisdictional questions in the Internet environment relate to issues of intellectual property (IP)—patent, trademark, and copyright. Intellectual property law is primarily national in origin, but the current trend in intellectual property lawmaking is generally awareness of and sensitivity to the international implications of state law in this area. Internationalization is leading to convergence and harmonization, reducing jurisdictional pressures. Except where international treaties apply, protection of IP rights in Cyberspace depends on protection in individual countries (or regions, such as the European Union). A U.S. patent, copyright or trademark, therefore, generally confers rights within the United States, but nowhere else. Rights owners have always had to register their IP assets internationally in order to enjoy international protection. Attention to international issues in the United States was quite apparent during the recent debates over the extension of the copyright term to “harmonize” with that of the European Union. The influence of other nations’ approaches was also evident with the changes in the U.S. patent laws in 1995 to count the term as beginning with the application for rather than the grant of a patent. While there are still some fundamental differences in the approaches to intellectual property, similarity across borders is increasing.

Several coordinated efforts at international cooperation to develop uniform international standards for IP protection include the Trade Related Intellectual Property appendix to the World Trade Organization Agreement, two recent copyright conventions, and the system for mandatory arbitration of domain name disputes implemented in late 1999 by the International Corporation for Assigned Names and Numbers (ICANN).

3.2. Competing Interests

Intellectual property owners perceive their interests to be different from those perceived by some Internet providers regarding jurisdiction over Internet-based activities. The perceptions may arise from conflating juris-
diction and substantive liability. Internet providers, including both those that provide connection services and those that provide content, usually want to circumscribe jurisdiction. They do not want to be liable to be haled into court in hundreds of fora or to be subject to the substantive law of hundreds of different sovereigns. Intellectual property owners, on the other hand, favor expansive interpretations of jurisdiction, especially in the United States. American intellectual property occupies a disproportionate position in global commerce, and thus it is likely that an owner of intellectual property will be resident in the United States. IP owners favor U.S. law when they defend their intellectual property, both because it is more familiar and because they are politically effective in obtaining legislation that protects their rights vis-à-vis those of users. They are more familiar with U.S. judicial procedure and like its pretrial discovery, statutory damages, jury trials, and possible punitive damages. Accordingly, if at all possible, they want to sue in U.S. courts and have U.S. law applied to their claims. Suing in U.S. court is more likely to be an option under expansive concepts of adjudicative jurisdiction, extending to the mere availability of infringing material on web sites visible in the United States. While existing case law does not support this position, intellectual property owners would like for the courts or treaty negotiators to extend adjudicative jurisdiction without any requirements for targeting.

Even when personal jurisdiction exists, however, territorial limitations on intellectual property may deny the plaintiff a claim. Intellectual property owners, therefore, also want choice of law rules that facilitate application of U.S. law by U.S. courts characterizing infringement as a tort. Localizing the harm anywhere a web site is visible maximizes the likelihood of application of U.S. law under the principle of lex locus delicti. Although trademarks and patents differ from copyrights in that trademarks and patents arise from registration, while copyright vests in the United States without registration, the interests of patent and trademark owners in the expansive interpretation of jurisdictional concepts are similar to those of copyright owners. Allowing personal jurisdiction wherever an allegedly infringing mark is visible or an allegedly infringing product or service is advertised increases the likelihood that a U.S. court hearing a trademark or patent infringement claim will have personal jurisdiction. Localizing the harm in the place where an accused mark or product is visible or made available makes it more likely that a claim exists under U.S. law, which will be applied under tort choice of law rules.

The conflicting interests between Internet service providers and intellectual property owners are obvious. In all of the described instances in which intellectual property owners would like to see jurisdiction expanded, Internet service providers would like to see it restricted, because they do not want to be liable for allegedly infringing material made available through their sites or services. This represents a zero sum game between intellectual property and Internet interests.
3.3. The Relevance of Physicality (Difficulty of Localization)

In the law of intellectual property, physical presence bestows jurisdiction in exactly the same ways that it does for other subject areas. Where the entity is resident, maintains a corporate headquarters, or operates its Internet activities, it provides the physical presence that supports an assertion of jurisdiction.

The difficulty of localizing legally relevant conduct and disputants is not a new problem in the intellectual property area. Copyright disputes long have encountered challenges in localization. All intellectual property interests are intangible, and legal fictions are used to localize these interests. Nevertheless, localization of copyright has been aided by the association of a copyright with a physical expression of the work, in the form of a book or newspaper. The Internet removes the physical-copy mechanism for focusing the power of law. Unlike copyright, patent law has been more closely associated with things, because of its historical attachment to inventions in the form of machines. Now, the extension of patent protection to software and business methods makes it more difficult to localize infringing activities at borders.

The trademark system may be in the process of breaking down because markets, many of which historically were relatively local and thus provided a limited arena within which a trademark functioned and within which consumers might become confused by infringing marks, are global on the Internet; there is no such thing as an Internet domain name that is in use only in a local geographic area. The targeting concept, however, may mitigate this problem to some extent.

Nevertheless, all intellectual property benefits from the conventional idea that intellectual property is a form of property and that only the forum where the property is located (or the forum that created the property right through its law) has jurisdiction to adjudicate and legislate with respect to that property. This concept is more easily applied to forms of intellectual property subject to registration requirements. The place of registration is the place where the property is deemed to be located.

In rem jurisdiction has found new life despite the intangible character of Internet assets. Pursuant to the Anticybersquatting Consumer Protection Act, which took effect on November 29, 1999, in rem jurisdiction may exist in disputes for forfeiture or cancellation of a domain name or for an order transferring it to the mark owner,\(^{317}\) when a domain name registrant allegedly registered, trafficked in or used the name with a bad faith intention to profit. The statute affords mark owners in rem relief against the domain name itself (rather than the owner) if the domain name violates the rights of the owner of a registered mark or a mark protected generally under

the Federal Trademark Dilution Act\textsuperscript{318} or under section 1125(a) of the Lanham Act\textsuperscript{319} and a court expressly finds that the owner either was unable to obtain personal jurisdiction over the defendant or, through due diligence, could not find her by (1) sending a notice of the alleged violation and intent to proceed with an \textit{in rem} action under the statute to the postal and e-mail addresses provided by the registrant to a domain name registrar; and (2) publishing a notice of the action “as the court may direct promptly after filing the action.”\textsuperscript{320} For purposes of an \textit{in rem} action, the domain name is deemed to be situated in the judicial district where the domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located or where “documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.”\textsuperscript{321}

### 3.4. Targeting

A focus on targeting as a mechanism for simplifying jurisdictional disputes and making their resolution more predictable is of only limited utility with respect to intellectual property. Infringers usually seek to make money where the infringers are located; they are essentially indifferent to where the intellectual property originated. Nevertheless, some jurisdiction cases involving trademark “cybersquatting” reason that an infringer implicitly targets the place of origin, because of its implied intention to extort money from the trademark owner.

Some targeting clearly exists, however, if the issue is jurisdiction over the IP owner. Contacts are first established through the registration process for patents and for trademarks or service marks;\textsuperscript{322} this process requires the publication and, subsequently, the open dissemination of the fact of these contacts. Registration establishes first and foremost the accession of the registrant to the jurisdiction of the nation-state in which the registration has occurred. Registration also gives notice (through the publication of the patent and/or the trademark both in print and on the Internet) of the jurisdictional relation to the registrant. This clearly establishes the pri-

\textsuperscript{318} See id. § 1125(c).
\textsuperscript{319} See id. § 1125(a).
\textsuperscript{320} See id. § 1125(d)(2)(A). These additional procedures are intended to assure due process. As a general proposition, courts may exercise \textit{in rem} jurisdiction to adjudicate the status of property only if due process would have permitted personal jurisdiction over those who had an interest in the res (or underlying property). See Shaffer v. Heiner, 433 U.S. 186, 207 (1977). However, when the dispute concerns ownership of the property located in the forum, its presence there constitutes “minimum contacts” between the claimants and the forum.
\textsuperscript{322} Registration does not require the registrant to be a citizen of the nation-state in which registration has occurred and, indeed, many patents and trademarks are registered in multiple jurisdictions, presumably subjecting the registrant to jurisdiction in any of those jurisdictions as well as the requisite contacts to sue or be sued in each jurisdiction.
mary source of jurisdiction for the rightsholder. But, of course, plaintiffs always want to sue where they are located. With regard to the possible infringer, the contacts and targeting based upon the same kinds of parameters as in tort, contract, and tax are most applicable.

The registration processes for trademarks parallel those of patents in many ways and also result in the publication of the registered mark both in print and electronically in databases and on the Internet. This publication serves as notice to the world of the ownership of the trademark, but also of the jurisdictional accession of the owner to the nation-state in which registration has occurred. The more difficult jurisdictional analysis may occur when the trademark has not been formally registered, but rather is a product of the common law and the use of the mark in commerce.

It is not yet totally clear what the relationship of a domain name is to a trademark. The Anti-Cybersquatting Act now governs the practice of using another’s trademark as part of a domain name separate from the trademark owner. That Act solves the jurisdictional question by allowing the trademark owners to sue domain names themselves, rather than the domain holders. Almost a dozen *in rem* actions were filed in the United States District Court for the Eastern District of Virginia in the first two months of 2000.323

Because, under U.S. law, the package of rights associated with copyright is created at the point of the fixation of the work324 there is no requirement of registration325 that would serve to create jurisdictional presumptions in the same way that patent and trademark would.

### 3.5. Power Shifts

The conventional wisdom is that digital technology shifts the balance of power in favor of infringers and against the interests of intellectual property owners. No doubt this is true in many situations, but it is important to realize that digital technologies and the Internet also create new weapons of detection and proof of infringement for intellectual property owners, and new forms of protection, because they permit copyright owners to “format” their material so that it is more difficult to copy. Also, new technologies, including encryption, permit copyright owners to charge fees

323. 59 PAT., TRADEMARK & COPYRIGHT J. 723 (Mar. 31, 2000). This, of course, merely has the effect of requiring Network Solutions, Inc., headquartered there, to release the pertinent information regarding the registrant for the purposes of the lawsuit.

324. This is the point that was established by the Berne Convention and is now used by all countries which are signatories to Berne, including the United States. 17 U.S.C. § 102 (1996).

325. In the United States, registration is a prerequisite to filing an infringement lawsuit for most works, but is not necessary to give rise to the rights themselves. 17 U.S.C. § 411 (1996).
for every use of their material rather than allowing unlimited use for anyone who has bought it or obtained a license.

In this regard, despite enthusiastic promotion of various complex centralized copyright licensing and clearingsine schemes in the late 1980's and early 1990's, the marketplace has shown no inclination to embrace these schemes, preferring the flexibility and efficiency of decentralized transactions.

3.6. Contractual Choice

Contractual choice plays no role in intellectual property piracy cases. In these cases, infringement is a relatively pure tort, and the claimant and respondent have no prior relationship in which choice of forum or law can be expressed. In other cases, involving claims of infringement arising from someone who exceeds the terms of a license, as an infringer who is privileged to use intellectual property for one purpose and impermissibly uses it for another, contractual choice may be relevant. The same issues relating to contracts of adhesion may operate when consumers are involved in these contracts as with respect to other consumer contracts.

Operation of the Internet domain system has, however, provided a unique opportunity for comprehensive use of contractual choice. Under rules developed by ICANN, Internet domain name registrars must agree to submit disputes over domain names that allegedly infringe trademark rights to alternative dispute resolution panels, such as those set up specifically for these kinds of disputes by the World Intellectual Property Organization. This ICANN dispute resolution machinery is one of the most interesting institutional innovations with potential to reduce transaction costs, including uncertainty, in Cyberspace.

ICANN dispute resolution procedures are enforced by contract. By registering a domain name, an applicant is deemed to represent that:

- the statements set forth in its registration agreement are complete and accurate;
- the registration, to the best of the applicant's knowledge, will not infringe upon or otherwise violate the rights of any third parties;
- the domain name is not being registered for an unlawful purpose; and
- the registrant will not knowingly use the domain name in violation of any applicable laws or regulations.\(^\text{326}\)

Under the terms of the Policy, an ICANN registrar reserves the right to cancel, transfer or otherwise change domain name registrations in response to an order from a court, arbitral tribunal, ICANN Administrative

---

Panel, pursuant to the terms of an applicant's registration agreement or other legal requirements, or in response to written or appropriate electronic instructions from the registrant.\textsuperscript{327}

Registrants are contractually required to submit to mandatory administrative proceedings if a third party complainant asserts that:

- a domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
- the registrant has "no rights or legitimate interests in respect of the domain name";\textsuperscript{328} and
- the domain name was registered and is being used in bad faith.\textsuperscript{329}

An administrative proceeding may be initiated by any third party mark owner, who must select a particular Provider from among those approved by ICANN.\textsuperscript{330} The World Intellectual Property Organization and other Providers identified on ICANN's web site are deemed to be "Approved Providers."

\textsuperscript{327} Id. § 3.
\textsuperscript{328} Id. § 4(a)(ii). This element may be negated by evidence that:

- before any notice of the dispute, the registrant used or had made "demonstrable preparations to use" either the domain name or a name corresponding to it "in connection with a bona fide offering of goods or services;"
- the registrant (either individually or as a business or organization) has been "commonly known by the domain name" even if it "acquired no trademark or service mark rights;" or
- the registrant is making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain by misleadingly diverting consumers or tarnishing the mark at issue in the dispute.

\textsuperscript{329} Id. § 4(c).
\textsuperscript{330} Id. § 4(a). Bad faith registration and use may be evidenced by any of the following circumstances, among others:

- registration or acquisition of a domain name "primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the . . . mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name;"
- registration of a domain name in order to prevent a mark owner "from reflecting the mark in a corresponding domain name," but only in cases where the registrant has engaged in "a pattern of such conduct;"
- registration of a domain name "primarily for the purpose of disrupting the business of a competitor;" or
- using a domain name to intentionally attempt "to attract, for commercial gain," Internet users to a web site or other online location "by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement" of the web site or location (or product or service offered at such site or location).

\textsuperscript{330} Id. § 4(d).
Under the applicable rules of procedure, the complainant generally is required to consent to jurisdiction in either the location of the registrar’s principal office or the address for the registrant, as listed by the registrant in the WHOIS database.

Relief from administrative panels is limited to cancellation or transfer of a domain name.331 The administrative panel proceedings, moreover, do not preclude judicial relief. Either party may submit the dispute to a court of competent jurisdiction.332 In fact, registrars may not implement any cancellation or transfer order for ten business days after being notified of a decision, in order to allow an adversely affected registrant the opportunity to initiate litigation. If, during the ten day period, a registrant provides “official documentation” evidencing the commencement of a lawsuit (such as a file-stamped copy of a complaint), the registrar will take no further action until notified of a judicial decision, settlement or dismissal or withdrawal.333

ICANN dispute resolution proceedings offer a potentially uniform, quick and inexpensive mechanism for resolving international disputes involving cybersquatting. Dispute resolution may be valuable in cases involving foreign registrars not otherwise subject to local jurisdiction (although not necessarily foreign registrants of names registered with U.S. registrars because of the potential availability of in rem relief under the Anticybersquatting Consumer Protection Act discussed earlier) or where neither party challenges the outcome. Dispute resolution procedures also may prove effective when a registrant seeks to transfer a domain name because ICANN has authority to ensure that the name remains subject to the proceedings (whereas under the statute the complainant must notify registrars and registries directly).

3.7. Interaction Among Jurisdiction and Intermediary Liability

As Ithiel de Sola Pool observed in the early 1980’s, copyright conceptually always has focused on choke points or bottlenecks in the distribution of ideas.334 Publishers and book sellers were the traditional choke points, and the battle over intermediary liability in the dialogue over the Clinton Administration “White Paper” and in the drafting of the Digital Millennium Copyright Act exemplifies the search for new choke points as enforcement targets.

331. Id. § 4(f). According to the Policy, all disputes other than those that qualify for administrative proceedings must be resolved in litigation between the affected mark owners and registrants.
332. Id. § 5.
333. Id. § 4(k).
Traditionally, republishers of infringing material were liable for infringement under a variety of theories. The Digital Millennium Copyright Act creates a safe harbor for intermediaries who provide information sufficient to allow copyright owners to complain of infringing material and who establish procedures to block access to the accused material pending resolution of the dispute. On the other hand, although the Amended Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market contains, in section 4, a limited immunity for intermediary service providers, the proposed European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, contains no provisions relating to intermediary liability.

**PAYMENT SYSTEMS/BANKING**

The receipt, transmission, loan and safekeeping of funds provided by financial services companies can be divided into two primary activities: (1) the traditional business services of banks, such as accepting deposits and making loans (banking), and (2) the operation of systems and structures to facilitate the transfer of monetary value (payments systems). The jurisdictional aspects of the two activities are not identical, either as conducted traditionally or in Cyberspace. The terms "banks" and "banking" refer to a wide variety of financial intermediaries and financial intermediation; "banks" are simply one of many institutional elements in the total global payments system.

**4.1 Financial Services and Jurisdiction**

**4.1.(a). Banking**

Financial services providers originally were limited to providing services within the boundaries of the sovereign that authorized them to conduct such business (e.g. states), or within even narrower restrictions imposed by that sovereign’s financial institution regulators (e.g. counties or cities). The power to establish limits on a financial institution’s activities, investments, and market has traditionally resided in chartering nation states (and sub-national units) as an outgrowth of their authority to control persons and things, as well as the creation and movement of money, within their borders. A financial institution has generally been subject to personal, regul-

337. In the United States, for example, the Comptroller of the Currency is the primary federal regulator of national banks. The Comptroller's authority, and the powers, investments, and activities of national banks are governed by the National Bank Act of 1863. See, e.g., 12 U.S.C. § 24 (1998). See generally THOMAS P. VARTANIAN ET AL., 21ST CENTURY MONEY, BANKING & COMMERCE 13-31 (1998). Other financial institutions (thrifts, credit unions, etc.) are regulated by separate federal agencies, and those chartered to operate by individual states are supervised by a state-level regulator.
ulatory, and enforcement jurisdiction at least within its “home” forum, that is, the forum under whose laws it was chartered and in which its principal office is located. That regulatory jurisdiction has included financial institution examination and supervision (prudential supervision).

The realities, however, of cross-border commercial activity, customer demand, improved communication infrastructure, the need to diversify risk, and competition among different types of financial services providers required that financial institutions extend their services beyond these political boundaries. Cross-border banking activities tended to subject the financial institution (1) quite directly to personal jurisdiction in the non-home forum in which the activity occurred, e.g., the domicile of the depositor and the situs of the property securing a loan, and (2) also to regulatory jurisdiction with respect to the various consumer protection and conveyancing laws of the non-home forum or fora that may be applicable to the particular transaction. Generally, a foreign jurisdiction would not be able to regulate the activities of a financial institution chartered elsewhere unless the volume of those activities in the forum provided the foreign forum with a sufficient basis to assert a broader application of its laws.

In the United States, during the period just prior to the advent of the Internet, financial institutions had, through different organizational techniques and communications technologies, in conjunction with changes in the law and expansion through the acquisition of failing institutions, expanded the geographic range of their operations to the point that, for all practical purposes, they could function anywhere they wished. The advent of the Internet as a delivery system for financial products and services alters the scope and scale of this trend but does not substantially change the nature of the issues being raised. By speeding up banking business processes, by producing greater flows of financial products and services, and by intensifying the marketing process, the Internet creates these same jurisdictional issues faster and more widely.

For example, in the United States, the jurisdictional consequences of banking changes based upon what the issue is. A commercial bank, savings bank, savings and loan association, or credit union is subject to the regulatory jurisdiction of a chartering authority (e.g., the state or federal government). That chartering authority determines what activities the institution may engage in (e.g., deposits, lending, letters of credit, insurance), where it may construct physical facilities (e.g., branches, loan production offices), and where it may offer products and services through means that are not necessarily tied to a branch location. Most financial institutions, whether federally or state chartered, may incorporate subsidiaries under state law that may establish facilities and provide similar or different services to customers throughout the country (e.g., mortgage banking or consumer finance subsidiaries). Many of these services may be “non-financial” in nature, a fact that reinforces a point made below that there is scant
basis for treating banking services and the services of any other e-merchant differently from most jurisdictional standpoints.

A financial institution may, however, also become subject to prescriptive jurisdiction wherever it targets and serves consumers. Thus, a bank headquartered in Minnesota may find that its financial subsidiary incorporated in Missouri is subject to Mississippi consumer laws when that subsidiary makes loans in Mississippi.

As mentioned above, the use of the Internet to provide financial products and services almost anywhere complicates these issues further. When state-chartered banks began entering neighboring states and then eventually began offering the products and services determined and regulated by one state in many states, state regulators had to decide how to apply their regulatory jurisdiction and how to examine the activities of such banks. Who should determine what products and services a Minnesota bank may offer in Mississippi, and who should be able to examine the Mississippi operations of that bank (particularly if the Minnesota bank has no physical premises in Mississippi)? To deal with this trend in the physical world, state and federal regulators reached agreements dividing up and delegating the responsibility for the regulatory aspects of jurisdiction. As banking institutions around the world have expanded beyond their borders, regulators around the world have entered into similar compacts as to certain aspects of their regulatory jurisdiction. Neither financial institutions nor their regulators, however, can always control jurisdictional choices; consumers and businesses can attempt to sue financial institutions anywhere and argue for the application of whatever laws they consider appropriate.

But even this system of national regulatory “treaties” may be coming under pressure as the Internet allows a financial institution to conduct its business everywhere on the planet without the need for any retail location. Indeed, the extent to which foreign banks can defeat the effects of U.S. banking laws and “treaties” by offering their products and services to U.S. citizens underscores the need for a reevaluation of banking laws and the consumer protections that may apply. The latter are more properly explored by other working groups that have contributed to this Report.

4.1.(b). Payment Systems

Systems to facilitate the local and cross-border transfer of value have existed for many centuries and have been largely founded upon a web of agreements among private parties, with the support of laws that have as much enabled as governed. As changes in the global economy and tech-

nological developments made cross-border commerce common, participants in the payments systems, including traditional financial institutions, developed structures that were able to handle greater volumes of payments, operate more efficiently and rapidly, and function over larger geographic areas.

It is in the nature of these systems to minimize and, if possible, eliminate disputes; without disputes, there are no jurisdictional issues. This is a model from which many other disciplines can learn. The volume of money in all its various forms that is transferred across borders today through existing payment systems is enormous. The system cannot tolerate disputes that might disrupt that flow. Hence, whether in reference to currency exchanges, letters of credit, or consumer transactions, payment systems have been constructed in such a manner that disputes are resolved outside the stream of commerce and according to established rules. These rules are created either by a governing entity (e.g., Nacha as to the operation of the automated clearinghouses system) or through contracts among the members participating in the system (e.g., MasterCard, VISA, American Express, etc.). All participants in these systems have a powerful incentive to "play by the rules." The price to a "player" to participate in the established system is to agree to established "rules" that are designed to allocate risks and losses either equitably or broadly across the system. The "rules" establish all the relative liabilities and responsibilities of the parties, and no party wishes to pay the penalty of exclusion for failure to play by the rules. The addition of sophisticated and powerful computing technologies and the advent of Internet transactions to these established mechanisms to conduct value transfers across political boundaries have resulted in few, if any, changes with jurisdictional significance.

4.2 The Relevance of Physicality (Localization)

The advent of the Internet and other mass electronic communication media has diminished substantially the importance, if not the meaningfulness, of the geographic location of various physical factors (parties and their associated infrastructure) as a basis for making jurisdictional determinations with respect to activities conducted in Cyberspace. Both banking institutions and payment systems have dealt with this issue even before the recent explosion of electronic commerce, because they have used proprietary credit card, wire, ATM and ACH networks to move money for more than 30 years, and financial institutions were among the "early adopters" in using information technology to automate their operations.

4.2.(a). Banking

Traditionally, financial institutions delivered their products and services mainly through physical facilities, such as branch office networks, whose
frequently imposing presence was obvious and tangible. The development of enhanced communication media, including the Internet, however, has created a world in which the same business services can be delivered by a financial institution that has no physical facilities other than a computer operations center (also its “headquarters”) and that maintains most of its records in intangible electronic form. The same technological development has enabled the institution to expand vastly the geographic range of its operations and to locate its own (or out-sourced) infrastructure virtually anywhere. In the main, the products and services of the financial institution are not evidenced physically but by digital files. The banking customer can access the institution’s web site from anywhere—in his home, in a cybercafe in any city on the planet, or traveling in an airplane across multiple jurisdictions while using a laptop with access to a wireless network. The bank’s web site’s server could be anywhere, and, indeed, as a result of mirror sites, the web site could be “located” in several places at once. The financial institution is, at the same time, in no particular place and everywhere at once.

In addition, technological developments have created a world in which financial institutions may be subject to the jurisdiction of an indefinite number of non-home fora for the reason that customers can obtain their services simply by being physically present in non-home fora and using physical facilities (e.g., any terminal with Internet access) located in those fora. This is a problem because of the bewildering variety of local regulations applicable to banking transactions, the adversity of the potential penalties, the high transaction costs of compliance, and the perverse incentives favoring larger institutions that can afford the compliance costs.

In all these various respects, there are no meaningful differences between a financial institution and any other e-commerce merchant, except for the highly regulated nature of banking. There is one respect, however, in which the implications of this diminished “physicality” apply with special force in the banking world. Where a financial institution is considered to be “located” continues to have special relevance when the chartering or similar authority of a nation state (or subnational unit) exercises its right to supervise and examine the institution’s financial status. This is true, even though with the advent of developments like interstate banking authority in the United States and European Union directives on cross-border financial services and distance marketing, the “location” of a particular financial institution is largely irrelevant to banking consumers as far as their individual transactions are concerned.

With respect to financial institutions, there is a key distinction between transactional risk and systemic risk. Regulatory jurisdiction to examine and supervise must be completely clear and, as a result of compacts and cooperation among regulatory authorities, must leave no gaps in coverage. Otherwise, a substantial risk to the soundness of the entire system is created. Within and among certain developed national and supranational
fora, such as the United States or E.U., compacts for supervisory cooperation and other protective modalities are in place that are generally recognized among their participant states and employed by the market. As mentioned above, in the United States, state regulators have created such compacts with respect to overlapping jurisdictional issues that arose in the 1980’s from the national expansion of banks in the United States. International regulators have constructed similar regulatory compacts with respect to capital requirements.\textsuperscript{339} Mutual recognition by sovereign states, however, of the circumstances under which their financial institutions could be subject to the regulation of another state could become strained as the number of actual and potential participating institutions, and their respective regulating states, continues to expand. For these reasons, cooperation among financial institution safety and soundness regulators seems especially imperative in the world of electronic banking.

4.2.(b). Payments Systems

In the case of payment systems, the concept of physicality is even less relevant than it is in the case of banking business services. In the case of payment systems, (1) the payment transactions occur using an infrastructure whose physical components can be located nearly anywhere; (2) the physical paths that the transactions take in flowing through that infrastructure are, to a large degree, random; (3) the various traditional ways in which the payors and payees can be "located" (state of incorporation, address of headquarters, domicile, etc.) are frequently irrelevant to the transaction; (4) the payor could be anywhere at the time of payment; (5) the payee’s web server (or other recipient facility) could be anywhere, and, indeed, as a result of mirror sites, the web site could be "located" in several places at once; (6) the payor “pays” by providing the merchant with a recognized, but essentially intangible, mode of payment, typically a credit card account, wire transfer or ACH account number; (7) the process for transmitting payment information and reducing it to an acceptable form of payment is nearly universally agreed upon; and (8) the verification of the information, currency conversions or exchanges, and billing and crediting transfers all occur seamlessly no matter where the merchant, consumer and the connecting infrastructure are located. In general, under existing electronic payment systems, the location of the payor and the payee and all their connecting infrastructure is wholly irrelevant to the transaction.

Underlying all these specific reasons for the decreased relevance of physicality is the fact that the payments system is essentially an already ubiquitous infrastructure. Commercial transactions and payments transactions

are mirror images of one another; that is why, as a matter of National Income Accounting, the total value of all goods and services exchanged in a given period in a jurisdiction must equal the total amount of the payments exchanged with respect to those goods and services. The payments system is the infrastructure over which the payments flow. It is like the road network, the telephone system, or the Internet backbone. It seems more likely that the commercial transaction underlying the movement of funds will generate a jurisdictional issue than that the corresponding payment will; and it is not likely at all that the institutional vehicle for transmitting the payment will generate a jurisdictional issue. Further, a physical factor is of greater use in deciding a jurisdictional issue to the extent that it can be located in one place rather than another. A payments system, however, like any infrastructure, is of more use to the extent that it is universally available, that is, "everywhere." By its nature the payments system is, therefore, not useful in deciding jurisdictional issues on a physical basis. This is even more the case to the extent that the payments system is conducted electronically.

4.3. Targeting

The concept of "targeting" in a jurisdictional sense rests on the facts that (a) a party can fairly (as a due process matter) be held to have intended the effects which have occurred in a particular forum as a result of its actions; and (b) those effects can be a proper basis for subjecting the party to jurisdictional consequences in that forum. While targeting has been a traditional basis for making jurisdictional determinations, the advent of the Internet and other electronic communication media have caused that basis to become more prominent because, in a world in which an electronic communication can be exchanged by everyone everywhere, it has become even a more useful and fairer basis to distinguish where the business is being done in Cyberspace for jurisdictional purposes.

4.3(a). Banking

"Targeting" is an efficient way of making jurisdictional determinations in Cyberspace. In many cases, financial institutions become subject to jurisdiction in a non-home forum when they "target" consumers in the non-home forum. For example, if a financial institution makes home mortgage loans in such a jurisdiction (electronically or otherwise), it will become, as to that transaction, subject to the regulatory jurisdiction of that forum's conveyancing laws and consumer protection laws. Similarly, where the "targeting" and delivery of products and services occurs electronically, the conventional Zippo analysis prevails. To that extent, insofar as financial institutions are deliverers of business products and services, there is no meaningful difference between them and other e-merchants.
4.3. (b). Payments Systems

As a general proposition, the participants in the payments system, operating as such, do not target fora or persons in fora. The payments system is essentially a conduit for the parties that use it (which parties may target fora). Hence, the concept of targeting is largely irrelevant.

These points may be illustrated as follows. Any web site that seeks to conduct e-commerce must incorporate a system to process "value" in exchange for the product or service offered. Most commonly, that system will involve one or more aspects of traditional payments—currency, credit cards, electronic transfers, etc.—and will of necessity require the involvement of a financial institution to process the payments made by purchasers. Thus, it may appear that the financial institution is targeting purchasers in the fora in which they are domiciled and should be subject to jurisdiction there. The financial institution, however, is operating as an element in the operation of the payment systems and is "targeting" that customer as a responsible party in a web-based transaction, not as its own customer but in effect on behalf of the merchant. The ancillary involvement of a financial institution as payment processor for the e-merchant that operates a commercial web site should not subject that institution to the jurisdiction of the state whose residents are targeted by that web site. Essentially, from the jurisdictional point of view, the payments system should be regarded as a collective Internet Service Provider. This point is discussed more fully below.

4.4. Power Parameters

4.4. (a). Banking

In recent years, there has been a very substantial increase in the ability of consumers to use technological means to comparison shop for various financial products and services. These means will only become more powerful in the future. This trend will help the consumer protect herself and may weaken the case for certain forms of consumer protection. This will depend on the effectiveness of consumer Bots, competition and self-regulatory mechanisms. At the same time, the technologies that underlie the more powerful consumer shopping tools also provide more powerful marketing tools to sellers. Further, it is not clear that the new consumer tools are as yet being used to any great degree to effect major sensitive financial transactions such as home mortgage loans (although they are widely used by consumers to narrow the number of competing providers with which online and off-line negotiations are held). In sum, no alteration in current jurisdictional rules seems advisable on that account, at this time, unless it is in the direction of reducing regulatory burdens on financial institutions which are meant to protect consumers as technology tempers the balance in kinds of circumstances that give rise to the need for such protections.
4.4. (b). Payment Systems

As electronic bill payment and presentment, person-to-person payment systems, smart-card technologies, and other encrypted micropayment systems become more widely accepted, they will require different regulatory approaches. But until they can sufficiently alter the relative power positions of the providing and using parties, the need for an alteration of current jurisdictional principles in the payment systems is not clear.

4.5. Contractual Choice

In an electronic banking scenario, the factors that suggest reliance upon the ability of parties to contract with one another for jurisdictional purposes are largely the same as those discussed in sections 1 and 6 concerning Advertising and Consumer Protection and the Sale of Goods. Developments that have resulted in some convergence with respect to the relevant substantive law regarding contractual choice of law in the banking area, such as the E.U.'s Second Banking Directive, earlier regional banking compacts in the United States, the Gramm-Leach-Bliley legislation in the United States, and the financial institution and investment provisions of the North Atlantic Free Trade Agreement, deal mainly with financial institution powers and allocation of regulatory authority rather than with substantive areas of the law regarding contractual choice.

4.6. The Intersection Between Jurisdiction and Substantive Liability for Intermediaries

Technology creates certain "choke points," that is, points where intermediaries (entities other than the primary parties) may be able to halt or condition electronic transactions. In cases where it is not feasible to obtain jurisdiction over the primary parties involved in a transaction, there may be tendency for nation states to achieve their regulatory goals by changing the applicable substantive law to impose certain obligations and liabilities on intermediaries subject to their jurisdiction. Payment systems themselves represent important choke points in commerce. Almost all payment systems create a fund from which dispute resolution awards can be satisfied (letters of credit and garnishments of bank accounts are examples), and they may involve prominent neutral third parties who can become dispute resolvers. Credit card chargeback mechanisms are an example.

This development is not seen with respect to banks insofar as they are rendering normal banking services; in that capacity, they are essentially primary parties. This development, however, is seen routinely with respect to the payments system generally and with respect to banks as participants in the payments system. For example, the Bank Secrecy Act in the United States 340 imposes substantial duties of investigation and reporting on

money and payments processing intermediaries. The Act provides severe institutional and personal penalties for non-compliance, which arguably require the intermediaries to act in a manner that is not necessarily consistent with the financial interests and privacy rights of their own customers and customers of their correspondents. The developing global personal data protection regime based mainly on E.U. Directive 95/46, and in particular on its “onward transfer” and enforcement requirements, provides another interesting example. Very substantial amounts of the personal data transferred globally are transmitted through the payments system. The prohibitions on onward transfer contained in the developing global privacy regime have the effect of using the payments system as a “choke point” to cause the substantive regulatory requirements of the sending jurisdiction to be exported to the receiving jurisdiction and to establish personal jurisdiction over residents of the receiving jurisdiction in the courts of the sending jurisdiction.

The imposition of obligations on the intermediary systems, particularly obligations involving potential exposure to liability, should never be the first choice; the first choice should be to impose obligations and liabilities on the primary parties. To blame the ISP for the content of a particular web site is akin to holding the telephone company responsible for a malicious telephone call. Similarly, a financial institution should not be subjected to responsibility for the merchant’s errors, because the financial institution is only acting as a processor within the payment system. In addition, an infrastructure is more useful to the community it serves to the extent that it is easily and efficiently open to users generally and provides its services rapidly, interoperably, and with minimum necessary cost. Hence, in the absence of a chargeback system on the primary parties, the imposition of an obligation on infrastructure results in a general system cost to all users. This may be resisted by non-primary parties as unfair and may result in higher administrative costs because it is applicable to the whole system. Further, there is a tendency to generate trade-offs that are difficult to weigh and administer (the desirable goal of controlling abusive speech on a corporate e-mail infrastructure can be achieved but only to the extent that undesirable costs in loss of privacy and systems overhead are also incurred).

Finally, there is a difference between the imposition of obligations on an intermediary and the imposition of liability. In the former case, the intermediary raises its prices to cover the transactional costs of meeting the obligations. In the later case, the intermediary raises its prices to cover both the transactional costs and the costs of building reserves and/or purchasing insurance to cover the costs of anticipated liabilities. In both cases it is spreading risks and costs to all users, but the costs to the total system are potentially much greater in the latter case.
4.7 General Conclusions

In general, "banks," insofar as they are deliverers of business products and services by electronic means, should be regarded as not meaningfully different from most other e-merchant conducting business-to-business, business-to-consumer, and business-to-government commercial activities. Banking does, however, share with certain other types of e-commerce a special public welfare sensitivity because of the potential for systemic damage if their activities are conducted unsoundly. Securities, insurance, telepharmacy, and telemedicine are other examples of such types of e-commerce. From a jurisdictional point of view, this means that the expansion of e-commerce with respect to these types of business requires a special degree of cross-border cooperation among regulators, self-regulatory bodies, and relevant private organizations.

PUBLIC LAW/GAMING

Changes in the global economy and technology have challenged traditional assumptions regarding jurisdiction. Cross-border contact and international transactions have raised fundamental questions with respect to the authority of a sovereign under identified circumstances to assert jurisdiction over persons not physically within its boundaries and to regulate conduct that occurred, at least in part, outside those boundaries. The issue of cross-border regulation of Internet activity has come to the forefront in connection with Internet gambling. It is, indeed, one area among the many considered in this Report where developing concepts of online jurisdiction may be used as a shield to avoid responsibility for conduct deemed illegal in the forum where it is being offered.

According to a Final Report published in June 1999 by the United States' National Gambling Impact Study Commission (the "NGISC Final Report"), annual revenues from Internet gambling surpassed $650 million in 1998, and are expected to exceed $10 billion by the year 2000. This dramatic increase may be attributed to several factors, including increased Internet access, improvements in technology which facilitate online betting, increased public confidence with online financial transactions, and national licensing for Internet gambling operations by several countries.

341. NATIONAL GAMBLING IMPACT STUDY COMMISSION, FINAL REPORT, at 2-15 (June 18, 1999) <http://www.ngisc.gov/reports/> [hereinafter NGISC FINAL REPORT]. According to the report, revenues from Internet gambling doubled from previous year. Id. at 2-16.
343. NGISC FINAL REPORT, supra note 341, at 2-16.
5.1. The Relevance of Physical Location

The application of extraterritorial jurisdiction (whether between jurisdictions within one country or between countries) typically focuses on the location of the activities giving rise to a legal claim. Physical location becomes an issue with respect to Internet gambling, because online gambling ventures are typically organized and located in jurisdictions in which gambling is legal and often reach into jurisdictions where such activity is illegal.

Most Internet gambling operations used by U.S. customers are physically located outside the United States, in jurisdictions where gambling is legal.344 Because cyber-casinos can be based in countries where gambling is legal and reach users in countries where gambling is prohibited, there is increased concern in many countries that, to the extent these offshore online casinos are unlawful, law enforcement and regulatory authorities cannot reach across national boundaries to prosecute the perpetrators in an effort to protect consumers.

In the United States, the gambling industry is regulated by a network of state and federal legislation.345 All but two states in the United States having some form of legalized gambling, and casinos exist on Native American tribal reservations throughout the United States.

In a number of personal jurisdiction cases involving online gambling, operators of online casinos have been held to be subject to the jurisdiction of U.S. state courts, based on the interactions by these remote casino operators with customers in such states. For example, in July 1999, a New York State court held that the state had the authority to enjoin a foreign corporation licensed to operate a casino offshore from offering gambling to Internet users in New York.346 The defendant in that case was a Delaware corporation that maintained corporate offices in New York. The defendant’s wholly owned Antiguan subsidiary was licensed by the government of Antigua to operate a land-based casino. The defendant’s subsidiary developed interactive software and purchased computer servers which were installed in Antigua to allow users around the world to gamble from their home computers. The defendant promoted its casino through

344. Nations including Australia, Antigua, Barbuda, Austria, Belgium, Costa Rica, Germany, South Africa, and several regions of the United Kingdom have licensed Internet gambling operations. NGISC Final Report, supra note 341, at 5.1 n.5.


Internet advertisements and print ads which were accessible to New York residents.

The fact that the activities were undertaken by an Antigua company did not prevent the court from ruling that the defendant had violated both state and federal gambling laws. State Supreme Court Justice Charles Edward Ramos found that:

It is irrelevant that Internet gambling is legal in Antigua. The act of entering the bet and transmitting the information from New York via the Internet is adequate to constitute gambling activity within New York State.347

The defendant was also found liable for selling unregistered securities, in violation of New York State law.

5.2. Targeting

In a number of cases involving gambling, whether a web site operator has “targeted” users in a given forum has been found relevant in the assertion of personal jurisdiction over such operators. Gambling web sites may reach customers in multiple jurisdictions. Operators of gambling sites may have to consider whether they are targeting customers in locations where such activity is illegal.

Targeting was discussed in one of the early cases involving Internet gaming. In State v. Granite Gate Resorts, Inc.,348 the Attorney General of Minnesota brought an action alleging deceptive trade practices, false advertising, and consumer fraud over the Internet against the defendant, who operated an online casino based in Belize.349 The complaint was filed based upon the fact that the defendant, on his web site, advertised in Minnesota that gambling on the Internet was a lawful activity, which in fact in Minnesota it was not.350 The Court of Appeals of Minnesota adopted a five-factor test for determining whether the defendant had es-

347. Id. at *5.
349. 568 N.W.2d at 716-17. The district court found that the defendant's activities over the Internet constituted minimum contacts with the state, and its exercise of personal jurisdiction was the issue on appeal.
350. Id. at 717. The court's opinion does not address the issue of applicable law. It (and presumably the parties) assumes that Minnesota law governs the issue of legality with respect to a gambling site accessed (or at least accessible; as a sanction for refusing to comply with discovery orders, the court established as a fact that the defendant's mailing list contained the name and address of at least one Minnesota resident) in the state. The law applied to determine the legality of conduct without reference to private claims of damage is always that of the forum. If it does not apply to the conduct (for example, because the legislature chose to make it illegal to operate a gaming site only if the site was physically located in Minnesota), the suit is dismissed.
tablished minimum contacts with the state. The court found that the defendant, in advertising his gambling service on the Internet, demonstrated a clear intent to solicit business from numerous markets, including Minnesota. This intent was evidenced by the multiple contacts the defendant forged with Minnesota as a result of its web site, including telephone calls from Minnesota residents to the defendant’s toll-free telephone number, the addition of Minnesota residents to a mailing list, and “hits” on the defendant’s web site. The court noted that “[d]efendants keep track of who is accessing their web site, and therefore know that Minnesota computers are accessing them.” Additionally, the cause of action at issue arose out of the advertisements on the web site and implicated Minnesota’s strong interest in “enforcing [its] consumer protection statutes and regulating gambling.”

Weighing the interest of Minnesota in enforcing its consumer protection laws against the inconvenience it would cause the defendant to defend against such a suit there, the court found that “[t]he state’s interest in providing a forum to enforce its consumer protection laws weighs in favor of exerting jurisdiction over appellants.” Therefore, the court held that the defendant’s Internet activities constituted purposeful availment of the protections and benefits of doing business in Minnesota, “to the extent that the maintenance of an action based on consumer protection statutes does not offend traditional notions of fair play and substantial justice.”

The Granite Gate court found that the defendant’s web site possessed a level of interactivity with Minnesota residents warranting the exercise of personal jurisdiction.

351. *Id.* at 718. The five factors employed by the court were: (1) the quantity of contacts with Minnesota; (2) the nature and quality of the defendant’s contacts; (3) the connection between the cause of action and the defendant’s contacts; (4) the state’s interest in providing a forum; and (5) the convenience of the parties.

352. *Id.* at 721.

353. *See* note 349, supra.

354. 568 N.W.2d at 718-19.

355. *Id.*

356. *Id.* at 721.

357. *Id.* at 722.

358. *Id.*

359. *See also* Missouri ex rel. Nixon v. Interactive Gaming & Communications Corp., No. CV97-7808 (Mo. Jackson County Cir. Ct. May 22, 1997). This case also resulted in a similar holding. The defendant, a Delaware corporation, actively sent promotional brochures into Missouri, and other promotional materials via e-mail. Further, the defendant, when questioned by an investigator from the Missouri Attorney General’s office as to whether it was legal in Missouri to gamble through the site, answered in the affirmative. Therefore, the court held that the active solicitation of business in Missouri fell under the state’s long-arm statute and enjoined the defendant from conducting further business within Missouri or with residents of the state.
In *Shapiro v. Santa Fe Gaming Corp.*, however, the court found that a Nevada defendant's web site was purely informational. The court discounted the plaintiff's claim that operation of the web site along with the maintenance of a toll-free number constituted "transact[ing] business in Illinois" in satisfaction of the venue requirement of 15 U.S.C. section 7899. More importantly, the court noted that a contrary holding "would impermissibly subject millions of people to personal jurisdiction merely because they had a website, e-mail address or toll-free telephone number."

5.3. Power Parameters

The Internet has changed the traditional power relationship between sellers and buyers. Traditionally, sellers were thought to seek out buyers. E-commerce theoretically empowers buyers, by giving them the tools necessary to seek out the sellers offering goods and services under the most favorable terms. The Internet has also lowered barriers to entry for smaller businesses.

It is unclear to what extent this framework of analysis applies to Internet gaming. Certainly, the Internet permits bettors in places where gambling is illegal to seek out sites at which they may place bets. The Internet has also permitted many small gambling operations to compete in the online marketplace (to an extent which would not be possible in the brick and mortar marketplace). Given the nature of the transactions at issue, consumers are putting themselves at great risk by wagering through sites against which they will have little legal recourse.

Apparently there is no case law to date in the United States in which an off-shore operator of a cyber-casino which does not actively solicit U.S. customers has been held liable for accepting a wager from a U.S. resident who actively sought out such a casino.

5.4. Contractual Choice

Most commercial web sites incorporate such clauses into the terms of use governing such sites. Although it is unclear whether choice of law provisions may be used to govern regulated activity (such as gambling),

361. Id. at *6.
362. Id.
363. Id. Actually, such a conclusion need not follow. The mere transaction of business does not subject a defendant to jurisdiction unless the claim is at least related to the business transacted. Here, for example, the claim was for attorney's fees allegedly owed to the plaintiff as a result of his investigation into short-swing profits realized by an insider in the defendant corporation. Those activities, however, occurred in either Nevada or New York (on the American Stock Exchange), not in Illinois. Nonetheless, the court is clearly correct that to characterize a passive web site as the transaction of business is disingenuous.
the issue of the enforceability of such provisions has been addressed by at least one court in an Internet gambling case.

In Thompson v. Handa-Lopez, Inc., a United States District Court found that the extensive interaction between the defendant, who ran an online casino, and the plaintiff, a resident of Texas who had allegedly won $193,728.40 gambling on the site, justified the assertion of personal jurisdiction. The defendant in Thompson not only provided a toll-free telephone number, but also "entered into contracts with the residents of various states knowing that it would receive commercial gain at the present time." The court found that each time a resident of another state, in this case Texas, played a casino game online, a new contract was created; furthermore, the plaintiff, while playing the games online, was effectively playing the games as if the casino was physically located in Texas, and the defendant would send any winnings to the plaintiff in Texas. Thus, the repeated formation of contracts with the plaintiff in Texas demonstrated the defendant’s purposeful availment of the benefits of doing business in Texas.

Finding minimum contacts, the court then proceeded to analyze the exercise of jurisdiction in the context of "fair play and substantial justice."

Interestingly, the Thompson court refused to enforce the following "inconspicuous" provision directing that any dispute:

shall be governed by the laws of the State of California . . . and shall be resolved exclusively by final and binding arbitration in . . . California . . . .

First, the court stated that the clause "is not a forum selection clause," reasoning that it didn’t preclude litigation anywhere but California. How that conclusion can be reconciled with the clause’s reference to the exclusivity of arbitration the court does not explain. It does continue, however, by noting the interests of Texas in “protecting its citizens by adjudicating disputes involving the alleged breach of contract, fraud, and violations of the Texas Deceptive Trade Practices Act by an Internet casino on Texas residents” and the plaintiff’s choice of the Texas court. While it merely concludes that those interests outweigh the burden imposed on the defendant by the Texas proceeding, thus making an assertion of personal jurisdiction reasonable, those same interests justify an unarticulated conclusion that Texas could constitutionally decide and in fact had decided to apply its own law rather than that chosen by the parties' con-

365. Id. at 744.
366. Id.
367. Id.
368. Id. at 744-45.
369. Id. at 741.
370. Id. at 745.
371. Id.
tract to the dispute. While such contract provisions have been upheld by the U.S. Supreme Court,\textsuperscript{372} when the dispute, as here, arises under state law, the provision's validity is a matter of state law.

5.5. Intersection Between Jurisdiction and Substantive Liability for Intermediaries

In the case of Internet gaming, one critical issue is whether authorities may regulate or prosecute the operators of online casinos and betting sites by going after the ISPs, who host or provide access to such sites, or third parties who provide software or financial services necessary for the processing of transactions on such sites.

To date, the trend in U.S. courts has been not to hold ISPs liable for illegal activity conducted on their servers, to the extent that such ISPs cooperate in the event of legal actions arising from such activities. The increasingly accepted view is that imposing such liability on ISPs for activities over which they have little or no control would hinder the development of electronic commerce.

It is also unlikely that financial services institutions will be held liable for processing transactions related to online gaming. In the one reported case on the issue,\textsuperscript{373} a plaintiff who lost twenty-five dollars at an online casino brought an action against the credit card company and bank that processed the transaction, alleging violations of the Racketeer and Corrupt Organizations Act (RICO). The plaintiff argued that the defendants' participation in financing the plaintiff's gambling activities constituted a RICO violation (based on the defendants' association with the casino), and that his obligation to the bank was uncollectible. The court dismissed the plaintiff's claim, finding insufficient evidence of a racketeering enterprise (rather, the court interpreted the defendants' relationship with the casino as a "routine contractual combination for the provision of financial services").

The plaintiff did not allege that the casino at issue was an entity involved in RICO violations. The court noted, however, that even if the casino were found to be a RICO enterprise, the provision of financial services by the bank and credit card company to such an enterprise would not support RICO liability.

SALE OF GOODS

6.1. Introduction

It is helpful to bifurcate the universe of "goods" to distinguish between those goods that may be ordered via the Internet but must be delivered


using real world, traditional, transportation systems (Brick and Mortar Goods) and those goods that may be ordered and delivered via the Internet (Cybergoods). For example, automobiles are Brick and Mortar Goods regardless of the medium for the transaction, because delivery of the automobile must be made via a traditional mode of transportation; it is not possible, at least presently, for the automobile to be delivered via the Internet. Other goods, such as computer software, can be ordered and delivered using the Internet by downloading the software directly from the manufacturer or an authorized reseller. Though the same purchase of software could also be completed by transferring the software to some other medium such as CD-ROM, where the intent is for the sale and delivery of the software to be conducted via the Internet, the software would be a Cybergood.\footnote{374}

\section{6.2. The Relevance of Physical Location}

Prior to the advent of the Internet, the sale of a particular good in a particular transaction necessarily involved the transfer of the good from the seller’s possession to the buyer’s possession. It still does, but when questions of jurisdiction arose in the pre-Internet world, a court could look to the location of the seller and the location of the buyer to determine if the court had, for personal jurisdiction, or the regulating jurisdiction had, for prescriptive jurisdiction, a nexus with the physical location of either the buyer or the seller. In the Internet age, such an analysis is still relevant for the sale of Brick and Mortar Goods because the seller must, by definition, identify a physical location where it is to deliver the goods; however, for the delivery of Cybergoods, the seller could live in jurisdiction A, lease an Internet web site on a server in jurisdiction B to handle the sale of the Cybergoods (though it is possible that the seller is unaware of the location of the server), have the buyer download the Cybergoods from a server located in yet a third jurisdiction to the buyer’s computer hard drive located in a fourth jurisdiction.

In this example, is the seller of Cybergoods responsible for complying with the laws of each of the four or more jurisdictions that arguably have prescriptive jurisdiction? Would each such jurisdiction also have personal jurisdiction over the seller? Does a distinction between Brick and Mortar Goods and Cybergoods lead to the correct conclusion? Why should the sale of computer software to a buyer in one jurisdiction be subject to additional governmental regulation solely because the method of delivery the buyer selected made it a Brick and Mortar Good rather than a Cybergood?

\footnote{374. The distinctions become more complex when technology blurs the difference between a “good” and a “service.” For example, are the words of a new novel downloaded to a consumer’s computer through the Internet the sale of a good or the provision of a service?}
Undue burdens and vagaries such as these emphasize the need for the creation of a transnational, adjudicatory, affordable forum to which parties to Internet based transactions may submit their disputes. Additionally, one or more certifying agencies or organizations with aspirational guidelines for the merchant members to follow would create certifiable business practice standards that would, in turn, further weaken the necessity for the quagmire of consumer protection based laws that make navigation of the global regulatory map unduly burdensome at best and impossible at worst.

6.3. Targeting

While the “targeting” standard has received broad acceptance by courts and other bodies in the United States, it fails effectively to distinguish between an active web site that processes a buyer’s order and a call center that fields calls in response to some other advertising medium. If an order is placed to a call center in Florida from a resident of California, and the web site was passive under the Zippo analysis, California may have no jurisdiction over the merchant. If the same merchant establishes a web site that is considered active under the Zippo analysis, and the buyer places an order, California may have jurisdiction over the merchant. This artificial distinction, without more, creates economic inefficiency, assuming that the cost of processing an order on the web site is less expensive than the same order processed by the call center.

While a broader assertion of jurisdiction, essentially submitting to the jurisdiction of every state or nation into which a merchant made a sale, would be economically disadvantageous, at least it would be consistent and logically defendable. This rule would burden the merchant with verifying the residence of its customers. In the case of a sale of Brick and Mortar Goods, the merchant has the ability to verify physical location because the goods must have a delivery address.

On the other hand, sales of Cybergoods do not lend themselves to such a clear filter. A merchant could require the buyer to declare its present location at the time of a purchase. Such an exercise could, however, lead to abuses in certain cases. For example, if the sale of child pornography was permitted in one country and banned in every other nation of the world, the web merchant would locate itself in the permissive country and program the web site only to permit sales to buyers who were residents of that country. When a buyer selects any other country, the web site would not permit the sale and would post the following disclaimer: “Sales of child pornography can only be made to residents of Country X.” Predictably, the buyer will back through the web pages until reaching the page where the residency selection is made and will then select that country, thus circumventing an otherwise well intentioned filter.

Some cases have focused targeting analysis on factors such as the language of the web site. In any case where there could be at least two
potential target audiences, this rule seems arbitrary and contrary to rules of parity.

If targeting analysis is to continue, it should be based on actual commerce within a jurisdiction that meets or exceeds some objective level of contacts that demonstrate availment of the laws and protections of that particular jurisdiction. Even where the combination of information from buyers and payment systems, such as credit cards, could provide a merchant with sufficient, available information to make a determination of the residency of the other party, permitting the parties to agree to the governing law and venue as the result of arms length (or Bot to Bot as the case may be) negotiation is a more equitable solution.

6.4. Power Parameters

Without question, the Internet has changed the power paradigm between sellers and consumers for all transactions, not just those for Cyber-goods and Brick and Mortar Goods purchased via the Internet. Vast amounts of information are available on the Internet, thus reducing the transactional costs formerly associated with traditional shopping, which required the consumer to venture from merchant to merchant, receiving selective bits and pieces of information about the products and subjecting themselves to the additional pressures of human (though not always humane) sales people.

This reduction in transaction costs has at least leveled the playing field if not tilted it in favor of the consumer. In addition to informational web sites, discussion groups, and chat rooms, consumers can now use highly programmable Bots to compare specifications, pricing, warranties, and any other terms and conditions of the desired transaction. While sellers can now reach potential consumers not previously available at greatly reduced costs through web sites, co-branding, and spam e-mails, the potential consumer who encounters any one of these forms of advertising hawking a product can ignore the marketing hype and conduct a market study on a scale and in a time frame not previously available or affordable.

Additionally, the developers of various payment systems specifically tailored to the Internet environment have the ability to provide at least one form of consumer protection by allowing consumers to contest charges on credit cards and other payment mechanisms when fraud or breach of contract is detected. These devices when combined with a universal, better business bureau type of fraud reporting system will further empower consumers in Internet-based transactions.

6.5. Contractual Choice

While generally parties are permitted the contractual freedom to determine the terms and conditions pursuant to which they will conduct commerce, these freedoms are at times interpreted to be, probably due to the
actual or perceived differences in bargaining power between sellers and consumers, terms of adhesion that are either heavily scrutinized or ignored completely. As discussed above, the Internet has created and will likely continue to create a drastic shift away from the traditional power paradigm.

The current generation of Bots already provides consumers with a filter so that the consumer may select an acceptable governing law and venue for the interpretation and enforcement of the online contract. The further evolution of Bots and other devices designed to facilitate e-commerce will likely enhance the consumer's ability to control these contractual options. This may not solve the prescriptive jurisdictional quagmire, but it will weaken the rationale for refusing to enforce contractual choice clauses to the extent that refusal is based on a consumer protection premise.

6.6. The Intersection between Jurisdiction and Substantive Liability for Intermediaries

Intermediary liability in the sale of goods realm may find limited application, at least theoretically, such as having third-party credit card issuers in the jurisdiction collect taxes on purchases made by residents of the jurisdictions. Practically, however, such an approach would likely create opportunities to substitute other third parties not subject to that particular state's prescriptive jurisdiction. In the credit card issuer example, economically motivated consumers would then opt for other payment mechanisms, such as a prepaid cyber-wallet, without a nexus to the state, thus avoiding the relevant taxes or straining the resources of the taxing body to monitor and collect the tax.

Except in certain cases, such as the sale of pharmaceuticals or guns, where the state or nation has an overwhelming health and safety interest in controlling the sale, use or possession of the product, the burden placed on third party intermediaries may be impractical. If the economic benefit of the Internet is to reach the consumers, these liabilities should be implemented with great restraint.

6.7. Conclusion

The overwhelming growth of the Internet has changed the balance of power associated with sales of goods. Under the new paradigm consumers are empowered by information and technology to make informed purchasing decisions. This power shift supports abandoning the traditional reliance on physical location and targeting analysis and recognizing of the feasibility, efficiency, and fairness of a choice of law and venue in the sale of goods arena, while leaving open the ability to shift responsibility in certain circumstances to intermediaries.

Wherever possible, the convergence and harmonization of the laws of the countries of the world, or at least of those that desire to participate in
and reap the benefits of a truly global, e-commerce fueled economy, should be expedited. Finally, the creation and adoption of reliable, efficient and transparent alternative dispute resolution bodies to adjudicate e-commerce based claims and a proactive e-commerce based commercial standards organization will greatly reduce the reliance on traditional regulatory and adjudicatory bodies.

SALE OF SERVICES: THE EXAMPLE OF TELEMEDICINE

7.1. The Relevance of Physical Location

States retain the right to assert jurisdiction over individuals who “practice medicine” within their borders. Medical boards are typically granted the right to regulate the “practice of medicine” on behalf of the state. The State of Colorado, using language common to the legislation of many other U.S. states, defines the “practice of medicine” as:

12-36-106 . . . .

(a) Holding out one’s self to the public within this state as being able to diagnose, treat, prescribe for, palliate, or prevent any human disease, ailment, pain, injury, deformity, or physical or mental condition, whether by the use of drugs, surgery, manipulation, electricity, telemedicine, the interpretation of tests, . . .

(b) Using the title M.D., D.O., physician, surgeon, or any word or abbreviation to indicate or induce others to believe that one is licensed to practice medicine in this state and engaged in the diagnosis or treatment of persons afflicted with . . .

The broad definitions found in health care provider legislation render traditional physical location considerations irrelevant. Where the policy underlying service regulation is public protection (as it is in health care legislation), states will assert jurisdiction over such activities without regard for the service provider’s physical location in order to ensure that the public is adequately protected. Except for the brief references to “within this state” or “in this state,” the definition found in most state medical practice statutes are silent with respect to a particular physical place of the physician. Accordingly, the “practice of medicine” is not defined by the location of the service provider, but rather, by the effects within a given jurisdiction.

In the absence of specific telehealth legislation (which may establish certain telehealth exceptions), the definition of the “practice of medicine” emerges as a critical consideration when assessing the relevance of physical location. Provided that a telehealth provider meets the definitional standard, the state medical board is likely to adopt the view that they retain prescriptive jurisdiction over that provider. As the practice of telehealth proliferates, an increasing percentage of the practice will occur across state borders, leaving telehealth providers subject to multiple statutory regimes.

An additional consideration may further complicate the analysis. The Internet creates certain difficulties when attempting to identify location at a particular point in time. With access conduits worldwide, the possibility exists for individuals to receive telehealth services outside their jurisdiction of “habitual residence.” For example, it is conceivable that an individual who lives in State A accesses a telehealth web site in State B from a computer in State C. This begs the question as to which law will apply—State A, State B, State C, or that of the physician. The use of “habitual residence” of the customer may be the most appropriate approach when attempting to determine if the physician responsible for the web site is “practicing medicine” in a given jurisdiction.

Telehealth, along with other online services, can only benefit from the existence of greater certainty in the applicability of regulatory regimes. Such certainty will help facilitate growth and create confidence within the marketplace. With a definite answer to the question of physical relevance, individuals will have a greater willingness to make use of online services, safe in the knowledge that they are protected by the regulations of their “habitual residence.”

7.2. Targeting

The Internet eliminates the need for service providers to establish local offices within each jurisdiction to which they provide services. In fact, telehealth, by its very definition, contemplates the establishment of relationships with patients beyond the immediate locality of the service provider. In light of current adjudicatory jurisdiction law, providers of telehealth services (as well as the online sellers of pharmaceuticals) must consider whether their sites are targeting multiple jurisdictions.

The court in Zippo established the passive versus active test for assessing the jurisdictional implications of web site activity. It ruled that the exercise of jurisdiction “is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.” Telehealth web sites, which typically meet the active standard established in Zippo, often neglect to reference which jurisdictions they are targeting. Moreover, these sites rarely implement technological measures to limit their availability to individuals of a specific jurisdiction. Rather, they are available to anyone with access to the Internet and thus likely to be subject to a court’s reach under the Zippo jurisdictional analysis. In the context of online pharmaceutical sales, it is possible for certain

377. Id. at 1124.
products to be approved in one jurisdiction but restricted in another, creating the potential for legal liability for an otherwise passive web site. For example, Pfizer maintains a web site for the drug Viagra.\textsuperscript{379} Although this highly publicized product is widely available in the United States, it was only recently approved for use in Canada. The company’s web site states that the information contained on the site is intended for residents of the United States. Prior to its approval, however, the mere advertisement of the unapproved drug contravened section 3(1) of the Canadian Food and Drugs Act,\textsuperscript{380} casting doubt on the effectiveness of a targeted disclaimer and the protection of the passive site characterization.

Although outside the scope of telehealth, the iCraveTV\textsuperscript{381} saga illustrates that the mere availability of information may be sufficient for the courts to assert jurisdiction. With the laws in Canada potentially allowing the retransmission of broadcast signals over the Internet, iCraveTV attempted to limit the scope of its audience through the use of disclaimers and a “click-wrap” agreement. The U.S. District Court was not convinced that these measures were sufficient.\textsuperscript{382} The court did not find iCraveTV’s attempts to target an exclusively Canadian audience effective enough to avoid being subject to U.S. federal jurisdiction.

7.3. Power Parameters

For most off-line sale of goods transactions, the seller enjoys a position of power vis a vis the consumer. In order to make an informed choice about their purchase, consumers typically rely on the information provided by sellers. Because sellers rarely disclose more information than is legally required, consumers often make purchasing decisions without complete information.

The Internet has the potential to reverse this power paradigm. Through informational web sites, discussion groups, chat rooms, and shopping Bots, the consumer enjoys unprecedented access to information, resulting in consumers who may be better informed than sellers.

The reversal of this power paradigm is less evident in the sale of services sector. For knowledge-based services such as medicine and law, regulations are designed to protect the public interest. The off-line regulatory frameworks for these services foster consumer confidence by assuring the public that they can rely on professionally provided services and that they enjoy rights of recourse if a problem arises. Although many new sources of online information about health care exist, these sources can never effec-

\textsuperscript{380} Food and Drugs Act, R.S.C., ch. F-27 (1985) (Can.), as amended.
\textsuperscript{382} Twentieth Century Fox Film Corp. v. ICRAETV, No. 00-121, 2000 U.S. Dist. LEXIS 1013 (W.D. Pa. Jan. 28, 2000).
tively achieve the same level of confidence that traditional regulatory practices instill with the average consumer.383

While a consumer may attempt to research thoroughly a particular product before purchasing it, a patient is less likely to exhaust all possible sources of relevant information about her physician. The patient, who remains in a subordinate power position, relies on the regulatory framework maintained by the state or regulatory body. If an individual holds himself or herself out to be a medical practitioner, the patient is confident that such an individual meets professional standards and will be able to address her situation. This dynamic poses particular concern in the online environment, because the patient may unknowingly rely on a regulatory environment that is nonexistent or cannot be effectively enforced.

7.4. Contractual Choice

Contractual choice does not affect the service sector in the same manner as it does the sale of goods. As discussed above, knowledge-based services are governed by regulatory frameworks designed to protect the public. These mandatory rules establish the boundaries within which service providers are permitted to act.

In contrast, the sale of goods operates on a default set of rules that are identified within the commercial code of the respective jurisdiction. These default rules are designed to operate in the absence of a formal contractual agreement. Commercial codes, however, enable the parties to contract out of the default provisions and replace them with contractual provisions that satisfy their specific needs.

The sale of services often prohibits such private bargains. For example, the onerous practice of medicine regulations ensure that all medical practitioners comply with a minimum standard. Parties may not contract out of these regulations because they are viewed as essential to ensure public safety and confidence. Any such attempt will be treated as unreasonable because the regulations remain applicable notwithstanding the contractual arrangement between the parties. As a result, telehealth practitioners are unable to avail themselves of contractual choice of law and choice of forum clauses in an attempt to elude state medical boards from asserting jurisdiction.

7.5. The Intersection between Jurisdiction and Substantive Liability for Intermediaries

Intermediary liability provides an alternative to the direct regulation of telehealth, particularly in the case of the online sale of pharmaceutical

products. Addressing the sale of such products at the source could eliminate the need for an Internet-specific solution to this emerging issue. But this raises critical regulatory, political and fairness issues.

All states require that medical practitioners examine patients before prescribing pharmaceuticals for which availability is restricted to "by prescription only." Professional standards typically mandate that the physician perform a "sufficient examination" and establish a "valid physician-patient relationship." In addition, certain pharmaceuticals may be approved for distribution in one jurisdiction but not another. The sale of unapproved pharmaceuticals contravenes the regulatory scheme for the dispensation of foods and drugs in virtually every jurisdiction. To maintain the effectiveness of the current regulatory framework in the online environment, the prescription and sale of pharmaceuticals may require new regulatory models.

Because pharmaceutical manufacturers directly benefit from Internet sales and have at least indirect knowledge of such sales, it would not be surprising if governments decided that one regulatory approach may be the imposition of liability on the manufacturers. Such an approach would target the source by ensuring that the manufacturers assume an active role in certifying that their products are dispensed without any impropriety. But the issues and obstacles that question the wisdom of this approach in the physical world are not mitigated in Cyberspace, notwithstanding the breadth and scale of the problem.

Of course, the imposition of such liability is really an imposition not on an intermediary but on a principal to the transaction. The seller of pharmaceuticals to consumers, currently the regulated party, is the actual intermediary. But to regulate the manufacturer directly with respect to distribution would change the liability landscape in an analogous fashion.

7.6. Conclusion

The five jurisdictional paradigm changes in this report produce interesting insights when applied to telehealth. The definition of the "practice of medicine" significantly reduces the relevance of physical location in the jurisdictional analysis. In addition, the active versus passive jurisdictional test established by the Zippo decision is likely to cast a wide net over many telehealth sites including passive sites that contain "regulated information" such as information on unapproved pharmaceutical products.

Both power parameters and contractual choice do not have the same relevance for online services as they do for other areas examined in this

385. For example, Oklahoma provides that the following is unprofessional conduct:

§ 59-509 13. Prescribing or administering a drug or treatment without sufficient examination and the establishment of a valid physician-patient relationship.
study such as the online sale of goods. The Internet does not alter the patient’s reliance on medical practitioners or place the patient in a particularly strong power position. In fact, the opposite may be true because the proliferation of telehealth web sites may result in the need for more comprehensive consumer protection regulation.

Medicine, along with many other services, is subject to a regulatory scheme rather than a commercial code. Parties cannot opt out of the regulations of a particular jurisdiction by simply altering a particular clause in an agreement. The nature of their actions, not the underlying contract, will determine the extent to which state medical boards can assert their jurisdiction.

The imposition of manufacturer liability could theoretically provide a regulatory alternative for certain online sales of services. The pharmaceutical industry could provide an example of how such liability could create the impetus for self-regulation of the industry. Although attacking the problem at the source might lessen the necessity to regulate sites that prescribe and sell pharmaceutical products, regulatory, political, and fairness issues dictate that such mechanisms are viewed as a last resort.

SECURITIES

8.1. The Internet Has Diminished and Will Further Diminish the Relevance of Physical Location

Because the Internet is wholly indifferent to the actual location of computers among which information is routed, there is no necessary connection between an Internet address and a physical jurisdiction. Web sites can be interconnected, regardless of location, by the use of hyperlinks. Information that arrives on a web site within a given jurisdiction may flow from a linked site entirely outside that jurisdiction.

The diminution of the significance of buyer’s and seller’s residence is accelerating in secondary securities markets. Trading markets are moving toward being globalized on a “24 x 7” basis. Investors and brokers already electronically select the regulatory authority of an exchange or alternate trading system to govern all disputes. As a result, there is or should be less focus on the residence of either the seller or purchaser and more focus on the marketplace where the transaction occurs. New issuances also tend to reduce the significance of physical location, especially when the investor

387. The Internet also uses “caching,” i.e., the process of copying information to servers in order to shorten the time of future trips to a web site. The Internet server may be located in a different jurisdiction from the site that originates the information and may store partial or complete duplicates of materials from the originating site. The user of the World Wide Web will never see any difference between the cached materials and the original. American Civil Liberties Union v. Reno, 929 F. Supp. 824, 848-49 (E.D. Pa. 1996).
belongs to a cadre of prescreened investors at a given web site that offers IPOs or private placement to the cadre. Nonetheless, because there is more involvement of the investor in a public or private offering of new securities (offering material must be delivered unless the investor is accredited), there is and will continue to be, to some extent, more focus on the investor’s residence in such transactions than in secondary trading.

Not only is the Internet today diminishing the relevance of terrestrial geography to jurisdictional issues, but also the Internet of tomorrow will introduce ever more revolutionary changes. Internet communication will involve the highly programmed, artificially intelligent cyber-agent (or Bot), which will perform many securities transactions for principals who will have greatly decreased involvement. These Bots will have extensive information about the background, assets, and preferences of their principals and will be equipped with enormous amounts of artificial intelligence, including analytical tools, computational abilities and the like. They will scour the cybersecurity marketplace and conduct transactions in multiple languages.

The residence of the investor will become very attenuated as a factor in secondary tracking. Industry observers foresee a consolidation of exchanges worldwide and disappearance of any distinctions between when markets are officially open and when they are closed; markets will be open all the time. The marketplace that these Bots can scour will be increasingly globalized and centralized, with few or no auction floors. In about five years, there will be three or four global exchanges, trading in securities from a multitude of different nations. All prices on all exchanges will be transparent, because those exchanges that do not provide transparency will be non-competitive and will not retain market share. Bots will determine which markets are most reliable and efficient. Moreover, the investor’s Bot will not be dealing with human intermediaries on the other side of transactions but with sophisticated systems and highly programmed sale Bots.

Bots will be programmed to know the laws of the jurisdiction that may be applied to the transactional contract. If the securities laws of a jurisdiction are not commercially reasonable and fair, the Bots will, everything else being equal, use their machine intelligence to avoid transactions that would call for the application of such laws. In other words, legal systems will ultimately be part of the overall auction evaluation, just as warranty terms are taken into account by first generation “shopping Bots.” This means that a weak legal system will result in loss of business to the forum.

There will also be a system of evaluating the performance and credibility of Bots. Those that prove unreliable in the cyber-marketplace will not be able to transact deals; such undesirables will be systematically ex-

cluded. In this environment, the one-dimensional, linear, sliding-scale spectrum basis for jurisdiction (i.e., passive—interactive—highly active) outlined in Zippo,389 while not rendered entirely obsolete, needs to be revised.

What all of this means is:

If an investor’s Bot searches out and transacts business at a given web site, whether that of an exchange or a dealer, the jurisdiction of the Bot’s principal should not—contrary to Zippo—automatically apply. To the extent the Bot is programmed to make a value judgment about the laws and fora within the site’s jurisdiction, the site’s laws should control in the default situation.

If an investor’s Bot searches out and transacts business on a site or through other electronic contact with a Bot of an issuer or market-maker or dealer, any agreement made as to (a) forum, (b) controlling law or (c) limitation on damages, whether click-wrap or otherwise, should control. Probably all securities transactions will involve agreed choices of law and forum.

As part of a “law merchant” for the Internet, the private sector, probably in cooperation with securities regulators and self-regulators, will develop a set of criteria as to what criteria will qualify Bots for a “seal of approval,” entitling them access to worldwide markets.

Interactivity between user and vendor should not be enough to support a claim of prescriptive jurisdiction for the user’s jurisdiction unless the location of the user is disclosed and germane. Indeed, in the world of securities-oriented Bots, such disclosure should be mandatory, but even such disclosure should not automatically trigger application of the user’s jurisdiction.

Thus, in contrast to the largely linear, point-to-point linking between buyers and sellers that has heretofore characterized traditional commerce and early e-commerce, securities transactions (as well as other kinds of commerce) will increasingly occur outside of any geographical place in a truly “virtual world,” conducted by highly programmed systems and agents applying highly sophisticated artificial intelligence without human intervention. In addition, in less than a decade worldwide commerce will “demonetize.” Instead of a law professor receiving and depositing a paycheck and then writing a check to pay a broker for securities bought on the Deutsche Börse, the monetary value of the professor’s services will be digitally transferred to the monetary value account of the seller. All these changes make it necessary to consider new, non-geographical or less geographical paradigms.

8.2. Change in Power Parameters: The Internet Gives Access, Information and Service to Individuals

The same factors that are breaking down territorial limitations—high-speed communications, greater computer power, twenty-four-hour trading on worldwide markets and the use of highly-intelligent Bots—will further empower individual investors. Already, individuals are steadily gaining more opportunities to participate in public and private offerings,\(^{390}\) attend IPO “roadshows,” participate online in analysts’ meetings and otherwise take full responsibility for managing their investments, initiating trades without the aid of a broker, analyzing securities, and evaluating their portfolios. They have access to increasingly sophisticated investment research tools which not so long ago were available only to institutions and securities professionals.\(^{391}\) Some commentators have long argued that because the Internet gives the “average” investor the same access to information once reserved for wealthy and sophisticated investors, the “average investors should be treated as ‘sophisticated’ under the federal securities laws.”\(^{392}\) When these tools and sources of information are combined with access to superintelligent Bots, the power of the individual will be vastly greater than it was when the \textit{Zippo} decision issued.

8.3. The Importance of Targeting

The prevailing trend in jurisdiction over securities transactions has been to focus on the place to which information on securities is directed by the offeror. This approach has been followed not only by the SEC\(^{393}\) and NASAA in the United States, but by the Australian Securities Commission and by the CSA in Canada.\(^{394}\) In the first several years of e-commerce, courts have emphasized the role of “targeting” in determining jurisdiction. This approach may be less appropriate a few years down the line, with well-programmed and highly sophisticated Bots moving through a wholly virtual space to communicate and carry out complex trading programs, frequently with other Bots, and without human intervention.

For an investor to engage in the use of Bots and other non-geographically based intermediaries is somewhat like the investor sending highly programmed, computer-driven spaceships into outer space to locate and “dock” at space stations for the purpose of conducting transactions. It

\(^{390}\) Prime examples are the “open IPO” of W.R. Hambrecht & Co. and the channeling of syndicate positions to “e-investors” by Wit Capital.

\(^{391}\) See, e.g., “Steven Wallman” in \textit{The Online Finance 40, INSTITUTIONAL INVESTOR}, Apr. 1, 2000 at 73, 106.


becomes harder to argue that the investor’s home jurisdiction should control in preference to that of the space station operator or owner. The web participant who unleashes a Bot into a digital environment awash with other Bots and virtual proxies arguably has “left” his geographical home, elected to transact in a different environment, and does not have a reasonable belief that the laws or courts of his home jurisdiction will apply.

As noted above, this changing environment calls for careful reexamination of *Zippo* to determine whether it would make more sense to create a modified “continuum” that enlarges upon *Zippo*’s horizontal continuum. The new continuum would not be based solely on the “passive-interactive” gradations of *Zippo*. Instead, it would also include a vertical component, based on how far the process is removed from direct human involvement and how materially affected that process is by the intercession of analytical software.395

At a minimum, the increasingly sophisticated environment in which Bots will operate argues in favor of making jurisdiction highly consensual, *i.e.*, controlled in all but outlandish cases by click-wrap terms or conditions imposed on or accepted by the viewer or by the Bots. In the absence of click-wrap acceptance, an activity by a Bot representing someone in Forum A should not necessarily establish jurisdiction in Forum A when the Bot deals with another Bot in Forum B. (This would, in a way, be the obverse of the stream of commerce theory: a person who sends a Bot into the Internet world can be deemed to foresee that, absent understandings to the contrary, it would be engaging in transactions that subject the person to the laws and courts of foreign jurisdictions.)

To the extent individuals will play diminishing roles in transactional models in the future, the elements that have been cited as “targeting” certain individuals and certain territories need to be re-evaluated. These include using a specific language or currency, specific tax information and the like.396

At the same time, the proliferation of Bots could actually make the use of disclaimers and screening devices, which are already recognized by most securities regulators as a way of jurisdictional avoidance, even more meaningful. Regulations that require screening and filtering would be one of the most sensible ways to invoke jurisdictional principles in cybersecurities. Technology will efficiently screen out properly-programmed Bots before they even access a screen, acting sort of like a long-range radar.397

395. Not to be overlooked is the need to minimize the effects test in cyberjurisdictional cases. Such tests have invoked forum jurisdiction when the conduct can be found designed to have an impact in the forum. We should require clear evidence of an intended impact before making a foreign entity subject to forum jurisdiction. Just because there is an effect does not mean the effect was actually intended, particularly when a piece of data can be circulated millions of times over in a matter of seconds.


397. There could, of course, be a sort of “Star Wars” struggle between more technolog-
8.4. Acceptability of Contractual Choice of Forum and Choice of Law

Because globalization of securities markets and the advent of Bots and related technologies remove the individual from the process of actual buying and selling, courts should give full deference to “click-wrap” agreements on applicable forum and applicable law, so long as the process of agreement was not commercially unreasonable. “Unreasonable” means that the terms were not properly displayed or otherwise communicated to the individual or his (or her) cyber-agent.

Buttressing the acceptability of contractual choices is the increasing degree of similarity in the substantive securities laws of different jurisdictions. When laws of two jurisdictions are similar, the policy reasons for preferring one over the other tend to evaporate. The Internet will continue to drive such convergence due to: (1) increased international competition and (2) language. With the trend toward “globalization” of securities markets, funds tend to move to the country that is perceived to provide the best return on investment for a given level of non-diversifiable risk. The resultant competition between countries for investment funds places additional pressure on countries to adopt securities laws that will be perceived to be the most likely to attract investment funds.

The second special factor is the sharing of a common language. Arguably, there is a tendency to copy the laws of a country whose securities laws can be more readily ascertained because they are set out in a language that is understood in the country borrowing the securities laws. The English language currently dominates the World Wide Web. The dominance of English may arguably facilitate the adoption of securities laws from other English-speaking countries, such as the United States or the United Kingdom.

8.5. The Intersection Between Jurisdiction And Substantive Liability

As just discussed, convergence in securities laws will continue. Not only have developments in communication—moveable type, telegraphy, telephonically-advanced Bots and the programs seeking to impose the “cyber-moat.” However, this is a promising area.

398. See generally Mark Gillen & Pitman Potter, The Convergence of Securities Laws and Implications for Developing Securities Markets, 24 N.C. J. INT’L. L. & COMM. REG. 83, 86-87 (1998). Securities laws typically have many common provisions, including mandatory disclosure requirements on the distribution of securities to the public, ongoing mandatory disclosure requirements for post-distribution trading of securities, and prohibitions against insider trading and market manipulation. Rules governing the manner in which takeover bids are made, the period over which such bids must be kept open, and the information that must be provided to offeree shareholders are also typical of regulatory regimes. Id.

399. Id. at 106-08.

400. Eventually, English will lose its present dominance in Cyberspace. Because of the limited subject matter involved in cybersecurities, it is probable that Internet users and their Bots will be able to communicate in all major languages.
ony—all led to less localism and more similarity in commercial laws, but also a globalized and efficient securities marketplace makes it critical that disparities in standards and enforcement be reduced to a minimum. There is really no valid policy reason in such globalized markets why there should be widely different regulatory regimes.

A new international securities regulatory scheme can be constructed, building on the memoranda of understanding and cooperative agreements already in place. As part of this new system, nations and states may have to surrender some local preferences to achieve uniformity, as has already happened in worldwide intellectual property protection. The system would involve international coordination of regulation and enforcement. An obvious focus for such coordination is the International Organization of Securities Commissioners (IOSCO).

In securities as in other fields, however, it may be desirable to seek a more binding kind of regulation, such as that available through the treaty power (e.g., the kind of enforcement exerted by WTO or under NAFTA and GATT). Thus, we could embed in the WTO a set of minimally acceptable standards for the protection of investors in all nations that become WTO signatories, and a common basis for jurisdiction.

An intriguing idea in the world of cybersecurities which could reduce the impact of jurisdiction over substantive liability is the development of new electronic “choke points.” This would involve sophisticated programs through which a securities transaction would have to pass before it could be completed. In a matter of nanoseconds, an electronic “gate” could determine whether current information was on file with regard to an issuer, whether a suspect trading pattern was beginning to develop, whether the jurisdictional choices and disclosures met minimal standards, etc. If, as argued earlier, in a few years we will only have three or four mega-exchanges worldwide, we will have a set of platforms that would lend themselves to becoming choke points. Again, international cooperation would be key to establishing such “choke points.”

**TAXATION**

9.1. Taxation is different

Taxation deals with a very different set of relationships than the other areas covered by this Report. As a result, the jurisdictional considerations and the existing legal framework for resolving jurisdictional issues are quite different from and independent of other legal structures. Nevertheless, there are connections that can be usefully made, and the pervasiveness of tax as a fundamental determinant of the structure of electronic commerce makes it imperative that it be included in any comprehensive discussion of jurisdictional issues affecting electronic commerce.

Each of the other legal regimes under discussion has as a primary goal, the protection of people, enterprises, and institutions from one type of
harm or another that would result in the absence of the rule of law. Taxation, on the other hand, has as its fundamental purpose the collection by the state of revenue from those very same people, enterprises and institutions in order to pay for the services rendered by the state, including many of those very protections discussed in other sections of this paper. The state is an essential and self-interested principal in any tax transaction. Thus, issues of prescriptive jurisdiction of the type discussed elsewhere do not arise when the state asserts that an extraterritorial person or enterprise is liable for a particular tax.

9.2. The Variety of Tax Systems

In discussing tax jurisdictional issues, it is useful to keep in mind that there are a number of different types of tax regimes, each with quite distinct characteristics, that can have a significant impact on electronic commerce. Most broad-based taxes fall into one of two categories: those that are primarily income-based and those that are primarily consumption-based.

9.2.(a). Income Taxes

Taxes levied on the income of enterprises or individuals are generally referred to as direct taxes; the person who is generally expected to bear the economic burden of the tax is also the one with the primary obligation to pay the tax. Taxing the income of enterprises is generally much more conceptually complex than taxing individuals on their income. Not surprisingly, it is also in the context of enterprise taxation that electronic commerce is causing the most difficulty.

Jurisdictional basis for tax. There are generally two bases for a state to assert jurisdiction to tax income: one is the “residence” of the taxpayer earning the income and the other is the “source” of the particular item of income sought to be taxed. When an individual or enterprise is potentially subject to tax in two different jurisdictions, there are frequently elaborate rules designed to prevent the multiple taxation of the same income. For such rules to be effective, of course, there must be common understanding among the competing tax authorities as to how to measure income, when to tax it, and how to define such basic concepts as source and residence. Even if there is such a common understanding, there must be agreement as to which basis for taxation takes precedence. If a resident of one state has income that has its source in another, which state should collect the tax?

In the international context, an elaborate set of rules has evolved to resolve competing claims by different sovereign nations to tax the same income. Some of these rules are contained in national tax laws, others in bilateral treaties. Historically, these rules have not been the subject of multi-national conventions or organizations. As a general rule, source-
based taxation will take precedence over residence-based. For example, under the federal income tax laws of the United States, a U.S. resident business with foreign source income will be entitled to a credit against its U.S. tax on that income for taxes paid to the country of source. Residence-based taxation is protected, however, by provisions in most bilateral tax treaties which limit the right of the signatory countries to tax active business income on the basis of source to income that arises out of a so-called permanent establishment in the source country. The concept of permanent establishment is complex, but at its heart it relies on a substantial and continuous physical presence within the country.

Within the United States, the coordination of the enterprise income taxes imposed by the various states is accomplished in quite a different manner, dividing the tax revenue to be derived from an enterprise’s income by apportioning it among the various states with a claim to it in accordance with a formula that weighs the enterprise’s capital, labor and sales within each state. Although each state is free to apply its own rules, they in fact coordinate their efforts through the auspices of a supra-state body called the Multi-state Tax Commission.

9.2.(b). Consumption Taxes

A consumption tax, such as a value added tax (VAT) and the sales and use taxes levied by most U.S. states, is hardly ever tied to the actual act of consumption but is generally collected at the time of purchase within the taxing jurisdiction by an end user of a taxable good or service. Where goods are purchased outside the jurisdiction for consumption within the jurisdiction, the taxable event is generally the act of bringing the good into jurisdiction. Although in theory such a tax could be imposed on all goods and services purchased or used within the jurisdiction, each system exempts some goods (e.g., housing, basic food, medicine) and many or all services.

There is a strong geographic element to consumption taxes. A state will never impose such a tax on consumption by non-residents that takes place outside its borders. Consumption outside the jurisdiction by residents of the jurisdiction would generally be taxable by the country where the consumption takes place. For example, VAT is generally imposed in the “place of supply” of the consumed item, but a consumer who takes the supplied good out of that jurisdiction for consumption elsewhere is frequently entitled to an exemption from or a refund of the tax imposed on the purchase.

Although the consumer is expected to bear the burden of a consumption tax, imposing the primary obligation to pay such a tax on the consumer directly has long been viewed as an administrative nightmare. Thus, VAT and sales and use taxes have developed as “indirect taxes,” with the retail seller (in the case of the sales and use tax) and all participants in the
distribution chain (in the case of the VAT) holding the primary responsibility to collect and pay over the tax. As discussed below, it is the state's ability to impose the administrative burden of this collection function that has given rise to controversy in the world of electronic commerce.

9.2. (c). Special Purpose Taxes

In addition to the broad-based taxes discussed above, there are many more narrowly targeted tax systems that are designed to raise revenue from, or impose a regulatory regime upon, a limited set of potential taxpayers. Telecommunications taxes and some proposed internet-related taxes like the infamous “bit tax” are examples. Fears that electronic commerce will cause erosion of the tax base of the more broad-based taxes have led some commentators to suggest that the lost revenue could be made up by levying some other type of tax that is borne in some way or other by electronic commerce. These suggestions have been highly unpopular in the industry and have engendered a political response that is in some measure responsible for the passage of the Internet Tax Freedom Act by Congress in 1998 and similar measures by some state legislatures. The proposals for a tax targeted at the Internet have included the “bit tax”—a tax on electronic commerce expressly based on or measured by the volume of digital information transmitted electronically, or the volume of digital information per unit of time transmitted electronically—and the “bandwidth tax”—a tax on electronic commerce based on or measured by the physical capacity of the electronic system used to transmit information.

These proposals, at best, provide a “rough justice” solution to the base erosion issues and risk aggravating the neutrality and fairness problems of the current system. Thus, given their extreme unpopularity, it is undoubtedly a waste of time to spend any significant effort developing them further on a conceptual basis.

9.3. Principal Jurisdictional Issues

The difficult jurisdictional issues that arise when the world’s principal tax systems begin to collide with the emerging world of global electronic commerce essentially concern enterprises, not individual taxpayers, except to the extent that individuals are the owners and operators of enterprises. Conceptually, these issues come in two quite distinct flavors. The first is the issue of when it is appropriate for a state to subject persons outside its borders to the economic burden (as opposed to the administrative burden)

401. See, for example, the California Internet Tax Freedom Act, which became effective for three years starting on January 1, 1999, and which forbids any city or county within the state from imposing discriminatory taxes on Internet access, online computer services or the use thereof. The legislation singles out the bit tax and bandwidth tax as being specifically forbidden
of a particular tax because of contacts with that state which are in whole or part electronic in nature. This is an issue that relates almost exclusively to the income taxation of enterprises.

The second significant issue is to determine when a state can legitimately ask that a foreign person assist in the collection of a tax on others, where those others are within the state’s legitimate taxing jurisdiction. That assistance can be in a variety of forms and arises in the context of a variety of tax systems:

- actually collecting and paying over the tax, as in the sales tax regimes in forty-six of the fifty United States;
- a withholding tax which is paid over to the taxing authority and reported to the actual taxpayer who is then entitled to credit against his or her actual tax liability, as in wage withholding;
- the filing of information returns with respect to various financial transactions.

These withholding and information-reporting regimes are frequently crucial components in the collection and enforcement of the taxes to which they relate.

In the United States, at least, the distinction made here, between jurisdiction to impose the burden of a tax and jurisdiction to impose a duty to help collect a tax, is not one that is reflected in the actual law of jurisdiction that has developed, but in a more global and technologically sophisticated economy it may become increasingly important to make this distinction.\footnote{402}

Consider, for example, a profitable enterprise E located in country (or state) X. E has a large capital investment in plant and equipment, all located in X; the individual owners of E are all residents of X; its many employees are all residents of X and perform their duties in X; E is the owner of very valuable intellectual property, used in the business which was all developed by scientists working and living in X who were trained at the leading university of X. Almost all of E’s customers, on the other hand, are residents of country (or state) Y. Clearly X has a better claim than Y to claim a share of E’s profits in the form of an income tax, in order to finance the various services and infra-structure provided by X in the present and the future to E and its owners and employees. On the other hand, Y arguably has a legitimate claim on E to assist it in the assessment and collection of consumption taxes from those Y residents who are E’s customers.

\footnote{402. For example, a significant sticking point in the ultimately unsuccessful attempt by The National Tax Association’s Communication and Electronic Commerce Tax Project to come up with an approach to sales tax collection by out of state vendors was the insistence by industry representatives that if a vendor agreed to collect sales tax on Internet sales into a state in which it had no physical presence, it would not be opening itself up to increased risk of claims for income tax as well.}
9.4. When should the state tax the enterprise income of a foreign person

As noted, enterprise income is generally taxed based on both the source of the income and the residence of the enterprise, with a variety of highly complex and quite imperfect mechanisms for keeping the same item of income from being taxed more than once. Our new global economy creates more ambiguity and planning opportunity with respect to both bases.

A taxpayer's country of residence is, broadly speaking, the country with which that taxpayer has the closest direct links. In the case of an individual, that will generally be his or her country of domicile, or, where that is ambiguous, the country where she or he spends the most time. An entity treated as a person for tax purposes will generally be viewed as resident in the country under whose laws it is organized or in the country in which its management or principal operations are located. As a practical matter, residence is a fundamentally physical concept.

New technology has made it much easier for an enterprise to conduct business in a jurisdiction in which it is not resident, but it has no real impact on the concept of residence itself. To the extent that the public policy goal of collecting the income tax is to pay for the services rendered by the state to the person earning the income, it clearly makes sense to impose a tax on the basis of residence, given the degree to which state services continue to be focused on the needs of its residents.

With the new technology, it is increasingly likely that enterprise E can earn income whose source is country X without having any physical presence in X. In the international arena, the use of foreign tax credits may result in that income being taxed in country X rather than in E's country of residence. A number of commentators have suggested that the rise of e-commerce and the globalization of the economy generally will result in a shift away from source-based and toward residence-based taxation.

As the economy becomes more global, it becomes more and more important for each country to make its enterprise income tax rules as consistent as possible with those of its trading partners. If there are differences in the way two countries determine the source of particular items of income, sophisticated taxpayers will be able to manipulate those differences in order to reduce or even avoid altogether the income taxes imposed by the countries in which they do business. Unwary taxpayers, on the other hand, may be trapped into paying tax to more than one country without the right to take a credit in either jurisdiction.

Globalization clearly requires a great deal more coordination among sovereign tax authorities than was necessary in the past. This is important not only because it facilitates consistency. There is also a significant concern that some nations will choose not to operate in a manner that promotes sound global tax policy but will engage in “tax competition,” luring electronic business to establish residence there in exchange for a low or
zero rate of income tax and thus facilitating global tax avoidance. Coordinated responses by the more responsible fiscal authorities may well be required to deal effectively with such efforts to exploit tax haven status.

9.5. Finding Jurisdiction over an Enterprise to Require Assistance in the Collection of Taxes

Earlier it was pointed out that the issue of when individuals and enterprises should be subject to substantive tax liability in a jurisdiction of which they are not a resident is clearly quite different than the jurisdictional inquiries in the other substantive areas discussed in this project and, quite rightly, has its own jurisprudence that does not fit neatly within the modes of analysis discussed by others involved in this project. The issue, however, of when a foreign enterprise should be required to assist in the assessment or collection of a domestic person’s tax liability is arguably much closer in nature to other regulatory regimes that require extraterritorial application in order to be effective. Bringing such third parties into the loop is not merely an extension of the revenue raising function, although that function is still central. Foreign vendors who conduct business with residents in a manner that facilitates inappropriate tax avoidance by those residents bear at least a similarity to those who facilitate avoidance of regulations on medical practice, gaming, securities trading and the like. There are three distinct “protective” aspects to such rules:

- protecting the revenue of the state necessary to provide the level of services desired by its residents;
- protecting those who do pay their appropriate share of taxes from bearing more than their fair share of those taxes; and
- in the case of consumption taxes, protecting domestic enterprises from having the burden of the tax shifted to the vendor rather than the consumer, i.e., protecting the in-state merchant from unfair competition from out-of-state.

Keeping the possibility of such similarity in mind, it should be useful to examine how the possibility of having such rules fits the “five thread” analysis that has been applied in the other areas.

9.6. Physical Location

There is no question but that a state can and should require enterprises that have a sufficiently significant physical presence within the state to assist in the collection of tax. Case law in the United States has focused on the issue of whether physical presence is a necessary requirement and, if so, how substantial that presence must be. In its most recent pronouncement on the topic the Supreme Court found that two distinct constitutional

doctrines, due process and the so-called dormant commerce clause, must be considered and, in a break with the past, ruled that each doctrine must be analyzed separately. The conceptual importance of this cannot be overestimated.

The due process analysis, which focuses on the issue of fairness, eliminates physical presence as a requirement altogether. Mere purposeful activity directed toward a state is sufficient to constitute "minimum contacts." The due process requirements are significant because they cannot be altered legislatively and thus act to limit how broadly Congress could legislate if it wished to eliminate the *Quill* commerce clause limitations discussed below.

The commerce clause analysis does not deal with issues of fundamental fairness, but rather with the limitations on the power of individual states to enact laws that have a discriminatory impact on interstate commerce when Congress has not exercised its right to regulate that commerce. In *Quill*, the Court reaffirmed its ruling in a prior case,404 a bright-line rule requiring physical presence for commerce clause purposes. But it based its decision not on the logic of that rule but rather only on the fact that it had been the rule for a significant period of time and that there had, therefore, been substantial reliance on the rule by various people in determining how to operate their businesses. The Court, in effect, affirmed the value of certainty and *stare decisis* in fostering business investment. It implicitly questioned whether the physical presence test is in fact the right test and explicitly invited Congress to overrule its holding if it deemed it desirable.

9.7. Targeting

As discussed above, the Supreme Court, in *Quill*, eliminated the requirement of physical presence in order to find jurisdiction to impose a sales tax collection requirement and substituted a targeting standard. Due process is satisfied if the out of state vendor "directed purposeful activity toward the state" whose tax is at issue. Even in the absence of congressional action, the physical presence standard has been further eroded. Although technically bound by *Quill*'s reading of the commerce clause, the highest courts of New York and Illinois have found, also in a sales tax context, that physical presence itself need not be substantial, but only "demonstrably more than a 'slightest presence'," to meet the requirements of the commerce clause. Factually, this requirement can be satisfied by the presence in the taxing state of a vendor's property or by the conduct of economic activities by its personnel or on its behalf.405

9.8. Contractual Choice

It does not appear that this thread has much relevance to issues of tax jurisdiction.

9.9. Power parameters and Intermediaries

These two threads interact in an interesting manner in thinking about the jurisdiction of a state to require participation by an enterprise in its tax collection mechanisms. The Internet has given rise to a large number of vendors whose potential for selling into many jurisdictions is vast compared to their size, sophistication, and economic strength. One of the legitimate concerns driving those whose cry is “don’t tax the Internet” is that the burden of being drawn into the tax mechanisms of many varied fiscal authorities will be literally overwhelming. In a word, we have created a new class of vendors which is collectively important but individually are without much power either to assist the fisc or to resist its demands.

Interestingly enough, however, there are several types of intermediary enterprises—those who provide the financing mechanisms and the electronic delivery mechanisms—who tend to be large, sophisticated and economically strong. They operate on a scale and have access to sufficiently sophisticated software that it seems to many that they could be asked to take a larger role in the tax collection mechanism, relieving the vendors of that burden.

CONCLUSION

Multiple bases for the assertion of personal and prescriptive jurisdiction obviously lead to multiple fora with internationally and constitutionally proper jurisdiction over actors and their conduct. Jurisdictional principles can inform business decision making; knowledge that certain uses of technology may result in a distant court asserting jurisdiction and judging conduct under its own law, rendering a judgment a business’ home forum would enforce, may determine what uses of technology a business undertakes. But jurisdictional principles can only acknowledge the reality that multiple laws, enforceable by multiple courts, may apply to the same conduct; it can not resolve whatever economic dislocations are caused by that reality.

No regime of regulation or of dispute resolution, however, has ever pretended to be the sole source to which parties turn to ease business intercourse. In every culture and in every time, private arrangements as well as governmental activity have attempted to reduce the occasions of conflict necessitating the exercise of judicial decision-making. The economic world of Cyberspace at the beginning of the 21st century is no different. Trade depends on confidence: confidence on the part of the buyer that goods or services will conform to legitimate expectations and
confidence on the part of the seller that payment will be prompt and complete. Such confidence, in the interests of all parties, is fostered by industry self-regulation that reflects an honest attempt to identify and resolve potential conflicts before they arise. The forms of such regulation are many and are being actively explored as e-commerce becomes an increasingly important segment of the global economy. They include voluntary codes of conduct, the provision of private arbitration for the resolution of disputes, escrow accounts, agreements between buyers, sellers and credit card companies etc.

Beyond private ordering the harmonization of substantive laws across state and national lines can obviate at least one of the jurisdictional issues, that of prescriptive jurisdiction. To the extent the law of all fora related in any way to the dispute is the same, it matters little which is applied. In many instances, of course, such harmonization will be exceedingly difficult; different states, with different understandings of the needs and rights of those they protect, will argue for very different results with respect to such things as consumer protection, gambling, libel etc. On the other hand, there is likely to be agreement that fraud in an offering of securities is to be prevented. The greater the common understanding, even if laws are not identical, the greater is the likelihood that differences will matter little to the parties; compliance with both will flow more easily from compliance with one.

The intersections between jurisdiction of various kinds, private ordering and harmonization are many and complex. This Project makes no pretense to absolute answers. It was designed as a snap shot of the jurisdictional world of today, and as an attempt to use that snap shot to predict what may lie ahead, what difficulties may arise, and how they might be resolved. It is part of a dialogue which—like electronic commerce and the century—is just beginning.

406. Private ordering is designed, of course, to avoid the need for litigation, but as cases considering the validity of contractual choice of forum and law clauses demonstrate, the judiciary can only remain uninvolved if both parties choose it to remain so.

407. States that share such common understandings may also be more willing to defer to contractual choices of a sharing state's law. See David R. Johnson, Susan P. Crawford, & Samir Jain, Deferring to Contractual Choices of Law and Forum to Protect Consumers (and Vendors) in Ecommerce (last modified Aug. 16, 1999) <http://www.kendlaw.edu/cyberlaw/docs/drafts/crawford.html>.