The Internet's fundamental characteristics—a borderless, faceless and paperless environment—support its seemingly limitless use as a tool for business but also present significant challenges. The same technology that allows the smallest entrepreneurs to enter millions of households throughout the world also subjects them to innumerable, conflicting foreign laws and jurisdictions, magnifying the legal impact of content errors. The ability to enter the households of millions of unknown persons poses difficult challenges of identification, privacy and security. And to magnify concerns, once a business "enters" these households, the opportunity to conclude thousands of transactions without face-to-face contact and signed paper contracts raises additional issues of transaction validation and authentication. It is precisely this "equality of access" to new markets and customers that renders traditional notions of the relevant "geographic" market and customer ineffective. The collective impact of these peculiar characteristics of the Internet on traditional notions of business not only offers the greatest opportunities but also exhorts the most challenging legal issues.

The Internet's recent effect on traditional business is due in part to the rapidity of its growth as a medium and in part to the potential for business growth. For a perspective on the Internet's business potential and consumer reach, consider the following:

- 304 million people have Internet access—45% are in the United States and Canada;¹
- nearly one-third of U.S. households are regular Internet users;
- in 1998, the "Internet economy" generated over $300 billion in total revenue in the United States alone;
- "commercial activity” on the Internet is expected to reach $100 billion in revenues in 1999;
- North American retailers generated $14.9 billion in online sales in 1998 and expect at least $36 billion in 1999 (a 145% increase);
- Internet traffic continues to increase—visitors to retail sites rose 300% in 1998 and online retail orders grew by 200%.²

Of course, this kind of data changes from month to month, but updates of both actual and projected data consistently show ever-increasing commercial activity.

Out of this ever-increasing growth has come the desire for regulation and application of traditional legal notions to a very new paradigm. Opponents of Internet regulation proclaim that neither the law nor its mechanisms of enforcement could hope to keep pace with the technological change of the Internet. True enough, the very infrastructure, applications and variations on content (and the legal issues that come with those variations) have changed greatly since the Internet was developed by the Advanced Research

Projects Agency of the U.S. Defense Department. To apply law to a virtual environment would be as fruitless as an attempt to “grasp” a river—once you place your hand into the flow, the water you grasped is gone.3

The purpose of this paper is twofold. The first two sections of the article outline legal developments regulating content and asserting jurisdiction over the Internet. The third section of the paper suggests that Internet regulation is a graspable “river.” Despite the fact that the Internet may never be regulated like a broadcast medium, we can and should try to develop regulations. Any attempt to set legal policy for the Internet should be centralized with delegated regulatory tasks closely monitored. Policy-making at the national level should, in the near term, pursue a goal toward international standard setting. When you consider the widely divergent ways in which content regulation and jurisdictional notions have developed, the second suggestion is likely self-evident.

I. REGULATION OF CONTENT IN THE DIGITAL FRONTIER

Information is the basic commodity of the electronic superhighway. The key to success in the emerging electronic marketplace will be a company’s ability to gather and utilize information from and about its customers quickly and efficiently. Such data is a prerequisite for conducting e-commerce. Traditional face-to-face verification techniques, such as hand-checking credit cards, driver’s licenses or signatures are unavailable. In the absence of any cash transactions, the identification of customers and authentication of transactions and payments become even more important. The collection and use of customer information also offer tremendous opportunities for companies to identify and respond to customer preferences and demand. However, the availability of, and access to, customer information and the increasing economic value of such information has raised concerns among consumers and regulators regarding the potential for misuse of private information. Consequently, the privacy of customers is a critical issue that any Internet business must address at the outset. However, a few other initial concerns are vital predicates.

A. The Concern for Privacy Must Begin With Security and Self Regulation

The technical nature of the Internet medium poses one of the most potentially difficult challenges to its utilization. Given that e-commerce is dependent on computer-based applications, any venture can become mired in issues of content portability, transmission speed and the all-important element of transactional security.

The key to security in business transactions where the customer is unseen is both identifying and then retaining the trust of the customer. The same is true for the Internet. The importance of this issue cannot be overemphasized. Most often, Internet-based businesses will require first-time customers to enter basic information about themselves, at the very least: a username, a password (to use the system with your username in the future) and an e-mail address. Once the customer decides to perform a transaction on the site, the business typically requests additional information, including name, address, phone number and method of payment. With the privilege of asking consumers for this information comes the obligation to ensure the security of the information from unwanted use or intrusion. Internet business security issues are commonly divided among hard-

---

3 For instance, in one attempt to visually represent the breadth and speed of global Internet connectivity, the Cooperative Association for Internet Data Analysis ("CAIDA"), a cooperative nonprofit research organization, published a graphical representation—a “snapshot”—of the Internet core taken from data collected during a 16-day period in Jan. 2000. COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS, VISUALIZING INTERNET TOPOLOGY AT A MACROSCOPIC SCALE, at http://www.caida.org/analysis/topology/as_core_network (last updated Jan. 19, 2001). The visualization is a composite of 220,533 Internet Protocol ("IP") addresses (374,013 links and 154,104 target destination IP addresses) from paths obtained in the merger of three separate sets of data. Id. In addition to the graphical topology representa-
ware (physical security concerns) and privacy concerns.

Among the hardware-related security issues to consider are: securing the web server and business data, securing transactional information (between the server and consumer), and in some cases, securing the consumer’s computer or network. Security risks to e-commerce run the gamut from “eavesdropping” and “packet sniffing” of transactional data, to cracking passwords and exploiting system flaws by hackers. Most security measures begin with installation and maintenance of computer “firewalls” to protect the business’s internal systems and data, and modes of encryption to disguise and protect information during an e-commerce transaction.

Consider the security breach of Hotmail, Microsoft’s Web-based e-mail service in late August 1999. The breach occurred when several nonpublic Web addresses, “Hotmail holes,” were discovered that allowed access to e-mail accounts without use of a password. During the several days that it took Microsoft to close the holes, unauthorized users could read and forward members’ old messages, read new messages and send e-mail under the name of the user without use of a password. This example reinforces the notion that supporting policies and practices are just as important as hardware and software concerns. Not only should consumers be aware of what security measures a company has taken, but also both company staff and customers should be aware of what steps they must take to ensure that security measures are effectively applied to individual transactions.

In the wake of the several high profile and internationally disruptive Internet security threats in early 2000, federal law enforcement authorities increasingly sought the help of computer professionals to combat “cyber-assaults.” Following the incursion of the “Love bug” virus, which brought down computer networks across the globe in April 2000, a special multination session in Paris was convened to discuss Internet security and cooperative enforcement. All countries participating in the conference, including the United States, Japan, Russia, France, Great Britain, Sweden and Brazil already had cooperated in “a service called 24/7 under which authorities [of any nation could] request help from participating countries at any time” in the event of a cyberthreat. The conference concluded without formal recommendations, as designed, but the discussions proved instrumental in developing policy proposals for subsequent G8 summits.

B. The Privacy Policy

Many Internet businesses are now using “privacy policies” to inform customers of the websites’ information practices. Typically, websites will communicate a privacy policy via a link at the bottom of the main page of the site. At a minimum, such privacy policy should: (1) be easy to understand and prominently posted at the website; (2) identify the site administrator and how he/she can be contacted; (3) disclose what information is collected; (4) describe how collected information is used (e.g., disclose how “cookies” are used), including whether such information is disclosed to third parties and the conditions of such disclosure; and (5) provide a method by which persons may restrict the use or disclosure of such information (an “opt-out”).

---

4 See Newton’s Telecom Dictionary 947 (16th ed. 2000). A web server is “a powerful computer [that] is connected to the internet or an intranet. It stores documents and files . . . and can display them to people accessing the server via hyperertext transfer protocol (‘http’).” Id.
5 See Chris Hardie, Independent Study on Electronic Security, at http://www.summersault.com/chris/techno/security/glossary.html (last visited Feb. 11, 2001). Packet sniffing is: [t]he process of trapping and analyzing network traffic that passes through a network interface, even if that traffic’s final destination is not at that interface. This has become a more common process over the years as more tools have been developed to do the sniffing and organize the information obtained in a reasonable manner. Id.
6 See Newton’s Telecom Dictionary 346-47 (16th ed. 2000) (defining firewalls as “[a] combination of hardware and software [that] limits the exposure of a computer or group of computers to an attack from outside”).
8 See id.
10 Anne Swardson, Multi-Nation Conference Confronts Cybercrime, Washington Post, May 17, 2000, at A18. One example of 24/7’s success included an incident where Thai authorities agreed to prosecute a medical entrepreneur in Thailand who was issuing prescriptions in response to Internet orders and then shipping them to the United States. Id.
11 See Federal Trade Commission, Privacy Online: Fair
In an attempt to forestall further government regulation, and with the tacit encouragement of the Clinton administration and congressional Republicans, a number of companies, associations and business organizations have been working aggressively over the past several years to promote awareness of privacy issues and to develop voluntary online privacy practices. A consortium of Internet companies formed the Electronic Commerce and Consumer Protection Group, which published “Guidelines for Merchant-to-Consumer Transactions and Commentary” (the “Guidelines”). In addition to defining the components of an e-commerce transaction and discussing “best practices,” the Guidelines suggest basic rules for providing: merchant contact information; descriptions of marketing practices; information about the goods or services provided; necessary information about the transaction; and all-important order cancellation, return and refund policies. The Internet Advertising Bureau also announced a similar initiative in early July 2000.

Many e-businesses also have contracted with privacy “audit and seal” organizations—firms that specialize in scrutinizing site policies for compliance with applicable law and prevailing consumer concerns about privacy. For example, TRUSTe, a well-known privacy consulting firm, will audit and certify compliant sites for a fee, and the e-business is then allowed to display the TRUSTe mark on the site.

Critical elements of any privacy policy are the actual implementation of and adherence to the policy once it has been adopted. After a policy has been relied upon by consumers in providing information, it is difficult to change the privacy “rules” of disclosure and use. Therefore, any company should carefully consider the nature of the information to be collected and how that information may be utilized in the future. Acting contrary to a posted privacy policy may create serious legal liabilities and result in an administrative enforcement action. For example, the Federal Trade Commission (“FTC”) stated in 1998 that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a “deceptive practice” under the Federal Trade Commission Act.

On July 10, 2000, the FTC brought an action in U.S. District Court for the District of Massachusetts to stop the sale of customer information by Toysmart.com which was allegedly in violation of its privacy policy. However, Massachusetts District Court Judge Carol Kenner ruled that “in the absence of a buyer, the commission’s action was premature.” Regardless of a buyer at this stage of the Toysmart bankruptcy litigation, Pam Kogut, assistant attorney general for Massachusetts, argued that consumers need to be put on notice that details such as “children’s names, ages and toy preferences” might be compiled.

Similarly, Amazon.com announced to its customers on September 5, 2000 that it had revised its privacy policy. The revised policy stated that customer purchasing and other information, as an asset of the company, could be sold with the company to a purchaser of its assets. In addition, Amazon “clarified” its policy, stating that it would not share customer purchasing information with third parties but could share such information with business partners of Amazon. The difficulty with Amazon’s revised policy is not in the content

---


13 See id.

14 The “IAB Privacy Guidelines” can be viewed at http://www.iab.net (last visited Feb. 11, 2001).

15 This means that a private organization has reviewed the site to determine if it complies with its stated privacy policy and applicable laws. See TRUSTe.com, How the Truste Program Works, at http://www.truste.com/webpublishers/pub.html (last visited Jan. 25, 2001).

AGREEMENT CONTAINING CONSENT

Frequently, the FTC staff will e-mail a site administrator advertising and privacy claims made or under the rubric of more restrictive privacy guidelines. Previously, Amazon’s prior privacy statement did not address the issue of customer information sale as being an “asset” or being shared with its “business partners.”

An investigation by the FTC led to an administrative proceeding against GeoCities for allowing third parties to collect and use personally identifiable information from website users, contrary to GeoCities’ privacy policy, which ultimately resulted in a consent decree. Since the GeoCities consent decree, the FTC has engaged in periodic reviews of Internet content. Under the aegis of the agency’s antitrust enforcement and consumer protection jurisdiction, including scrutiny of any deceptive and misleading advertising, the FTC’s Internet Task Force engages in “Internet surf days,” where Task Force members review the advertising and privacy claims made by certain sites. Frequenty, the FTC staff will e-mail a site administrator, notifying the site of a violation and giving the site thirty days to comply with requested changes. Further, on May 3, 2000, the FTC issued a working paper to assist Internet advertisers with applying the FTC advertising guidelines in an online environment.

In addition to the issuance of the working paper, the FTC has pledged to continue discussions with Internet advertisers toward a set of voluntary privacy standards that companies would follow in conducting “blind” profiling of Internet consumers. The principle issue of continuing talks centers on the way companies should disclose profiling practices (most often conducted through the use of “cookies”), and “how and when consumers should be able to exclude themselves from scrutiny.”

Even with a privacy policy in place, businesses should be extremely wary of surprising consumers with drastic changes in the way the company uses information. Consider Amazon.com’s August 1999 decision to give consumers access to purchasing data organized by corporate or organizational affiliation. Touting the new feature as a “fun” way to encourage community building, Amazon published such information as the top selling book among National Semiconductor employees, “101 Nights of Grreat Sex,” and the most popular CD among employees at the FDIC, “Zoot Suit Riot: Swingin’ Hits of the Cherry Poppin’ Daddies.” Privacy experts were swift in their criticism of Amazon’s actions, noting that to “highlight data in your collection of customer profiles . . . throws fuel on the fire,” alienating consumers who are already fearful of how their personal privacy can be invaded by the Internet. Amazon has since given consumers the ability to opt-out of such lists, but the incident left many consumers unnerved.

Amazon, however, seemingly did not learn their lesson. In late September 2000, it was revealed that Amazon had been engaging in a sales strategy called “dynamic pricing,” which “gauges a

---


24 Federal Trade Commission, Dot Com Disclosures, at http://www.ftc.gov/opa/2000/05/dotcom.htm (May 3, 2000). The working paper advises online advertisers that the same consumer protection laws that apply to commercial activities in other media apply online, and that any disclosures required to prevent an ad from being misleading must be clear and conspicuous. Id. In late Nov. 2000, the FTC took a more proactive stance, warning more than 100 online retailers that if they made “quick ship claims” in order to entice consumers for Christmas sales and then do not fulfill the orders on time, they will be subject to penalties under the Mail or Telephone Order Merchandise Rule. Press Release, Federal Trade Commission, FTC Follows up on “Project Too-late.com” With “Surf” of E-tailers, Educational Campaign On

---


26 Id. An agreement eventually reached with the Commission would include provisions for “fines and other disciplinary actions against companies that violate those standards and collect information surreptitiously.” Id.


28 Id.
shopper’s desire, measures his means and then charges accordingly.\textsuperscript{29} As a result, different Amazon customers were purchasing, for instance, the same DVD at the same time but for different prices.\textsuperscript{30} Amazon stated that the pricing model was a test, employed only briefly and that the company would not further engage in dynamic pricing.\textsuperscript{31} Within two weeks after the incident was reported, Amazon not only apologized but also issued refunds to appease angry customers.\textsuperscript{32} As before, Amazon revealed its intentions and the substance of the corporate strategy, and then backtracked after unintended exposure and consumer furor.

Industry also has learned that the best of privacy intentions may not be enough. The chief executive officer of E-Loan, Inc., Chris Larson, discovered that despite considerable investment in consulting and attention to privacy protection, his company was still exposed and vulnerable to all the policies and practices of its e-business partners. E-Loan touted a public image that its website was “cookie free,” which means that it did not compile user information unless requested to do so, and spent $250,000 on a website privacy audit by PriceWaterhouseCoopers.\textsuperscript{33} Much to Larson’s chagrin, the audit found that one subsidiary, CarFinance.com, was still using cookies pursuant to pre-existing contracts; a strategic partner, and LiveCapital.com was operating a user-habit tracking-tool on E-Loan clients that linked to the LiveCapital site. To make matters worse, the Internet advertising firm DoubleClick, Inc. had been hired to track those who clicked on LiveCapital’s banner ads placed on other websites (a practice often called “floating a tracker”).\textsuperscript{34}

Many e-commerce executives have accepted the inevitability of further privacy regulation, noting that in the FTC’s 2000 Online Privacy Survey, 92% of respondents stated that they do not trust online companies to keep their personal information confidential and 82% recommend legislative action to rectify that lack of trust.\textsuperscript{35} eBay has indicated that it would “support minimal regulation if [it] curtailed states’ rights to impose a ‘patchwork of differing rules.’”\textsuperscript{36} Also, BellAtlantic’s Internet division indicated that it would find “baseline” rules to be useful.\textsuperscript{37}

Unfortunately, these concessions have come in the wake of several high-profile deviations from the industry’s effort to self-police. DoubleClick, Inc. was widely criticized in March 2000 for its plan to match a massive database of consumers’ catalogue shopping habits with information that the company routinely collects as Internet users move from site to site.\textsuperscript{38} DoubleClick has been able to perform the latter service for clients by tracking Web user movement through banner ads it places on contracted sites. Until it announced its purchase of Abacus Direct, Inc., DoubleClick did not have the ability to match Web user habits with personally identifiable purchasing information, while Abacus Direct has collected information for years on the buying habits of catalogue shoppers.\textsuperscript{39}

Many prominent websites such as AltaVista and Kozmo.com quickly announced that they would no longer release visitor data to DoubleClick unless the consumer expressly agreed to allow information to be shared.\textsuperscript{40} Soon after, DoubleClick abandoned its effort to merge the two data sources but not before several complaints were filed against it with the FTC.\textsuperscript{41} Similarly, America Online and Netscape Communications were sued in early July 2000 in the Southern District of New York for allegedly illegally tracking downloads by Internet users in violation of the Computer Fraud and Abuse Act.\textsuperscript{42} In early August 2000, America

\textsuperscript{30} See id.
\textsuperscript{31} See id.
\textsuperscript{34} Id.
\textsuperscript{35} The survey was based on data collected from a random sample of 335 websites. See PRIVACY ONLINE, supra note 11.
\textsuperscript{36} Jerry Clausing, \textit{Fate Unclear for FTC’s Privacy Push}, N.Y. TIMES, May 22, 2000, at Cl.
\textsuperscript{37} Id.
\textsuperscript{39} Id.
\textsuperscript{40} Id.
\textsuperscript{42} See Plaintiff’s Complaint, Specht v. Netscape Comm. Corp. and America Online, Inc., Civ. Act. (S.D.N.Y. July 6, 2000). Section 1030 of the Computer Fraud and Abuse Act provides for penalties against “[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any pro-
Online agreed to remove the monitor feature from a technology it inherited by purchasing Netscape Communications in 1999. 43 Nonetheless, privacy protection will not be unlimited. In balancing First Amendment with Due Process concerns, courts have been increasingly reluctant to allow online critics to remain anonymous. For example, on June 14, 1999, the California Superior Court enforced a modem company's request to unmask an anonymous online critic posing as a Xircom employee, rejecting arguments that a subpoena would violate the critic's free speech rights. 44 The Court noted that there is no right to defame. 45 Similarly, the Miami-Dade County Circuit Court in Florida rejected the First Amendment arguments of several Internet critics who sought to protect their anonymity. The court ordered that Yahoo! and America Online comply with a subpoena and disclose the real names of certain online service users "so that they may be formally named as defendants in a libel case." 46

I. Federal Privacy Regulation

Although the United States has encouraged self-regulation by industry, some basic federal privacy protections have emerged. Federal legislative efforts began by addressing the illegal misappropriation of information gathered from the Internet and other electronic sources. On October 30, 1998, President Clinton signed the Identity Theft and Assumption Deterrence Act (the "Identity Theft Act"). 47 The Identity Theft Act makes it illegal to (without consent) knowingly transfer or use another person's identification means with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law or that constitutes a felony under any applicable state or local law. 48 Significantly, the Identity Theft Act includes punishment by fine and up to twenty years imprisonment for an offense that is committed to facilitate a drug trafficking crime in connection with a crime of violence or subsequent to a prior conviction for identity misappropriation under the Identity Theft Act. 49

More recently, federal legislation has addressed privacy concerns involving children and financial information. The Children's Online Privacy Protection Act ("COPPA") was signed into law on October 21, 1998. 50 The statute institutes stringent regulations for obtaining electronic information from children under 13 years of age, including the necessary parental consent. 51 The FTC rules implementing COPPA, effective April 21, 2000, apply the requirements to a website or online service directed to children that collects personal information, or websites whose operators have "actual knowledge" that they are collecting personal information from children. 52 In addition to posting a prominent link on the masthead page and a clear description of the site's information practices, the rules require sites to display this prominent link wherever the site collects personal information. 53 The notice of information policy must disclose: (1) the name and contact information of all operators collecting or maintaining children's personal information through the site; (2) the kinds of information collected; (3) how the operator(s) use the information collected; (4) whether the operator(s) disclose the information to third parties; (5) that a parent has the option to agree to information collection while restricting its use by third parties; (6) that the operator(s) may not require a child to disclose more information than is reasonably necessary to participate in the activities of the site; and (7) that a parent can review his/her child's personal information, ask to have it deleted and refuse further collection of infor-

45 Id.
51 Id. at §§ 6501–6505.
52 16 C.F.R. § 312.3 (1999).
53 Id. at § 312.4(b) (1999).
The Financial Services Modernization Act ("FSMA"), enacted on November 12, 1999, stipulates that financial service companies must create a privacy policy and clearly state it to consumers.54 The data protection provisions in Section 5 of the Act are implemented by the FTC and federal bank regulators, including the FDIC, the Federal Reserve Board and the Office of the Comptroller of the Currency at the Treasury Department.55 The Securities and Exchange Commission will oversee its implementation in the securities industry, and state insurance commissioners will apply it to insurers. Regulations implementing the FSMA, drafted through a cooperative effort among federal banking regulators, require financial firms to tell customers about the types of nonpublic personal information that is shared with affiliates and third parties. "Nonpublic" is defined by the Act as information gathered from consumers applying for financial products and services.56

In addition, the FTC has adopted a rule interpreting the FSMA broadly by defining "financial information" to include any personal information gathered by a financial institution, including names and social security numbers (often called "credit header" information).57 Consequently, financial institutions, insurers, banks, retailers and any other business issuing credit must offer customers an "opt out" opportunity before allowing credit bureaus to resell personal information. Credit bureaus and direct marketers are "up-in-arms" over the new rule, complaining that the FTC has gone far beyond the mandate of the FSMA. A House Banking Committee spokesman confirmed to The Washington Post that the FTC's rule "matches the intentions of the legislation's authors."58

This is not the first time that the FTC has "pushed the envelope" with regard to regulatory initiatives aimed at privacy protection. However, FTC initiatives have not always garnered the full support of the administration or Congress. On May 22, 2000, the FTC issued its third report to Congress on "Fair Information Practices in the Electronic Marketplace" ("Privacy Report"), which comments on the results of the Commission's 2000 Online Privacy Survey ("Survey") and recommends legislation setting forth a "basic level of privacy protection for consumer-oriented commercial Websites."61 The proposed legislation would have established basic standards of practice for the collection of information online, specifically addressing notices of information practices, opt-out choices, restrictions on third-party access and reasonable security. Additionally, the legislation would provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act. Although not abandoning self-regulatory efforts, the FTC points to Survey data establishing that such efforts have been ineffective.62

Republican lawmakers found themselves in an odd alliance with the White House and Commerce Department in opposing the legislative action recommended by the FTC. Outgoing Commerce Secretary William Daley commented to The New York Times that "legislation would not be necessary" if the industry could show that it was effectively policing itself.63 Publicly, both White House officials and Billy Tauzin (R-LA), the previous Chairman of the House Subcommittee on Tele-

59 Robert O'Harrow, FTC Curbs Personal Data Sales, WASHINGTON POST, June 2, 2000, at E1.
60 PRIVACY ONLINE, supra note 11.
61 Id. at 36.
62 Id. at ii. The Survey notes that while almost all websites (92%) collect personal information from consumers, only 14% disclose anything at all about how the information is used. Id. In addition, despite "significant improvement" in the frequency of privacy disclosures, the FTC notes that only 10% of the sites posted privacy policies touching on all four of the fair information practice principles. Id. at i. Of all sites surveyed, only 8% display a privacy seal as the result of a privacy audit. Id.
communications, Trade and Consumer Protection, said that government should continue to rely on industry to police itself and that the White House should have a deeper interest in promoting privacy laws in other areas, including health care and financial services. Republican FTC Commissioner Orson Swindle also took issue with the FTC recommendations. He noted in his dissent to the Privacy Report that the report "is devoid of any consideration of the costs of legislation in comparison to the asserted benefits of enhancing consumer confidence." Chairman Tauzin added, "with the finding that websites have improved dramatically their privacy policies, [the FTC is] now recommending legislation. It seems to be a contradiction that needs to be understood."

Appealing to the sentiments of Congress and the Clinton Administration, a consortium of major Internet companies agreed on July 27, 2000 to a resolution with the FTC that would allow Internet companies to continue regulating themselves for the time being. The important difference between this agreement and the prior tacit approval of self-regulatory measures is the FTC's imposition of an enforcement mechanism. The agreement reached at the meeting with the Net:

---

64 Forthcoming national rules on privacy for health care information, preceded by the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.), do not mandate but will likely state that doctors should request that a patient sign a consent form before personally identifiable treatment and case information is made available on the Internet for studies and other purposes. Robert Pear, U.S. Plans Tighter Rules on Medical Files' Privacy, but Some Want More Limits, N.Y. TIMES, Aug. 20, 2000, at A20. The rules will give health care industries and insurance companies two years to come in compliance. Id. However, it has been noted by several medical ethicists that many physicians already feel ethically bound to use patient consent forms before entering information. Id.


66 Labaton, supra note 63, at C1.


69 Id. (reporting that, surprisingly, DoubleClick has stated that it would abstain from merging its Abacus databases with "blind" online data despite the agreement reached with the FTC).


72 The European Parliament had similarly introduced a draft directive on the use of digital signatures, but perhaps because of technical difficulties, the draft remained tabled until passage of the Electronic Commerce Directive, which passed in May 2000 and is discussed below. See European Parliament and Council Directive on a Common Framework for Electronic Signatures, EUR. PARL. DOC. (COM 297 final) (1998). On Nov. 20, 2000, the European Commission announced a proposal to speed recognition of electronic invoices in all 15 Member States of the EU. See Alan Osborn, EC Calls for Broad Recognition of Electronic Invoices, TOTAL TELECOM, at http://www.totaltele.com/view.asp?ArticleID=34047&pub=tt&categoryid=626 (Nov. 21, 2000). At present, in some EU Member States, electronic invoicing is prohibited, whereas in others, e-invoicing has to be accompanied by parallel transmission of paper invoices. Id. The fact remains that many businesses simply lack the technical ability and wherewithal to make use of digital signatures under the new law.
2. State Privacy Regulation

Although the federal government has moved cautiously to address privacy concerns, many states have adopted online privacy protections.73 States with privacy statutes have been aggressively enforcing them. The consequences of not adhering to a privacy policy were forcefully demonstrated in a suit against U.S. Bancorp ("Bancorp") and its subsidiaries.74 On June 30, 1999, U.S. Bancorp agreed to a costly settlement of a suit brought by Minnesota for Bancorp's practice of sharing customer account information without customer consent for the marketing of nonfinancial products.75 The attorney general of Minnesota alleged the bank's transfer of confidential customer information to a direct-marketing firm was contrary to its published disclosure policy and violated various federal and state laws.76 Although the case was settled quickly, the financial and public relations consequences to the bank were substantial.77

3. International Privacy Regulation, a Marked Difference in Approach

For the most part, foreign governments have been moving much more aggressively to respond to consumer privacy demands. In 1995, the European Union ("EU") adopted its Data Directive to control the use of information from consumers and specify their privacy rights. The Data Directive went into effect in October 1998 and requires companies to ensure that data is: (1) collected only for specific purposes; (2) accurate and current; and (3) discarded once no longer needed.78 Under the Data Directive, European customers have the right to access collected data, correct the data, object to data uses, oppose automated decisions and seek judicial remedies.79 Most importantly, the Data Directive controls the extraterritorial flow of such information by prohibiting the transfer of data to countries that do not provide "adequate" privacy protection.80

A Safe Harbor agreement ("Safe Harbor") for U.S. companies under the EU Directive was finally reached with the European Commission on May 31, 2000. It applies the Data Directive basics to U.S. banks, airlines and multinational companies that build databases in the course of their operations in Europe and want to transfer that data to the United States.81 The United States will not be required to pass new laws regarding data protection in order to access the European market. Rather, companies wanting to transfer data from Europe must register for "Safe Harbor" protection with the U.S. Department of Commerce and declare publicly that they are following EU data protection rules.82 Companies will be subject to legal action by the FTC for "deceptive acts or practices" if they "publicly disclose" and then do not follow the rules.83

Thankfully for U.S. e-businesses, the agreement does not apply the rules to information collected by many commercial websites—a European visiting a U.S. site and leaving personal data on a registration form, for example, is not covered by the agreement.84 But from the EU point of view, U.S. websites would ignore this aspect of the Data Directive to their peril as the Internet may later be covered by the EU Data Directive. The European Parliament recently issued an opinion that the Safe Harbor does not offer adequate protections,

---


76 See Hatch, supra note 74.

77 Olson, supra note 75, at C2; Tripp, supra note 75, at B2.


79 Id.

80 Id.


82 See id. at § 1. A mixed system of enforcement was adopted for the Safe Harbor, which not only allows companies to develop self-regulatory schemes for enforcement but also to agree to cooperate with EU data protection authorities if they prefer. See id. (explaining that this latter method of registration has the benefit of being the only way under which a company can transfer human-resource specific data).

83 Id. at § 5.

84 See generally id. In addition, many important business sectors, most prominently the financial services sector, are at present excluded from participating in the Safe Harbor. Id.
because they neither provide for monetary damages for breach nor right of appeal in the United States. The European Parliament's opinion, however, was nonbinding, and although implementation might have been slightly delayed, indications were that the European Commission would implement the Safe Harbor given that it had already found its protections adequate. The European Parliament finally approved the principles of the Safe Harbor on July 27, 2000, the same day it found the laws of Switzerland and Hungary adequately represented the Data Directive.85

Within a month following the Safe Harbor's implementation, several companies "in the 'privacy business,' such as watchdog groups," could be counted among Safe Harbor U.S. participants.86 The sole aberration to this initial trend was the Dun & Bradstreet Corporation's registration for the Safe Harbor.87 Although permission to cut off data flows under the Data Directive is suspended until June 2001, the EU is having difficulty "getting its own Member States in line."88 As of November 30, 2000, it had "sued six countries for their failure to comply with the Directive at all."89

The nature of the agreement reached on the Data Directive underscores the divergent dynamics behind U.S. and pan-European regulation of privacy and the Internet. The EU and certain Asian countries, particularly Singapore and India, have instituted rigorous privacy standards, whereas the United States, with the exception of the FTC, still largely favors industry self-policing. In keeping with its Asian and European counterparts, the United Kingdom implemented the UK Data Protection 1998.90 The Canadian House of Commons approved Bill C-6 on April 4, 2000,91 which covers a wide range of industries using personal information for commercial purposes and requires Canadian companies, including Internet Service Providers ("ISPs"), to obtain affirmative consent from customers before providing their personal information to third parties.92

Privacy-related protections and their proponent countries on both sides of the Atlantic have not operated in this evolving legal environment without a certain degree of duplicity. Early in 2000, the European Parliament concluded a special investigation with a report on U.S.-led eavesdropping on private Internet and data communications.93 Using artificial intelligence methods and a global network of relays, the U.S. "Echelon" program, which had its beginnings as early as 1947, regularly sifts through voice and data communications in Europe for "key words that its overseers suspect may represent security threats."94

The British intelligence equivalent of the United States Central Intelligence Agency, MI5, has begun construction of a £25 million e-mail surveillance center that "will monitor all e-mails and Internet messages sent and received in Britain."95 The new computer-center, codenamed "GTAC[,] Government Technical Assistance Center," will be completed by the end of 2000 inside MI5's London headquarters.96

---

87 Id. Dun & Bradstreet's rationale for its early registration was that, by its corporate practices, it "already complied." Id.
88 Id.
89 Id.
92 Id. (stating that "currently, Internet service providers have access to a wide variety of information on their customers and can sell it, without user consent, to Internet marketers").
94 Id. European politicians have used the Parliament report to suggest that the Echelon program "has been used to benefit U.S. corporations in economic and industrial espionage." Id. Such claims are unsupported at present, but some scholars are quick to add that indictments of U.S. intelligence efforts ignore similar privacy-offensive activity in Western Europe. Id. The British government admitted in June 2000 that it has cooperated with the United States on Echelon in the interests of its own national security. See Nicholas Rufford, MI5 Builds New Centre to Read E-Mails on the Net, LONDON SUNDAY TIMES, Apr. 30, 2000, at 5G1.
95 Nicholas Rufford, MI5 Builds New Centre to Read E-Mails on the Net, LONDON SUNDAY TIMES, Apr. 30, 2000, at 5G1.
96 Id.
of GTAC has sparked criticism, both in Britain and abroad, particularly given the British Parliament’s approval of the Regulation of Investigatory Powers Act (“Investigatory Powers Act”) on July 27, 2000.97 The Investigatory Powers Act requires ISPs to facilitate wiretapping and access to encryption keys to assist British authorities.98 However, both the Investigatory Powers Act and the GTAC initiative parallel European Commission preparations for a directive granting similar authority to enforcement agencies across the EU.99 Furthermore, the proposed legislation would address the prevention of anonymous and unsolicited e-mail (“spam”) and set out the conditions under which telecommunications carriers must allow law enforcement agencies to intercept e-mail messages.100

Canada did some backpedaling shortly after passing its revolutionary privacy legislation. Bowing to public pressure, it scrapped a database of citizen information. The May 16, 2000 release of the annual report of the Canadian privacy commissioner revealed that a government bureau, Human Resource Development Canada, managed a secret government database called the Longitudinal Labour Force File.101 The database contained over 2,000 pieces of information on every Canadian citizen.102 Culled from tax returns, child tax benefit files, provincial and municipal welfare files, federal jobs, and job social insurance master files, the breadth of the privacy protection breach shocked even Canadian Privacy Commissioner Bruce Phillips.103 Again bowing to pressure, the Canadian government agreed to dismantle the database.104

Despite both missteps and divergent methodologies in Europe and North America, many Asian nations have followed suit with privacy regulations and in some cases have drawn criticism of their own. India’s Lok Sabha, for example, unanimously approved its Information Technology Bill.105 Previously objectionable sections requiring cybercafes to keep detailed records of users and their activities were dropped, but the bill still included the controversial Section 79, which gives a deputy superintendent of police the power to conduct search raids of the cafes without warrant.106

Other efforts in Asia have been directed particularly at developing e-commerce while protecting consumer rights. New Zealand announced plans in April 2000 to develop a “model code of conduct” for e-commerce, following government consultations with traders and consumer groups.107 Basing its initiative on a similar model code in Australia, the New Zealand code “will require internet shopping sites to display a physical address, as well as their privacy and security policies, provide details of refund, exchange and complaint policies, and advise which laws apply to transactions made by customers.”108 Thailand took a similar step in April 2000, announcing plans for e-commerce and digital signature legislation before 2001.109

C. Internet Content Issues in the United States

Content that is entirely or mostly generated by an Internet site owner in the United States typically presents the least complex liability issues. In

---

97 Regulation of Investigatory Powers Act 2000, c. 23 (Eng.).
98 Id. at §§ 2, 12.
100 See id.
102 Id., supra note 101.
103 Id.
104 See Canada Scraps Citizen Database, supra note 101.
108 Id.
this regard, U.S. site owners have significant First Amendment and other legal protections available to them. Many website owners license content from others rather than develop their own. Licensing agreements between the site owner and the content creator ensure the site owner has the rights it needs to distribute, alter, republish or otherwise use the licensed content. Yet, as the interactivity of websites increasingly becomes a draw for retaining Internet customers, more sites are building community content, such as chat rooms, message boards and e-mail with their primary provision of e-commerce transactions.

Many of the most prominent Internet businesses, including America Online, began by offering the e-mail and message board functions of a traditional ISP before engaging in e-commerce. As a result, much of the content in these "extra" areas is created by users of the site and cannot, as a practical matter, be reviewed or edited by the site owner. In addition, the now common practice of linking to, or "framing," the content of other sites can subject site owners to either: 1) vicarious liability for knowingly linking to another site that engages in infringing activity; or 2) direct liability for infringing on the trademark of the linked site.

1. Legislative Activity

With regard to defamation, the United States Congress included Section 230 in its enactment of the Communications Decency Act of 1996, which largely immunizes ISPs from liability arising from the statements of third parties. Subsequent legal decisions have held that under Section 230, a website owner cannot be held responsible for the defamatory or otherwise tortious statements of individuals who post on its message boards.

Congress enacted a limitation on copyright liability for ISPs—and thus substantially altered case law that held ISPs liable for copyright infringements committed by the ISP's users. Title II of the Digital Millennium Copyright Act ("DMCA") categorizes each separate function of an ISP and provides that each such function cannot create monetary liability for copyright infringement. For example, an ISP would incur little or no liability for its transmitting/routing and caching functions, third-party postings, or use of its information retrieval tools.

The DMCA does not change existing U.S. definitions and requirements for copyright infringement. Rather it decreases the stakes for providers of a technology not contemplated when America's federal copyright laws were enacted. Generally, these liability limitations apply only to passive activities, where the ISP does not exercise any control over, or interact with, the content of the infringing material.

Some prospects for Internet-related legislation were hotly debated during the 106th Congress but...
2. Judicial Activity

Where Congress has had difficulty legislating, the courts have made some inroads. Several legal decisions have held that certain methods of conducting Internet business can be successfully patented. In the past two years, at least ten specific Internet-based patents have been issued, covering such online processes as: reverse-price auctions, "shopping carts," secure online payments, online incentives, pay-per-view advertisements, personal privacy and "push" technology.

Apart from copyright issues, patents and other content concerns, the Internet can serve as a stage for content liability that previously might never have been expected. For example, in August 1999, eBay prevented a user from auctioning off a "fully functional" human kidney but not before the "item" brought in bids totaling more than $5.7 million. Noting that trafficking human organs is a federal felony, punishable by a minimum of five years in prison and fines of $50,000 or more, eBay's vice president of marketing swiftly affirmed that "eBay has a zero tolerance for illegal items on the site," despite its hands-off approach as a platform for consumer sales.

3. Uniform Laws

The anonymity, speed and geographic reach of patents are often a minimum of $9,000 in legal fees, and recent changes in patent law make patent application secrets public within 18 months, whether or not the application is approved. Steve Roblee, Investors Downplay Patent Importance, POTOMAC TECH. J., at http://www.potomactechjournal.com/displayarticledetail.asp?art_id=45045 (Dec. 8, 2000). Thus, "[i]f you have a technology to turn into a one-product company, it's probably more important to get to market than to go through the process of getting a patent, . . . [but if the technology] is useful for more than one thing, it's probably worth going after the patent." Id. Particularly, patent filings for "methods of doing business," popular in the past three years, may not have the value that filers would like, as the Patent and Trademark Office is expected to be more discriminating in types of business patents it grants. Id.

Jay Walker, founder of Walker Digital, which develops new tech-driven business models, patents them and spins them off into businesses, has particularly benefited from these rulings. Steven Levy, Wired for the Bottom Line, Newsweek, Sept. 20, 1999, at 43. Walker Digital's first successful concept company, Priceline, enables customers to name their own price for airline flights, using the Internet to connect the user with an airline willing to make the deal. Id.


Online Shoppers Bid Millions for Human Kidney, supra note 125.
the Internet also have presented significant challenges to traditional contract principles, including: contract formation, permissible terms, evidence of the contract and enforcement. New and repeat customers seeking to utilize a system for e-commerce will rely on registration agreements "executed" with the company prior to use of the site, both for their protection and the company's. These "online contracts" or registration statements can be as simple as having the customer key several choices indicating that they have read the rules prior to using the system, or they can be as complex as formal agreements executed through use of a "digital signature." Regardless of the complexity of the agreement with customers, key features of a digital transaction system should be: confidentiality and verification of user identity, proof of transaction/repudiation, and retention of a positive record of the transaction.

After years of debate and aborted efforts on the issue, the National Conference of Commissioners on Uniform State Laws ("NCCUSL") convened in July 1999 to discuss two draft uniform laws to apply to e-commerce transactions. The first, the Uniform Computer Information Transactions Act ("UCITA"), reflects the NCCUSL desire to ensure that consumers can: 1) thoroughly review an e-commerce transaction before agreeing to it; and 2) rely on procedures for the consumer to manifest assent to the transaction. Among the other concepts addressed by the UCITA are: limitations on consumer liability for "unauthorized" transactions, institution of policies for product return, rules for warranty disclaimers and limitations placed on a business's choice of law and forum.

The Uniform Electronic Transactions Act ("UETA") recognizes the legal enforceability of contracts in electronic form with an electronic signature. Apart from simply stating that an electronic record may satisfy the requirement of a legally binding writing, the UETA also would require businesses to institute built-in safeguards to prevent sending erroneous transaction records to consumers. Although both uniform acts were debated at length during the July 1999 meeting of the NCCUSL, no votes were taken on the UETA. Some states have begun adopting variations of the draft law despite the difficulty in developing consensus on its provisions. The UCITA fared much better in deliberations and has been fast-tracked by many states since July 1999.

D. International Internet Developments

On May 4, 2000, the European Parliament approved the long-awaited Electronic Commerce Directive ("E-Commerce Directive"), clearing the way for the measure to become law within 18 months. The E-Commerce Directive had been introduced, in draft, in November 1998 but had long been tabled over the issue of ISP liability for content. Like its legislative counterpart in the United States, the E-Commerce Directive establishes an exemption from liability for ISPs where they play a passive role as a "mere conduit" of information from third parties. Similarly, the E-Commerce Directive limits ISPs from liability for other "intermediary" activities, such as storage of information, or "caching." In one of the earliest, most restrictive and most

---

128 Id. at 290-335.
129 Id. at 266 n.88.
130 Id. at 169-200.
131 Id. at 79.
133 An example of a safeguard may be the use of a confirmation screen or return confirmation before execution of an order. Id.
138 Id.
139 Id.
140 Id. The primary provisions of the E-Commerce Directive also address the following issues:
- Place of establishment—The E-Commerce Directive defines the place of establishment as the place where an
productive Internet regulatory initiatives, Singapore’s minister for information and the arts introduced regulations establishing broad categories of proscribed content that may not be accessed by Internet users in Singapore. Encompassing a wide variety of subject matters under the broad definition of “undesirable content,” the regulations were introduced in March 1996 and directed to “rid the Net of content that ‘threaten[s] public order and national security, religious and racial harmony, and morality.’”141 The regulations require licensing all Singapore-based ISPs and “Internet Content Providers” (“ICPs”) (e.g., Usenet groups) who must then “use their best efforts” to remove from their communications any “undesirable content.”142

II. JURISDICTION AND THE INTERNET
(BECAUSE CONTENT MUST GO SOMEWHERE)

Because of the Internet’s universal reach, a business in “Modeltown, U.S.A” potentially is subjecting itself to the uncertain and conflicting laws of countries throughout the world. For the last few years, the Internet has posed unique jurisdictional difficulties for courts. The reason is easy to deduce: e-commerce orders leap from computer to computer without regard for national borders. The good news is that the United States, through statutes and case law, has developed an approach to evaluating jurisdiction in Internet-based cases that applies the traditional minimum contacts test. The bad news is that for most other countries determining proper jurisdiction is anything but a settled issue.

All bases for asserting jurisdiction, whether for interstate or international Internet activity, are rooted in a few basic principles where a state may assert its substantive laws are applicable to particular persons, transactions or communications. Most often, when an act committed in one state causes injury in the territory of another, jurisdiction is based on the locus of the injurious effect, regardless of where the act or omission occurred. Alternative principles of “territory” and “nationality” are less frequently invoked grounds for jurisdiction internationally.

For a given effect to support a particular U.S. jurisdiction, the threshold test is whether a defendant has “purposefully availed” itself of a forum’s laws.143 But few nations carve out such an explicit niche in which specific jurisdiction will be asserted. In fact, some jurisdictions (including the EU) are proposing to tie jurisdiction over Internet activity to the forum of the consumer. Despite what “minimum contacts” may or may not exist with the forum, these proposals are based on

---

141 Sarah B. Hogan, To Net or Not to Net: Singapore’s Regulation of the Internet, 51 FED. COMM. L.J. 429, 436-37 (1999) [hereinafter Hogan].

142 Id. at 440. Although touted as a measure to make “tired state-owned news sites” more interesting, China has created an office of Internet news regulation. Matt Pottinger, China Sets Up Office to Regulate Internet News, REUTERS, at http://www.totaltele.com/view.asp?ArticleID=27131&pub=tt&catid=626 (Apr. 21, 2000). Many concerned with Singapore’s regulatory burdens are similarly wary of China’s Information Management Bureau, whose mandate includes countering the “infiltration of harmful information on the Internet.” Id. Both licensed entities and content providers can be subject to prosecution under this regulatory scheme. See generally Hogan, supra note 141. However, as the closest link to user-created content before it reaches the Internet via an ISP, ICPs are considered “primarily responsible” for undesirable content and bear the initial threat of enforcement. Id. at 443-44. Although the regulations seemingly straitly levels of liability for Internet content, Singapore officials have provided little or no guidance as to what constitutes “undesirable content.” Id. at 457-460.

145 See infra notes 149-56 and accompanying text.
jurisdiction is evidenced by "continuous, systematic and substantial" contacts between the defendant and the forum; specific jurisdiction exists if the claim results directly from the defendant's contacts with the forum state.148 Thus, to support jurisdiction in the United States, the threshold test is whether a defendant has "purposefully availed" himself of a forum's laws, whether specifically (with activity targeted toward the forum) or generally (by making certain minimum activity available to computer users in the forum).

2. Early Internet Cases and the Development of a "Sliding Scale"

U.S. courts initially had great difficulty applying a minimum contacts test to Internet activity.149 Although Internet activity can be characterized and quantified for purposes of identifying "purposeful availment," the intangible nature of Internet-based communications led courts to assent to jurisdiction infrequently because of "traditional notions of fair play and substantial justice."150

To find "purposeful availment" for evaluating jurisdiction, American courts have grouped Internet cases into three categories of activities along a "sliding scale."151 First, purposeful availment can most easily be established when "a state's interest in adjudicating the dispute; 3) the plaintiff's interest in obtaining convenience and effective relief; 4) the interstate judicial system's interest in obtaining the most efficient resolution of controversies; and 5) the shared interest of the several states in furthering fundamental substantive policies. Burger King, 471 U.S. at 478. This is the common law guidepost to justify assertion of jurisdiction applied to the Internet. See, e.g., Pres-Kap, Inc. v. System One, Direct Access, Inc., 636 So. 2d 1351, 1352 (Fla. Dist. Ct. App. 1994); CompuServe, Inc. v. Patterson, No. C2-94-91, 1994 U.S. Dist. LEXIS 20352 (S.D. Ohio), rev'd, 89 F.3d 1257 (6th Cir. 1996).

See, e.g., Panavision Int'l v. Toeppen, 141 F.3d 1316, 1320-21 (9th Cir. 1998) (holding that "domain name hijacker" who registered domain name "panavision.com" and attempted to profit by reselling the domain name to plaintiff owner of registered trademark Panavision was amenable to California jurisdiction because his action was conducted expressly aimed at a resident of California); Patriot Sys. v. C-Cubed Corp., 21 F. Supp. 2d 1318, 1324 (D. Utah 1998) (holding that in an action alleging trade secret misappropriation, unfair competition, copyright infringement and business tort, defendant's website, which the court characterized as passive advertisement, was not sufficient to support exercise of personal jurisdiction); SF Hotel Co., L.P. v. Energy Inv., Inc., 985 F. Supp. 1032, 1034 (D. Kan. 1997) (holding that defendant's connection with Kansas, including plaintiff's allegation that the injury occurred therein, as "tenuous" because mere "passive" website advertising, without more, is insufficient to support jurisdiction over nonresident defendant in dispute involving use of the trademark Sierra Suites); Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119,
defendant clearly does business over the Internet with clients from a particular jurisdiction—e.g., the defendant enters into contracts that require the “knowing and repeated transmission of computer files over the Internet” into a jurisdiction.\(^{152}\) A second, middle category encompasses “interactive websites where a user can exchange information with the host computer.”\(^{153}\) Third, “[a] passive website that does little more than make information available to those who are interested in it,” generally is inadequate to support personal jurisdiction.\(^{154}\) Jurisdiction is asserted often for activity encompassed by the first category, occasionally for the second and rarely for the third. This three-part categorical approach to finding jurisdiction through Internet activities and effects has largely been parroted in recent cases.\(^{155}\) Whether the exercise of jurisdiction is appropriate typically depends upon “the level of interactivity and commercial nature of the exchange of information that occurs on the website.”\(^{156}\) The early Internet cases in the United States indicate how the “sliding scale” would develop.

*CompuServe, Inc. v. Patterson*\(^{157}\) is a seminal decision holding that a computer user cannot come under the jurisdiction of the Ohio courts merely because a computer network was based in the state.\(^{158}\) However, because the defendant placed items into the “stream of commerce” utilizing the Ohio-based computer system, he was “doing business” in the forum sufficient for jurisdiction. The lower court in *CompuServe* held that it would be “manifestly unreasonable” to assert personal jurisdiction in Ohio merely because CompuServe was located there.\(^{159}\) In reversing that decision, the Sixth Circuit pointed out that the software was stored in CompuServe’s Ohio computer system, and although the defendant had never physically entered Ohio, he purposefully conducted business within Ohio over the Internet.\(^{160}\) The right that Patterson sought to protect, a common law trademark for which CompuServe wanted a declaration of noninfringement, was governed by Ohio law and could only come into existence as a result of the operation of Ohio law.\(^{161}\) The *CompuServe* court recognized that the defendant’s activity in Ohio and a common law trademark action were sufficient for jurisdiction, whereas the location of the server alone was insufficient grounds.\(^{162}\)

In addition to sliding scale considerations, most U.S. jurisdictions have determined that apart from the mere access to Internet activity in the jurisdiction, “something more” is needed to show that the defendant purposefully directed his activity to the forum. The cases suggest that the “something more” generally may be identified by answering two basic questions: (1) Would the plaintiff have been injured “but for” the defendant’s conduct in the forum?; and (2) Would the exercise of jurisdiction against the defendant be reasonable, i.e., comport with “fair play and substantial justice” because of the defendant’s purposeful contacts with that jurisdiction?

3. More Recent Cases: How Courts Have Applied the "Sliding Scale"

Raising the bar on the threshold for purposeful availment, in *Bensusan Restaurant Corp. v. King*\(^{163}\) the court held that mere injury occurring through use of the Internet in New York is not enough for personal jurisdiction.\(^{164}\) A defendant who merely makes information available on the Internet, which is then read in New York, does not “avail” himself of the forum, as opposed to one who ad-

\(^{1123-24}\) (W.D. Pa. 1997).

\(^{152}\) *Zippo*, 952 F. Supp. at 1123–24 (holding that electronic commerce involving knowing and purposeful transactions with Pennsylvania residents is sufficient to constitute “doing business in Pennsylvania” for purposes of long-arm jurisdiction in a domain name dispute case).

\(^{153}\) Id.

\(^{154}\) Id. at 1124. Thus, where “a defendant has simply posted information on an Internet website[,] which is accessible to users in foreign jurisdictions,” this activity usually will not suggest personal jurisdiction. *Id.*


\(^{156}\) *Zippo*, 952 F. Supp. at 1123; see also Timothy Nagy,

\(^{157}\) 89 F.3d 1257.

\(^{158}\) *CompuServe*, 89 F.3d at 1265–68.


\(^{160}\) *CompuServe*, 89 F.3d at 1261, 1264–65.

\(^{161}\) Id. at 1267.

\(^{162}\) Id. at 1265–66; see also *Pres-Kap*, 636 So.2d at 1353 (suggesting that the nature of online computer services is such that to bring suit at the site of the central database would be inefficient and subjecting users to the jurisdiction of the database’s location would be “unreasonable”).


\(^{164}\) Id. at 301.
vertises, promotes and sells specifically within New York via the Internet, causing injury. The latter would, in fact, constitute purposeful availment of the forum’s law—the “something more” necessary to assert jurisdiction. That “something more” was detected in Blumenthal v. Drudge, where a publisher of a political gossip website was found to have engaged in a persistent course of conduct in Washington, D.C., creating adequate contacts for jurisdiction. The Internet “magazine” was not targeted exclusively at a Washington audience, but by promoting and gathering information and conducting interviews for his Internet magazine in that forum, Matt Drudge, the site’s publisher, purposefully availed himself of District of Columbia law.

Both Bensusan and Blumenthal represent the nebulous “middle ground” of the evolving sliding scale for finding jurisdiction, where the websites involved can be considered neither completely “passive” nor completely “active.” As in Blumenthal, most of the more recent cases signal that courts look for traditional business contacts with a forum (sales or targeted advertising as in Blumenthal) coupled with the availability of the active website in the forum to support jurisdiction. For example, in Millennium Enterprises, Inc. v. Millennium Music, L.P., the defendants’ interactive website, where consumers could purchase compact discs, request franchising information and join a discount club, was found insufficient to create personal jurisdiction in Oregon. Again, in that more difficult middle category of activity, the court held that the standard for finding jurisdiction requires further refinement to constitute “deliberate action within the forum state.” In Millennium, the defendants had “consummated no transaction,” and made no “deliberate and repeated” contacts with Oregon through their website.

In Coastal Video Communications Corp. v. Staywell Corp., also a middle category case, the plaintiff alleged personal jurisdiction over the defendant based on its website offering products for sale to Virginia residents and sales in Virginia. The court did not decide whether it could exercise general jurisdiction but remanded the case for further development of the record. However, in dicta, the court noted that the defendant’s website:

went well beyond mere advertising and solicitation of products... allowing the online visitor to purchase products through the website, without ever speaking to a representative... in essence, [the defendant] has established an online storefront that is readily accessible to every person in Virginia with a computer, a modem, and access to the World Wide Web.

As in Bensusan, the Coastal court found that the existence of a website alone would not be enough to establish general jurisdiction without evidence that it had reached some segment of the Virginia population and generated sales.

By contrast, the jurisdictional lines for passive and active website contacts with a forum generally can be drawn clearly. For instance, in Jewish Defense Organization, Inc. v. Superior Court of Los Angeles County, the plaintiff sued the New York-based Jewish Defense Organization in California state court for allegedly defamatory statements. Jurisdiction was claimed in California because the Jewish Defense Organization used three California-based companies to host its website. The court decided that merely hiring an Internet pro-

---

165 Id.
166 992 F. Supp. 44.
167 Id. at 56.
168 Id. at 56-57.
170 33 F. Supp. 2d 907.
171 Id. at 920-24.
172 Id. at 921.
173 Id. (quoting CompuServe, 89 F.3d at 1265); see also Winfield Collection, Ltd. v. McCauley, 105 F. Supp. 2d 746, 749 (E.D. Mich. 2000) (finding that sales of two craft items, developed through the allegedly infringing use of a copyrighted pattern, to Michigan residents was the result of random bids made on eBay and did not amount to targeted sales in the forum).
175 Id. at 566.
176 Id. at 569 (finding no specific jurisdiction because there was no evidence the product at issue had been sold to Virginia residents).
177 Id. at 571-72 (declining to decide the question without more information on the record). But see Archdiocese of St. Louis v. Internet Entm’t Group, Inc., 34 F. Supp. 2d 1145, 1146 (E.D. Mo. 1999) (exercising jurisdiction over a “passive” website that specifically targeted information to forum residents); Intercon, Inc. v. Bell Atlantic Internet Solutions, Inc., 205 F.3d 1244 (10th Cir. 2000) (finding personal jurisdiction to be proper over a defendant who knowingly directed e-mail traffic to plaintiff’s server located in the forum).
179 Id. at 1050.
180 Id. at 1055-56.
vider that may have facilities in California would not be enough to exercise jurisdiction over a non-resident defendant in that forum.\textsuperscript{181} In \textit{Mink v. AAAA Development, L.L.C.},\textsuperscript{182} the U.S. District Court for the Southern District of Texas dismissed a complaint on similar grounds.\textsuperscript{183} The developer of a computer software program brought an action against purported competitors, alleging conspiracy to copy a program in violation of the developer’s federal copyright and patent pending rights.\textsuperscript{184} On the developer’s appeal from the district court ruling, the Fifth Circuit held that the corporate defendant’s maintenance of an Internet website accessible to Texas consumers did not support exercise of personal jurisdiction over that defendant.\textsuperscript{185}

At least one case held that an out-of-state defendant could be subject to jurisdiction despite seemingly “passive” contact with the forum. In \textit{Bochan v. LaFontaine},\textsuperscript{186} the U.S. District Court for the Eastern District of Virginia noted that the America Online facilities in the state were “integral” to the act of publishing the material that was the subject of the defamation action.\textsuperscript{187} The court, however, also found a New Mexico defendant subject to jurisdiction because his website, accessible to Virginia Internet users, constituted “doing business” in Virginia even though no sales were conducted over the site.\textsuperscript{188}

In those cases where the contact with a forum is obviously “active,” the basis for jurisdiction often rests on “specific” jurisdictional notions of traditional business contacts with the forum. Such defendants frequently have engaged in contracting, negotiating or systematic traditional sales in the forum in addition to maintaining a fully “active” website, which would itself have suggested “general” jurisdiction over the defendant. Such was the case in \textit{PurCo Fleet Services, Inc. v. Towers}.\textsuperscript{189} In \textit{PurCo}, personal jurisdiction was found proper in Utah over Florida defendants who not only used their websites to solicit business from a Utah resident but also attempted to obtain a cash settlement from the Utah-based plaintiff in exchange for relinquishing rights to a domain name.\textsuperscript{190}

One of the more recent developments in jurisdiction over e-commerce, however, was the limitation of such jurisdiction for a negligence claim related to personal injury through a traditional forum selection clause on a website. The plaintiffs in \textit{Decker v. Circus Circus Hotel} filed suit based on a hotel’s reservation website.\textsuperscript{191} The site included a forum selection clause requiring that any customer making a reservation over the Internet agree in advance to have all disputes settled in Nevada state and federal courts.\textsuperscript{193} Despite the high level of interactivity involved in the site and the court’s ruling that the defendant had placed its services into an “endless stream of commerce,” the court held that the forum selection clause should be enforced.\textsuperscript{194} If this decision is to be considered a portent of developing Internet “contract” law, site administrators would be well served to have customers affirm that they have read and understand a forum selection clause by “clicking” on a link before being allowed to engage in a transaction.\textsuperscript{195}

\textsuperscript{181} Id. at 1055–56, 1061–62; see also \textit{Lofton v. Turbine Design, Inc.}, 100 F. Supp. 2d 404, 411 (N.D. Miss. 2000) (holding that allegedly defamatory remarks placed on a “passive” site did not amount to jurisdiction under Mississippi’s long-arm statute).

\textsuperscript{182} 190 F.3d 333.

\textsuperscript{183} Id. at 333.

\textsuperscript{184} Id. at 335.

\textsuperscript{185} Id. at 337.

\textsuperscript{186} 68 F. Supp. 2d 692 (E.D. Va. 1999).

\textsuperscript{187} Id. at 699.

\textsuperscript{188} Id. at 701.

\textsuperscript{189} 38 F. Supp. 2d 1320 (D. Utah 1999); see also \textit{Online Partners, Inc. v. Atlanticnet Media Corp.}, No. C 98-4146 SI ENE, 2000 U.S. Dist. LEXIS 783 (N.D. Cal. Jan. 18, 2000) (finding jurisdiction over a Florida defendant that operated a website targeting a substantial population of gay men residing in the forum with subscription memberships, membership contracts and online credit card payments).

\textsuperscript{190} \textit{PurCo}, 38 F. Supp. 2d at 1323–26.

\textsuperscript{191} 49 F. Supp. 2d 743 (D.N.J. 1999).

\textsuperscript{192} Id. at 747.

\textsuperscript{193} Id. at 748.

\textsuperscript{194} Id.

\textsuperscript{195} However, if passed and implemented nationally in the United States, UCITA would apply a two-pronged approach to forum selection clauses in consumer e-commerce transactions. First, if a forum selection clause is used in the on-site contract, the forum chosen would apply in the absence of a state law preventing such a selection in the state where the e-business is located. Uniform Computer Information Transactions Act, Draft 1999 § 109(a), at http://www.law.upenn.edu/bl/ulc/ucita/citam99.htm (1999). Second, in the absence of a clause, the governing law would be that of the forum where the e-business is located unless the consumer contract requires delivery of a physical copy of the agreement, in which case the law of the jurisdiction where the copy is to be delivered would apply. \textit{Id.} at § 109(b)(1)–(2). In all other cases, the governing law would be that of the jurisdiction with "the most significant relationship to the transaction." \textit{Id} at § 109(b)(3).
B. European Union and Member State Law
Interaction on Jurisdictional Issues

In the case of an action commenced in a national court against a defendant domiciled within the EU, "personal jurisdiction" presently will be determined in accordance with the 1968 Brussels and 1989 Lugano Conventions ("the Conventions"). Under the Conventions, the basic jurisdictional rule is that a defendant should be sued in his place of domicile. For persons domiciled outside the EU, subject to any agreements as to jurisdiction made between the parties, "personal jurisdiction" is determined in accordance with the traditional jurisdictional rules of the national forum, whether they focus on minimum activity or domicile.

In the most notable example of the application of national jurisdictional law of an EU Member State to a U.S.-based ISP, a Bavarian court asserted jurisdiction over and convicted CompuServe’s German manager for violating German anti-pornography laws. In 1995, German police had served CompuServe with a list of 282 Usenet newsgroups, which, in their view, contained images of violence, child pornography and bestiality. The incriminating content had been stored on CompuServe-U.S.A.’s newsgroup servers. In response, CompuServe-U.S.A. blocked access to the vast majority of the newsgroups by all of its worldwide subscribers, unblocking the newsgroups only after it provided parental control software to its subscribers. Citing the German Criminal Code, German authorities charged CompuServe-Germany’s manager with providing access to illegal content. CompuServe attempted to defend itself under a liability exemption for “online service providers” in Article 1, Section 5 of Germany’s Telecommunications Act. The court, however, rejected the argument that CompuServe-Germany was not an “online service provider” by virtue of its simple hard-line connection to CompuServe-U.S.A. On June 3, 1998, the Landesgericht (District Court of Munich) handed down a two-year suspended sentence and fined the manager $56,200. Ironically, even the prosecutor in the case appeared concerned about its implications and appealed the conviction.

The CompuServe decision posed a dangerous precedent for Internet publishers and ISPs. This case extended liability to the ISP rather than the user-group entity that posted the offending material. Given the prevalence of such material on the

---


197 Reports on Conventions on Jurisdiction and the Enforcement of Judgments in Civic and Commercial Matters, art. 17, 1990 O.J. (C 189) 93. For instance, as Professor Dutson explains, English rules as to service of process outside of the jurisdiction are based in Order 11, r.1(1)(b), (c) and (f) of the Rules of the Supreme Court (Eng.). Dutson supra note 196, at n.18 (citing Conventions, supra note 196, at arts. 4, 21; Case C-351/89, Overscas Union Ins. v. N.H. Ins., 1991 E.C.R. L-3317).


202 Somm supra note 201, at § II.1.

203 Id.

204 Id. at § IV.1.B.2.b. (citing Article 184 Abs 3 StGB of the German Criminal Code). Pursuant to the statute, CompuServe need only "have knowledge of third-party content, i.e. . . . has to know that the unambiguous newsgroups . . . make violent, child, or animal pornographic representations available for use. [This] knowledge, however, does not mean that the accused had to know to individual contents of the respective . . . articles" in order to have violated the Act. Id. at § IV.1.B.2.b (citations omitted).

205 Id. at § IV.1.B.1 (citations omitted).

206 Id. at § IV.1.B.1. The distinction between parent and subsidiary prevented CompuServe-Germany from being considered a "provider" pursuant to Section 3 of the Telecommunications Act, and thus, CompuServe-Germany was unable to benefit from the Telecommunications Act’s liability exception. See Telecommunications Act, art. 1, § 3.


208 Wilske & Schiller, supra note 200, at 122 n.24 (referencing Somm, supra note 201, at § III–IV).
Web and the ease of international access to such sites, it is easy to see how international jurisdictional and enforcement questions will continue to be of great concern to Internet publishers. The CompuServe appeal remained pending for over a year and a half, but in November 1998, Chief Judge Lazslo Ember announced the German state court’s reversal of the decision. As long professed by CompuServe lawyers, Judge Ember agreed that the technical ability to effectively block content simply did not exist at that time, adding that “more could not have been asked of” the accused. In the interim, the lower court verdict adversely has affected Internet business in Germany. In direct response to the lower court ruling, PSInet’s London-based ISP physically moved its Web servers out of Germany for fear of violating Bavarian law. Such drastic steps in response to an assertion of jurisdiction over Internet-based activity are rare, but they provide vivid examples of the extent to which judicial action in a forum can affect a developing business.

Applying the same jurisdictional principles of territoriality, the European Court of Justice (“ECJ”) had permitted a Member State to require service providers who operate in the forum to obey national laws. In Shevill v. Press Alliance, S.A., the ECJ held that only courts of the state in which an Internet publication originated can award damages for the publication of the same libel in other EU Member States. However, broad application of a territorial approach to jurisdiction would preclude Internet users from accessing offending websites from hardware operating within the forum territory. The net result is likely to be an extraterritorial chilling effect on website content. For example, in the CompuServe case, German law was held applicable to bar German users access to certain news groups. As a consequence, the defendants in CompuServe claimed that “German law is dictating what American citizens can read and view.” This effect, the Bavarian court held, simply was due to the “inability of CompuServe to tailor its services to the laws of each country in which it operates” and thus, was “incidental.”

Similar issues regarding an ISP’s ability to block illegal content from an individual country have arisen in France as well. In May 2000, French trial court Judge Jean-Jacques Gomez issued a ruling, which banned French users from Yahoo! English-language auction sites where “Nazi books, daggers, SS badges and uniforms” were sold. The ruling was confirmed by a French court in November 2000. Yahoo!’s defense was two part. First, argued that its auction services were governed by U.S. law, and thus, auctions of Nazi material “cannot be barred because of U.S. constitutional rights to freedom of speech.” Second, asserted that there was “no failsafe way to identify French users and block access” by those users to Yahoo! auction sites. Expert evidence presented at trial showed that only 70% of French Internet users could be identified and then perhaps excluded from use of the Yahoo! site. However, in November 2000, the court gave Yahoo! a deadline of three months to implement a filtering system or face fines of roughly $13,000 per day.

In addition to legislative efforts to define jurisdiction and developing jurisdictional case law, courts worldwide have been frustrated by issues of enforcement. For instance, in the UK, a leaked copy of an official report into alleged “satanic ritual abuse” of twenty-one children in Broxtowe, England was published on the Web by journalists. The county council, which had commissioned the report, refused to publish it, and an English court issued an injunction requiring journalists to remove the report on the basis that such
publication was a violation of copyright. Before the injunction took effect, however, free speech advocates had downloaded the text and sent copies across the Web, rendering subsequent efforts to suppress the report largely futile. Similarly, German authorities ordered the closing of a website operated by a group of Dutch activists when the group published instructions for sabotaging a railway station. Before this site could be closed, copies of the page were downloaded and forty duplicate sites appeared on the Web. Thus, a forum ultimately may decide to assert jurisdiction and enforce its laws, but practical success in stopping the offending Internet activity may not follow. Although a court may grant injunctive relief against an Internet publisher, proliferation of the material may prevent compliance. Thus, limitations on defendant jurisdiction and liability become all the more important.

C. The Effects of National Legislative Efforts to Apply Jurisdiction

When principles of nationality control jurisdiction, the result is the grant of a state’s right to regulate the conduct of its own citizens anywhere in the world. In one example of this approach, Germany makes its nationals residing abroad subject to its prohibition against the dissemination of child pornography. Applications of this type of jurisdictional principle, however, are infrequent, due mainly to the inherent difficulties in the extraterritorial enforcement of such laws. When such “universal” restrictions exist, states typically focus on prohibiting any activity by citizens relating to pornography or the exploitation of children.

Nonetheless, because of universal access to the Web, extraterritorial enforcement issues are becoming increasingly common. For example, the UK’s Financial Services Act of 1996 makes it a criminal offense to place investment advertisements in the UK unless they are approved by the Financial Services Authority (“FSA”). Applying this regulation, the FSA notified the U.S. national mutual fund association, the Investment Company Institute (“ICI”), that mutual fund websites available in the UK are considered to have been issued in the UK. The FSA acknowledges the problem this presents for U.S. mutual fund companies and has stated that it will not take enforcement action against U.S. companies if they comply with certain criteria, including the placement of warnings or disclaimers on their websites. As in the lower court CompuServe ruling, this application of the nationality principle will have a chilling effect on the content of mutual fund websites developed domestically, whether UK courts decide to style the extraterritorial effect as “incidental” or not.

Similarly, an action was brought in France against the Georgia Institute of Technology for running an English-language Internet site from a satellite campus in France. The site allegedly violated a French law requiring that goods and services sold in France be sold and advertised in the French language, but the appellate court upheld the lower court’s decision to dismiss the case on procedural grounds. Despite the fact that the jurisdictional issue was not resolved, Georgia Tech spent more than $20,000 in legal fees, illustrating the monetary consequences to Internet publishers of defending such suits abroad.

1. Legislation in the United States

U.S. legislative efforts aimed at protecting domestic copyrights in the context of the Internet
have employed a territorially principle of jurisdiction. Addressing growing concerns over the potentially unlimited liability of ISPs for website content, the United States enacted new legislation amending the Copyright Act of 1976 ("Copyright Act") to codify technologically sound guidelines for liability. The Online Copyright Infringement Liability Limitation Act was enacted by Congress as Title II of the DMCA.\footnote{Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.); see also Jennifer E. Markiewicz, Comment, Seeking Shelter from the MP3 Storm: How Far does the Digital Millennium Copyright Online Service Provider Liability Limitation Reach?, 7 COMMLAW CONSPECTUS 423 (1999) (discussing the DMCA and its legal implications).} The DMCA limits liability for ISPs and substantially alters case law holding service providers liable for copyright infringement.\footnote{Declan McCullagh, Digital Copyright Law on Trial, WIRED, at http://www.wired.com/news/politics/0%2C1285%2C3716%2C00.html (Jan. 18, 2000) (discussing retrieval tools). These limitations are at the heart of the DMCA, which does not change existing U.S. definitions of and requirements for copyright infringement, but decreases the stakes for providers of a technology not contemplated when the original Copyright Act was enacted.\footnote{17 U.S.C. § 512(a)-(d).} Generally, the functions for which liability is limited are passive activities where the service provider does not exercise any control over, or interact with, the content of the infringing material. The requirements for each function differ, and they are independent of each for determining whether the action of a service provider is protected.\footnote{Id. at § 512(a)-(d).} Thus, an ISP’s activities may qualify for protection as passive activity under one category but not another.\footnote{Id. at § 512(j).}

With regard to defamation, the U.S. Congress included Section 230 in the Communications Decency Act of 1996, largely immunizing ISPs from liability arising from the statements of third parties communicated over an ISP’s facilities but does not include a provision for extraterritorial application.\footnote{Id. at § 512(n).} Subsequent legal decisions have held that, under Section 230, a website owner cannot be held responsible for the defamatory or otherwise tortious statements of individuals who post on its message boards.\footnote{See, e.g., Blumenthal, 992 F. Supp. 44.}

2. The EU Draft E-Commerce Directive on Electronic Commerce Jurisdiction

Perhaps the most troubling development involving the Internet and international jurisdiction was a draft EU directive ("Draft EU Directive"), granting jurisdiction over consumer-based e-commerce transactions to the locus of the consumer. Some observers claim that this jurisdictional approach seriously could stunt the growth of e-commerce and lead to a damaging trade dispute with the United States.\footnote{See, e.g., U.S., EU Closing in on E-Privacy Deal, Official Says, CHI. TRIB., Feb. 7, 2000, at 13.} The European Commission met to hear public comment on the EU Draft Directive in November 1999.\footnote{See, e.g., U.S., EU Closing in on E-Privacy Deal, Official Says, CHI. TRIB., Feb. 7, 2000, at 13.} The legislation would allow disgruntled Internet shoppers to sue e-commerce firms in their own national courts, regardless of whether the company had "actively sought" to sell its product in that country.\footnote{See, e.g. Fiachra O'Marcaigh, Pitfalls in the E-shop, E-COMMERCE, IRISH TIMES, Nov. 8, 1999, at 12. This strong public consensus for analysis as to how the EU Draft Directive might be a disincentive to e-commerce businesses also was reflected in the prehearing submissions. These submissions can be viewed in their original form at the DG-XV website of the European Union at http://europa.eu.int/comm/scic/conferences/991104/contributions.doc (last visited Mar. 4, 2001).}

The EU Draft Directive established the basis for...
jurisdiction as the forum where the "operator" (e-commerce consumer) pursues an activity through a "fixed establishment" (a website). This focus on the activity of the operator and not the e-business is referred to as a "country of origin" approach, meaning "origin" of the consumer activity and not the service provider. This concept forces e-businesses to address potential litigation in the Member State jurisdiction where the consumer resides.

Under prior EU law, unhappy e-commerce customers generally could only seek redress in the country where the e-business is based. However, the EU Council was anxious to update the rules of private international law of the Member States with respect to jurisdiction, particularly the Lugano and Rome Conventions. In May 1999, the Council unanimously agreed on a proposal, which the Commission passed as a proposed regulation on July 14, 1999. Article 15(c) of the proposed Regulation would amend the Rome Convention, allowing a consumer engaged in an e-commerce transaction to "bring an action before the courts in the state of his domicile, without having completed" the necessary steps to conclude the e-commerce contract in that state. This change in the Rome Convention would give force and effect to the "country of origin" principle at issue in the EU Draft Directive.

Although the European Commission approved both the EU Draft Directive and proposed regulation, each needed to be ratified unanimously by EU justice ministers after consultation with the European Parliament. This and other jurisdictional elements were addressed within the E-Commerce Directive. Article I of the approved Directive generally provides that the "law of the country of origin will . . . govern the setting up and provision of online services offered by e-commerce business established in the European Union." Thus, the determination of the place of establishment of an e-commerce service provider is generally of great importance to the application of the "country of origin" principle. Certain legal areas, including taxation, data protection, cartel law, notarial activities and gambling activities, however, are expressly excluded from application of the service provider country of origin principle. In addition, an annex to the Directive excludes additional legal areas, including "contractual obligations concerning consumer contracts" from the operation of the principle. Thus, the country of origin principle, as it is now applied, would be of considerable benefit to e-commerce businesses based in the EU, as it means that their services would need to comply only with the law of the Member State of their establishment. The principle, however, does not apply to the provision of services from outside the EU, and such services provided by an establishment in the United States, for instance, still may be required to comply with the separate laws of all fifteen Member States. The principle arguably does not apply to consumer contracts whether they are consummated with e-commerce providers established within or outside of the EU. Thus, the same multiple Member State application of laws seemingly choice regarding the law applicable to a contract and in the absence of a forum selection stipulates that:

[T]he contract shall be governed by the law of the country with which it is most closely connected . . . It shall be presumed that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence.

would apply to all consumer e-commerce contracts.

III. SETTING RULES

A. Content Regulation Will Likely Continue, but With an Emphasis on Privacy

For the moment, the U.S. preference for industry self-policing seems to have weathered the storm of recent privacy-related legislation and far-reaching recommendations. In the case of the U.S./EU data “Safe Harbor,” self-regulation even may have found a happy coexistence with its highly-structured European legislative counterpart. Grudging acquiescence, however, by companies such as eBay and Bell Atlantic to the likelihood of privacy regulation suggests that some combination of legislative and regulatory initiatives will revisit privacy protection. Despite the Clinton administration’s and Congress’ reluctance to support the FTC’s recommendations, high-profile privacy gambles like those of DoubleClick, and as alleged of Amazon, may drive public opinion to support increased regulation. One only need watch the actions of industry to anticipate where and when the next hot-spots for legislative and regulatory privacy restrictions will be pursued. Given the FTC’s verve in its role as “bad cop” to the administration’s “good cop,” eyes likely will be on Constitution Avenue in Washington for the next regulatory step.

Self-regulation by industry is a necessary first step, although the legislative model suggested by the EU deserves additional debate and consideration by Congress. Given the lengths to which the burgeoning industry could go to merge profiling with personally identifiable customer information, the FTC’s decision to take an active role to monitor and facilitate this self-regulation is appropriate. At present, there is no strong legal protection for consumers and Internet users who casually type personal information about purchases or product preferences into online databases. Further, there is little public understanding of the depth to which online businesses can go to passively profile customer activity on the Web. Thus, a certain degree of regulatory paternalism at this stage is necessary, if only to facilitate industry’s “best practice” policing of itself. Formal regulations governing consumer privacy on the Internet, however, must be developed cautiously with a careful eye toward the impact of such regulations on developing Internet applications. The FTC’s proposal for formal privacy legislation and its subsequent regulatory authority was “too much too soon.” FTC Chairman Robert Pitofsky’s proposal to “marry today’s efforts at self-regulation with an appeals process that would defer to a regulatory body”257 goes further to protect the rights of consumers in an Internet environment, while industry eventually will stray from its own self-regulatory vision, given the opportunity. Such case-by-case appeals, however, easily could overwhelm an agency that has no enforcement authority to monitor and take action against sites that violate customer privacy before appeals develop.

B. Assertion of Jurisdiction—Toward International Standards

Although case law in the United States has developed an approach to evaluating jurisdiction in an Internet-based case, determining the proper jurisdiction internationally is anything but a settled issue. To assist in alleviating this disparity, the American Bar Association concluded a two-year study of international jurisdiction issues with the June 2000 release of its “London Meeting Draft” on Global Jurisdiction Issues Created by the Internet.258 Apart from including a voluminous discussion of Internet issues and how these have affected application of traditional jurisdiction principles internationally, the London Meeting Draft suggests international cooperation to develop jurisdictional standards. The draft proposes a multinational “Global Online Standards Commission” to study jurisdiction issues and “develop uniform principles and global protocol standards by a sunset date,” working with other international bodies considering similar issues.259

259 Id. at 24. For example, the London Meeting Draft notes that international working groups such as the Global Business Dialogue, the Hague Conference on Private International Law, the Internet Law and Policy Forum, the Inter-
Despite the transactional and “access to content” violations of national laws, the “country of origin” approach the EU seems to be taking with regard to consumer-transaction e-commerce jurisdiction wholly is inappropriate at this stage of the medium’s development. As it exists, the jurisdictional element of the E-Commerce Directive seemingly would mandate that both non-EU entrepreneurs and consumers have a knowledge and understanding of the relevant laws of the fifteen EU Member States (in addition to any future EU members). E-commerce participants would face action in each jurisdiction in which a consumer is located. Proponents of the jurisdictional element countered that in applying the country of origin principle, the directive now “recognizes Member States operate a number of different sets of rules regarding marketing promotions and commercial communications, which are impossible to harmonize without killing off the electronic commerce sector in its infancy.”

This argument negates a basic principle of the Internet as a commercial medium. E-commerce, despite ever-increasing gross online product figures, still is in its infancy. A primary merit of the medium for trade is its ability to equalize access to new and underdeveloped markets among both large existing businesses and entrepreneurs. For entrepreneurs, this equality of access effectively would be negated by imposing the law of the consumer’s forum on an Internet transaction without any regard to “minimum contacts” or purposeful availment considerations. When an entrepreneur specifically seeks to sell and advertise in a forum, traditional notions of minimum contacts and purposeful availment with that forum ensure that jurisdiction can be asserted properly. Giving a consumer the ability to simply “assert” that jurisdiction will be asserted regardless of the significance of the Internet venture’s contacts with that forum, however, will stifle the development of e-commerce start-ups. Alternatively, the legal risks arising from the jurisdictional element could force Internet entrepreneurs to exclude EU consumers from the site. Although, as the CompuServe and Yahoo! cases exemplify, such exclusion is rarely possible, and even where possible, likely will not be effective.

Until more jurisdictions clarify the legal liability of Internet users—including ISPs and publishers—e-commerce businesses will remain interested in which forums may assert jurisdiction over them for potential offenses. Some Internet-based businesses may choose to remove operations from forums where laws are not conducive to the services they provide, as PSInet did in response to the CompuServe case. Again, depending upon the technical capabilities of the service provider, it simply may decide to block the availability of the service from the forum. What makes the proposed EU directive particularly troubling is that if passed, the second alternative—blocking the content—becomes perhaps the only viable and safe option for a company concerned about foreign litigation.

Until international standards are developed and implemented, it also will be increasingly important to consider whether a foreign jurisdiction has attempted to enforce its harsher laws against a foreign infringer in assessing how a particular foreign jurisdiction might treat material posted on the Web. As with any business in an uncertain legal landscape, effective e-commerce initiatives should contain an element of risk management. As the above discussions indicate, even the most attentive e-commerce business model with substantiated profit projections can get mired in extraterritorial legal action if the Internet developer does not remain cautiously aware of the risks. Until more foreign jurisdictions define levels of responsibility/liability, as the United States has done for copyright protection, each component—the Internet site, the ISP, the user-group, and the publisher—has a stake in determining whether a foreign state can or will assert jurisdiction over it for a potentially offending site. Unfor

---


C. Infrastructure

This third component of the “legal” Internet, very easily could occupy an article by itself, and it has in this journal and many others. For this reason, the focus of this article has emphasized both content and jurisdiction. Without minimizing the importance of infrastructure regulation to development of the Internet, the concern at this stage is for both access to and improvement of the highest capacity to deliver content. Indeed, the Federal Communications Commission (“FCC” or “Commission”) concluded three reports, two issued pursuant to the direction of Congress (Section 706 of the Telecommunications Act of 1996)262 in January 1999263 and August 2000,264 respectively (collectively, the “706 Reports”)—and an additional report released in October 1999, subsequently republished by the Practising Law Institute (“Cable Bureau Report”).265 The 706 Reports and the Cable Bureau Report gauge the development of high-speed and advanced telecommunications services. All three reports generally conclude that advanced telecommunications capability is being deployed in a reasonable and timely fashion. The three FCC reports, however, concede that rural access to the Internet still is sadly lacking in the United States.266 The debate over Internet access has been fueled, in part, by the debate over unbundled access to cable infrastructure, just as the Telecommunications Act of 1996 mandated unbundled access to telecommunications infrastructure. For the moment, the U.S. Court of Appeals for the Ninth Circuit in AT&T Corp. v. City of Portland267 held off on creating the same degree of open access to cable infrastructure.268

Additionally, the D.C. Circuit has stepped in on the issue of telecommunications carrier compensation for the provision of Internet services. Invalidating much of the FCC’s February 1999 Declaration Ruling on reciprocal compensation,269 the D.C. Circuit found the FCC’s conclusion that ISP traffic is “nonlocal” for purposes of reciprocal compensation was not the result of “reasoned decision-making.”270 The D.C. Circuit accepted the FCC’s assertion of jurisdiction over the provision of Internet services but vacated the conclusion

265 See generally Deborah A. Lathan, Broadband Today, 593 PLI/Pat. 491 (2000).
267 216 F.3d 871 (9th Cir. 2000)
268 See id. at 877 (differentiating both broadband cable programming via high-speed Internet from its more traditional cable counterpart and the need to mandate third-party access at this time).
269 In re Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, Inter-Carrier Compensation for ISP-Bound Traffic, Declaratory Ruling, 14 FCC Rcd. 3689 (1999). Under the “reciprocal compensation” system, established local phone companies pay fees to competing telephone carriers to connect calls for ISP traffic but do not see compensation in return. See Jeremy Pelosiński, FCC Paves to Closed Loophole on Internet Traffic Fees, Total Telecom, at http://www.totaltele.com/view.asp?ArticleID=34350&pub=tt&categoryid=626 (Nov. 29, 2000) [hereinafter Pelosiński]. Because calls to the Internet are not “returned” under the present system, unless states establish different rules, established phone companies will pay roughly $2 billion in compensation in 2000 to rivals without seeing reciprocal fees. Id.
270 Bell Atlantic Tel. v. FCC, 206 F.3d 1, 7 (D.C. Cir. 2000) (explaining that while perhaps sound for jurisdictional purposes, the FCC’s “end-to-end analysis” does not explain how ISP traffic can be viewed as “linked telecommunications” and “continuous works” in order to obviate the view that “calls to ISPs appear to fit” the definition of local calls).
that ISP-bound traffic is not local.\textsuperscript{271} By vacating this conclusion, the D.C. Circuit permitted individual states to continue applying their own rules to allow reciprocal compensation for ISP-bound traffic. However, in upholding the FCC's assertion of jurisdiction over ISP traffic, the D.C. Circuit likely was affirming that component of the Declaratory Ruling that was of prime importance to the Commission on this issue.\textsuperscript{272} If nothing else, the combined impact of the D.C. Circuit's affirmation of FCC jurisdiction with regard to the reciprocal compensation issue and the success of the Commission's argument against cable open access in \textit{AT&T v. City of Portland} should put ISPs on notice. As the FCC continues to define its regulatory role with regard to the Internet, courts have begun to recognize differing elements of its jurisdiction over Internet issues, whether or not increased regulation is a public goal of the Commission.

The access debate, however, additionally has led to close scrutiny over the consolidation of content and infrastructure providers. One argument is that if mergers such as AOL/Time Warner and WorldCom/Sprint are permitted to occur, access to diverse content and high-speed networks, respectively, would be stifled. Given consolidation among large content providers like AOL and Time Warner, one fear is that the Internet simply will become a series of "channels" providing interactive content generated by several large "networks," similar to the way content is provisioned by the major networks on television. Similarly, the WorldCom/Sprint merger was blocked by the Justice Department in August 2000, primarily because of a fear that the combined company largely would control Internet backbone services, blocking open access to rivals.\textsuperscript{273} This debate over the results of proposed mergers has led to considerable discrepancies in how various agencies would preserve competition and/or protect open access. For instance, the same high-speed cable lines that the FCC and Ninth Circuit chose to leave "unbundled" prior and subsequent to the \textit{City of Portland} decision are now being examined for open access by the FTC in light of Time Warner's control over similar cable lines in certain markets.\textsuperscript{274}

The next stage for developing regulatory concern in the United States likely is wireless Internet access and "openness." The UK's BT CallNet Ltd. bowed to pressure on June 21, 2000, allowing its customers to choose rival Internet portals as the home page on their cell phones.\textsuperscript{275} Similarly, in May, 2000, the EU forced France Telecom to take similar action.\textsuperscript{276} By contrast, Sprint PCS, "the most aggressive U.S. wireless service provider, currently offers no way for customers to reprogram cell phones to select home pages"; however, Sprint has indicated a willingness to discuss "openness" issues.\textsuperscript{277}

D. One Internet

When asked to describe the confluence of the Internet and law, the picture I most often suggest to both lawyers and nonlawyers alike is of a wooden ship. The infrastructure of the Internet: the telephone lines and routers, fiber and cable networks, satellite up-links, etc., is the superstructure of the sailing ship—the keel and cross-members. The content of the Internet, whether it is video, data, e-mail, chat sessions or whatever else might keep a college student up at 2:00 a.m., is the system of decks. Depending on our individual needs as Internet consumers, we position ourselves on certain decks and shield our loved ones from content that would otherwise be inappropriate, yet, the decks are still there. Third and finally, jurisdiction is represented by the hull of the ship. Depending on which perspective you take, the hull can either keep content out or hold content in, and the true utility of a fully-developed Internet jurisdictional paradigm will be its ability to accomplish both in a predictable fashion, depending on contacts with the forum. Just as a ship cannot function without the unified support of keel, hull and deck structure, regulation of the Internet

\textsuperscript{271} Id.

\textsuperscript{272} The FCC announced in late Nov. 2000 that it hoped to soon begin a plan to phase out the reciprocal compensation loophole within two years. See Pelofsky, supra note 269.

\textsuperscript{273} The combined company would have controlled access to 53% of the Internet backbone. Dan Carney et al., \textit{Whose Net is it, Anyway?}, Bus. Wk., July 31, 2000, at 100.

\textsuperscript{274} See Jill Carroll & John R. Wilke, \textit{Time Warner, AOL} and the Culture of Regulatory Change

\textsuperscript{275} [\textit{Huddle in Washington, Wall St. J.} Sept. 22, 2000, at A3. The FCC similarly indicated in late Aug. 2000 that it is not satisfied with AOL and Time Warner's pledges of Internet service access. See id.]

\textsuperscript{276} See Dan Carney, \textit{Whose Web is it, Anyway?}, Bus. Wk., July 31, 2000, at 100.

\textsuperscript{277} Id.
cannot have strength without a consistent, supportive structure.

To conceptualize the Internet in this fashion is to accept that regulatory policy must be both developed and monitored centrally, if at all. The increased availability of high-speed infrastructure will impact the availability of new and advanced content, apart from the basic notion that content simply cannot exist without it. For example, availability of IP Multicast\(^2\) or similar full motion video applications on the Web will depend on the infrastructure’s ability to support the content. Likewise, that content will be accessible in jurisdictions that heretofore would have not been considered by a content provider. Development of jurisdictional systems with international predictability will facilitate when, where, and how applicable laws and regulations will apply to the Internet. How each of these three components of the Internet are managed and regulated will impact each other in time, if not immediately.

Internationally, the Internet Corporation for Assigned Names and Numbers (“ICANN”) often has been pressured by Internet professionals to take on a larger quasi-regulatory role beyond its current mission to administer domain names.\(^3\) ICANN, a nonprofit California corporation, was appointed in October 1998 to “assume duties for managing domain name” and Internet root serv-

---

\(^2\) Typical Internet communications are conducted in "unicast," whereby each communication consists of an individualized stream of data between the sender and one or more receivers. Unfortunately, the unicast method of information delivery simply cannot scale to support a vision of widespread radio and television broadcasts on the Internet. When using a unicast application for a teleconference, for instance, copies of the same data are sent point-to-point to however many receivers are present. IP Multicast enables one copy of digital information, such as a video stream, to be received by multiple computers simultaneously. See Vicki Johnson & Marjory Johnson, IP Multicast Background, 1, at http://www.stardust.com/mcast/whitpap/ background.htm (June 25, 1999). With IP Multicast, one stream is sent by the server to the network and then a distribution tree forms. Leonard Giuliani, Deploying Native Multicast Across the Internet, 1, at http://www.stardust.com/mcast /whitepapers/ sprint_multicast_01.htm (2000). Interested listeners simply add a branch to the tree and routers replicate packets of the multicast stream at each branch in the tree. Id. In this way, no packets are ever duplicated in the network, and the server never has to send more than one stream of data. IP Multicast is an Internet application, but it uses the topology of the Internet backbone very differently. In addition, unlike transmission of a standard cable television signal, IP Multicast broadcasts involve “two-way information exchange and storage, even when a user views seemingly static content.” Portland, 216 F.3d at 877 (differentiating broadband cable pro-

---

\(^3\) ICANN’s duties also include overseeing the competing interests of trademark holders and small businesses, and of multinationals and foreign nations. Apart from obvious conflicts in mediating these two groups of competing interests, some observers feel that it is “not possible to put a private organization in charge of public rights.” Both the leadership of ICANN and those who interact with it on a daily basis insist that the organization is not seeking a greater role in Internet governance. By contrast, such a role is being arguably sought by the International Telecommunications Union (“ITU”). For instance, at a “World Development Symposium for Regulators” in late November 2000, sponsored by the ITU in Geneva, an “electronic regulatory hotline” was proposed. The hotline would be staffed at the ITU’s Bureau for Telecommunications Development by a volunteer pool of regulators who would provide rapid response to questions and best practice on issues ranging from telecommunications “first call” to regulation of e-commerce transactions. Although not a private, self-regulatory-organization (“SRO”) like ICANN, the ITU’s bureaucratic speed and regulatory inefficiency have driven the primary arguments to date against its increased role in Internet governance.
Governance has been discussed widely and to an extent, implemented. Apart from ICANN's international domain name jurisdiction, on the national level, the "Complaint Centre" in Germany is an SRO of German ISPs, which deals with complaints by Internet users against German providers of Internet content. When appropriate, the Complaint Centre can inform the legal authorities in cases involving content that is illegal in Germany. In theory, vesting aspects of Internet governance in an international SRO seemingly could encompass both U.S. preference for self-regulation over e-commerce and the more structured legislative approach of the EU. This concept, however, presents three immediate challenges. First, no one, existing organization is suited for this international role. Second, the success or failure of the EU's Safe Harbor enforcement compromise with the United States likely will give a strong indication as to whether self-regulation and legislative constructs can coexist internationally with regard to the Internet, an international medium. Third and finally, successful SROs with broad regulatory authority arguably have taken decades to develop, as did the New York Stock Exchange before being vested with SRO authority pursuant to the Securities Exchange Act of 1934.

At the national level, there likely is not a present need for one U.S. agency to have national regulatory authority over this developing medium. An Office of Internet Policy, with close contact and interrelationship with involved departments and agencies, however, should be fostered in the new administration. At the very least, this office should seek to both advise and liaison between involved governmental organizations and multinational corporations to ensure that if regulations are created or international governing bodies fostered, the impact of these efforts can be measured carefully and centrally across regulatory jurisdictions before they are implemented.

At first glance, and for purely domestic reasons, it would seem that industry prefers the current self-regulatory posture of the United States. However, this preference has weakened the U.S. bargaining position for purposes of international negotiation and regulatory standard-setting. Despite the unique posture of several multinational corporations, including WorldCom and Sprint, at the forefront of Internet regulatory issues, U.S. corporations have had little to point to as a domestic regulatory model for comparative negotiation. Thus, coalition building and development of uniform policy positions with foreign corporate counterparts must be a near-term goal.

The National Telecommunications and Information Administration ("NTIA") has an executive level mandate to: "support a predictable, minimalist, consistent and simple legal environment that will facilitate the growth of electronic commerce, and help resolve privacy, content regulation, copyright protection, taxation and other similar issues." This mandate, however, should either be strengthened or re-delegated. Without strong, central authority over Internet policy, agency "turf battles" over nascent regulatory jurisdiction will likely become more prevalent. The NTIA does not seem to have the public administrative support or passive authorization to alleviate this. For instance, despite the FTC's recent report and legislative proposal on privacy regulation, and the agency's interaction with the FCC on issues relating to the AOL/Time Warner and other mergers, the FTC is not referenced as an agency the NTIA assists in developing Internet policy.

Both the FCC and FTC have admirably begun to address Internet issues under existing regulatory authority. This existing authority, however, is not sufficient to alleviate jurisdictional conflict, particularly over issues of content and open access. The FTC's pro-competitive regulatory authority will, at times, be at odds with the FCC's "public interest" standard for scrutinizing mergers and alliances. Even within a single agency, subtle turf issues are discernible. Consider the FCC Cable Services Bureau's ("Cable Bureau") issuance of a separate report on the state of broadband access. Although each FCC report relating to further development of, and open access to, broadband technology is crucial to further development, the Cable Bureau report on inherently similar cable and common carrier issues and tech-
technology, is peculiar as a separate and very individual effort.

A strong executive-level office also should ensure that international standard-setting authority, particularly in the areas of international jurisdiction, the World Trade Organization and ITU, is vested closely to the Office of the President. The goal of such an office would be to develop a cohesive plan of action to bring to any international negotiating table, whether or not final negotiating authority is delegated to the State Department, separate agency experts or corporate representatives. The Internet has and will continue to affect each of our lives. In the most basic sense, regulation of this developing medium is a “risk management” attempt. In a litigation setting, the primary objective of risk management is to “marginalize” a potential plaintiff’s success. In the world of e-commerce, centralized planning and awareness of the regulatory risks associated with regulation of this medium is not only crucial to securing our own national success in this environment, but also would serve to secure the future of the emerging virtual economy.