1 Va. J.L. & Tech. 3 (Spring 1997) <http://vjolt.student.virginia.edu>
1522-1687 / © 1997 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL of LAW and TECHNOLOGY

UNIVERSITY OF VIRGINIA	SPRING 1997	1 VA. J.L. & TECH. 3

Jurisdiction in a World Without Borders*

by Dan L. Burk**

"*Man should not draw lines on the land. The winds will dim them, the snows will cover them, and the rains will wash them away.*"

-- attr. Cochise

I. Introduction

1. As humankind enters the 21st century, the words of the nineteenth century Native American leader Cochise have suddenly taken on new meaning. Confined in his later years to the invisible boundaries of a government-created Indian reservation, the Apache leader knew all too well the central role of political boundaries in Western jurisprudence. Yet not even Cochise could have foreseen that before the end of the millennium, the white man's own technology would blur those imaginary lines far more effectively than the elements ever could.

2. In particular, the advent of global computer networks has rendered geographic boundaries increasingly porous and ephemeral. Use of the global Internet computer network is rising exponentially.[1] As Internet subscription increases, just as where any sizable number of human beings interact, disagreements may be expected to arise. As the community of Internet users grows increasingly diverse, and the range of on-line interaction expands, disputes of every kind may be expected to occur. On-line contracts will be breached, on-line torts will be committed, on-line crimes will be perpetrated. Although many of these disputes will be settled informally, others may require formal mechanisms for dispute resolution.

3. In response to growing on-line activity, the federal legislature has begun paying some attention to the network,[2] and state regulators seem equally anxious to leave their mark on the burgeoning field of "cyberlaw." The first fruits of their efforts are already beginning to appear. The Georgia legislature has enacted new law prohibiting cybernauts from "falsely identifying" themselves on-line.[3] Similar legislation is pending in California.[4] In Texas and Florida, regulators overseeing the legal profession have interpreted their rules on professional conduct to cover law firm web pages -- including, apparently, the pages of out-of-state firms -- as "attorney advertising" within their states.[5]

4. Of course, even without the enactment of new laws or regulations, there are already on the books plenty of laws that states might apply to the Internet, including consumer protection statues and other public law to police on-line behavior and commerce. The Minnesota Attorney General's office in particular has been very aggressive in pursuing what it considers to be on-line violations of Minnesota law, filing a flurry of lawsuits against out-of-state advertisers and service providers.[6] The Illinois Attorney General's office is by all accounts equally eager to get into the cyberspace game.[7] By contrast, the Attorney General of Florida, has opined that because of the novel nature of the Net, forays into on-line enforcement of current law would be premature.[8]

5. The wisdom of the Florida position becomes apparent when the nature of the Internet is carefully considered. The Internet extends beyond the boundaries of any of the states, and the effects of state regulation will likewise spill over state borders. Such regulatory leakage implicates constitutional doctrines designed to preserve both the sovereignty of the individual states and the coherence of the United States as a whole. The prospect of states applying haphazard and uncoordinated multijurisdictional regulation to the Internet's seamless electronic web raises profound questions regarding the continued growth and usefulness of this medium. And, given the international nature of the network, even centralized federal attempts at regulation raise grave questions regarding international sovereignty and jurisdiction.

6. Among the most serious questions raised by state or federal Internet regulation are those relating to personal jurisdiction: a tribunal's ability to subject an individual to adjudication in that forum. During the latter part of 1996, a wave of court decisions relating to personal jurisdiction surged out of United States trial courts. But these decisions for the most part have failed to seriously grapple with the nature of the Internet and the broader implications of stretching current legal doctrine to

fit this new medium. The geographic transparency of the Internet may well place such adjudication of transborder disputes outside of any jurisdictional analysis yet contemplated by territorially-bound law. Although problems of multijurisdictional coordination and competition are not unique to regulation of the Internet, the unique nature of the Internet may necessarily trigger constitutional limitations designed to limit governmental regulation originating outside the state's physical borders. But in order to fully appreciate the difficulties involved in applying current law to Internet jurisdiction, one must begin by considering the nature of the medium at issue.

II. The Nature of The Net

7. The Internet has been called a network of networks, local computer systems hooked to regional systems hooked to national or international high-capacity "backbone" systems.[9] Each link, or node, in this web is a computer or computer site, all connected together by a variety connections: fiber optic cable, twisted-pair copper wire, microwave transmission, or other communications media. Each computer in the network communicates with the others by employing machine-language conventions known as the IP, or Internet Protocols.[10] Indeed, it is these protocols that define the network; those machines that talk to one another using IP are the Internet.

8. This medium defined by these shared protocols is distinctly unlike any other. First, the Internet is a packet switching network.[11] Unlike communications media that tie up the entire channel in real time during transmission, the Internet breaks information into discrete packets of bits that can be transmitted as capacity allows. Packets are labeled with the address of their final destination, and may follow any of a number of different routes from computer to computer until finally reaching their final destination, where they are reassembled by the recipient machine. Thus, packets from a variety of sources may share the same channel as bandwidth allows, promoting more efficient use of available carrying capacity.

9. Second, the Internet is designed around "smart communications." Because it is a network of computers, mechanical intelligence is available at every node of the network, and the design of the Internet takes full advantage of this characteristic. Computers at each node monitor traffic on the network, and route packets along the least congested route to the next node, from which the process is repeated. Each computer in the network assesses whether to temporarily hold packets or send them on, so that maximum use is made of the available carrying capacity at any given time.[12]

10. There is no centralized control of the packet routing, or for that matter, of almost any other aspect of the Internet.[13] From a technical standpoint, each computer acts autonomously, coordinating traffic with its nearest connected neighbors, and guided only by the "invisible hand" that arises from the sum of millions of such independent actions. From a management standpoint, each node is similarly autonomous, answering only to its own systems administrator. This means that there is no central authority to govern Internet usage, no one to ask for permission to join the network, and no one to complain to when things go wrong.

11. Finally, the Internet protocol provides for "telepresence" or geographically extended sharing of scattered resources.[14] An Internet user may employ her Internet link to access computers, retrieve information, or control various types of apparatus from around the world. These electronic connections are entirely transparent to the user. Access to Internet resources is provided via a system of request and reply; when an on-line user attempts to access information or services on the network, her local computer requests such access from the remote server computer where the desired is housed.[15] The remote machine may grant or deny the request, based on its programmed criteria; only if the request is granted does the server tender the information to the user's machine. The "virtual machine" created by the connection appears to be the one at the user's fingertips -- indeed, depending upon local network traffic, a distant facility may prove to be faster and more responsive than one in the next room. Internet users may therefore be completely unaware where the resource being accessed is in fact physically located.

12. These features make available a vast array of interconnected information including computerized digitized text, graphics, and sound. The usefulness of such computer networking has not been lost on businesses, or for that matter, on consumers. A crop of private Internet access providers has developed to offer network access and facilities to such customers outside the research community. Consequently, although the academic and scientific research community remains an important part of the Internet community as a whole, private and commercial traffic is becoming a dominant force in the development and growth of the "electronic frontier." Businesses of all types routinely use the Internet for a variety of commercial transactions, and consumer services have begun to appear. At present, commercial traffic on the network generally culminates in an exchange of physical goods, and it is presently possible to access a variety of mail-order catalogs on-line, to arrange for purchase of music, books, fast food delivery, even flowers.[16] The variety and availability of such consumer services is likely to grow, as are attendant facility for on-line advertising and marketing.

13. In particular, the network offers novel opportunities for transactions involving information-based goods and services.[17] The network already supports access to a wide variety of information utilities including databases and computational facilities, as well as archives of text, music, graphics, and software. Information and information-based services on the network have traditionally been offered for free, but will increasingly be offered on a commercial basis. Unlike transactions involving physical goods, delivery of digitized information products such as music, photographs, novels, motion pictures, multimedia works, and software can be accomplished entirely within the network itself. Such information products already comprise an sizable portion of the gross national product of developed nations. That portion is likely to increase world-wide, and the Internet will facilitate such increases.

III. Geographic Indeterminacy

14. However, the rules of the road for on-line commerce are likely to be very different than those for

business interactions in real space. Much of this difference stems from the Internet's telepresence features, which render the network technologically indifferent to physical location. So insensitive is the network to geography, that it is frequently impossible to determine the physical location of a resource or user.[18] Such information is unimportant to the network's function or to the purposes of its creators, and the network's design thus makes little provision for geographic discernment. In real space, a business can usually locate the person or entity with whom it is interacting; this tends to facilitate identification of partners and validation of transactions. This process is far more difficult in cyberspace, when the parties in a transaction may be in adjoining rooms or half the world away, and the network offers no way to tell the difference.

15. For example, screening or blocking of Internet resources by country is nearly impossible. In theory, it might seem that the request-and-reply sequence of access to Internet resources could be used to screen requests, denying those requests originating in jurisdictions with which the host machine's operator did not wish to have contact. But in practice, such screening is eminently unworkable. Internet protocols were not designed to facilitate geographic documentation; in general, they ignore it. Internet machines do have "addresses," but these locate the machine on the network, and not in real space.[19] Of course, some Internet addresses do include geographic designators, or designators that might be geographically identifiable -- for example, an Internet address containing the domain ".uk" located in the United Kingdom. An Internet host who wished to deny resource access to British users might instruct her machines to refuse access requests originating at the ".uk" domain.

16. Unfortunately for the success of such a screening system, the majority of Internet addresses contain no such geographic clues. More to the point, all Internet addresses are eminently portable because they are not physical addresses in real space, but are rather logical addresses on the network.[20] Today the operator of the "foo.bar" domain may reside on a machine operating in London, but tomorrow he may transfer his operation -- and his Internet address -- to a host machine in Tokyo.[21] The transfer need not even involve physical movement; the operator may remain in London, if indeed he does not already dwell in another jurisdiction altogether. This transfer, whether physical or logical, will be completely invisible to Internet users; when they seek access to resources at that address, the request will be routed to that location on the network, without reference to its physical location.

17. There is, in other words, simply no coherent homology between cyberspace and real space. Even if in some instances an Internet address tells one something about the location of a given machine, it tells nothing about the location of the user of that machine.[22] For example, an Internet user located in California can easily maintain accounts on computer systems located in other states -- in, say, Virginia. The user can effortlessly use the Internet utility called "telnet" to access the Virginia account from his California account, and use the Virginia account exactly as if he were physically there -- from the user's perspective, the connection is completely transparent.[23] Similarly, any system that the user accesses via the Virginia will "see" the user as being "located" at an Internet domain in Virginia -- but the data is in fact being passed through to California. If

California domains were on a site's list of prohibited access, access via Virginia would elude current protocols for screening and blocking.[24] Similar access could be achieved by dialing up an account in another jurisdiction via a toll-free 800 number.

18. Such Internet features allowing remote access and anonymous login strip the network of any meaningful clues by which one might screen users by geographic region.[25] A user need not actively cloak her activities on the Internet for her physical location to be obscured; geographic indeterminacy is simply part of the network's normal operation.[26] Additionally, it must be emphasized that these examples of remote log-on anticipate only the most routine uses of the Internet's capabilities; they do not involve exotic -- but readily available -- technology, such as public key cryptography[27] or anonymous remailers,[28] that could be used to *actively* conceal a user's location. Neither do the examples contemplate illegal activity, such as unauthorized hacking into another's computer account, in order to mask a user's physical location.[29]

19. And finally, to fully appreciate the inchoate nature of Internet geography, it is important to consider the common Internet practice of "caching" copies of frequently accessed resources.[30] In order to better manage packet traffic, some Internet servers will store partial or complete duplicates of the materials from frequently accessed sites; keeping copies on hand alleviates the need to repeatedly request copies from the original server. An Internet user attempting to access the materials will never know the difference between the cached materials and the original. The materials displayed on the user's machine will appear to come from the original source, whether they are actually transmitted from there or from a nearby cache. Note again that in using the term "nearby," I refer to logical proximity, not physical proximity -- the resources may be accessed from a cache that is physically farther from the user than the original source if the cache is more accessible because of lower traffic or usage.

20. Thus, the user may be accessing materials at a particular site, or he may be accessing copies of those materials located on a different machine half a world away. Or, he may be receiving materials transmitted from the cache, updated by occasional transmissions from the original server. This means that not only is it impossible to be certain of an Internet user's physical location, it is equally impossible to be certain of an Internet resource's physical location. Indeed, given that the network lends itself to distributed computing applications, an Internet resource may well have no discrete physical location -- portions of the resource may be resident on many different machines around the world, to be transparently and seamlessly assembled as needed when called for.

IV. Criminal Jurisdiction

21. Questions of criminal jurisdiction will almost always be couched in terms of venue. This is because criminal jurisdiction is always based upon the physical presence of the defendant within the forum and before the tribunal.[31] The Constitution's confrontation clause precludes criminal "default judgments." In turn, physical presence for a criminal trial within the United States is almost never an issue because of the constitution's extradition clause[32] and an implementing

extradition compact among the states[33] -- as long as there is a facially proper complaint, extradition is available. As a practical matter, then, a criminal jurisdiction question can really only turn on whether there was a facially proper complaint, that is, whether there is probable cause to believe that the defendant committed all or part of the crime alleged within the venue of the particular forum.[34] Under criminal jurisdictional doctrine, venue lies if a material element of the crime was initiated or completed within the forum. For some multi-jurisdictional crimes, such as kidnapping, a material element of the crime need only have been in the process of execution within the forum.[35]

22. The interaction of these rules may subject cybernauts to unexpected criminal liability in almost any jurisdiction with Internet connectivity. The government may have wide lattitude in deciding where to bring a prosecution against alleged on-line offenders, as the nature of the Internet is to facilitate contact between many jurisdictions, and elements of the offense may conceivably have been initiated, completed, or furthered not only where the defendant was physically located, but in all the jurisdictions that his actions electronically touched. Once venue is properly established, obtaining extradition -- and hence jurisdiction over the person of the defendant -- from another state is relatively trivial. This problem was demonstrated in a non-Internet electronic communications case, *United States v. Thomas*.[36] The defendants were convicted of supplying obscene materials to Memphis Tennessee from their dial-up computer bulletin board service (BBS) in Milpitas, California. The defendants argued that venue in Tennessee was improper because the files entered the jurisdiction via were downloaded by a subscriber, rather than sent by the BBS operators. The court rejected that argument, holding that because the effects of the defendants' conduct reached Tennessee, venue was proper there.

23. The on-line environment of the Internet of course differs substantially from that of the dial-up bulletin board. Yet the geographic indeterminacy of the Net may be of little consequence where criminal provisions are concerned. Criminal statutes may in some instances operate on a strict liability standard, and simply trafficking in the on-line contraband will be sufficient to trigger some jurisdiction's penal provisions. And even where a mens rea requirement is specified, it will seldom relate to the defendant's knowledge of concerning jurisdiction. In the *Thomas* case, the statute in question was held not to require knowledge of the jurisdiction to which obscene material was downloaded, but simply knowledge that the material was being accessed.[37]

24. Such a statutory construction of the knowledge element of an offense is fairly routine.[38] Internet users may be unaware of the jurisdictions their activities touch, and it would be impossible as a practical matter for them to know the law of every jurisdiction they might touch -- yet they are still presumed to know the law. The apparent unfairness of this rule is ameliorated only slightly by constitutional due process requirements: in situations where a jurisdiction requires affirmative steps that the average citizen could not anticipate, and of which the citizen has no notice, due process may be relieved responsibility for the failure to act. This rule was articulated by the Supreme Court in *Lambert v. California*,[39] where the court held that "knowledge" for purposes of a felon registration statute meant knowledge of the registration requirement. This is a very

limited rule, however; *Lambert* has been followed very seldom and requires more than simple ignorance of the disputed statute.[40] In order to invoke *Lambert*, it would seem that the an unwary cybernaut would have to run afoul of a local ordinance so unusual that the he cannot be presumed to have notice of its requirements. The inherent dividing line may be one of malum prohibitum versus malum in se;[41] where the activity is prohibited by a common sense of morality, rather than by the whim of the legislature, citizens will be presumed to know of its requirements.[42] Yet, ironically, in an on-line environment, citizens cannot be frequently will be unaware of the jurisdictions their actions may reach.

V. Civil Jurisdiction

25. In contrast to criminal proceedings, civil proceedings in the United States may proceed in the absence of the defendant, and result in a default judgment. The question of when it is permissible to proceed without the defendant's presence has generated a body of constitutional law related to procedural fairness and due process. Much of this jurisprudence was spurred by the mobility of the populace, and the personal jurisdiction problems posed by virtual commerce and Internet telepresence are in many ways the culmination of a long evolution of legal doctrine occasioned by changing technology.[43] Traditionally, jurisdiction over the person was premised on the physical presence of the individual in the forum; this continues to be a viable jurisdictional basis.[44] However, increased physical mobility due to automobiles and other modern transportation placed this jurisdictional basis under severe strain,[45] as did disputes over "virtual" entities such as corporations that have no physical situs,[46] and over "virtual" properties such as stocks[47] and debts[48] that similarly lack physical form.

26. As a response to the imminent collapse of jurisdiction based on physical presence, the Supreme Court configured new rules based upon a kind of "virtual" presence. Beginning with the notorious *International Shoe* opinion, the Supreme Court began developing a set of criteria for requiring non-residents of a state to defend lawsuits in that state.[49] According to *International Shoe* and its progeny, the Due Process Clause of the Fourteenth Amendment constrains state courts from exercising personal jurisdiction over defendants who lack sufficient contacts with the forum state.[50] Via "long-arm" statutes, states may authorize their courts to exercise jurisdiction over extraterritorial defendants up to the limits of inherent in the Fourteenth Amendment. This constraint preserves both the sovereignty of the states in a federal system,[51] and the individual right of a defendant to affiliate himself with one or another of those sovereigns.[52] Unless the defendant has sufficient quantum of contact with the forum state, that state's exercise of jurisdiction over the defendant would offend "traditional notions of fair play and substantial justice."[53]

27. Two broad classes of jurisdictional situation have been recognized with regard to a defendant's contacts. The first situation, classified as "general jurisdiction" involves an attempt to assert jurisdiction over a defendant when the defendant's contacts are unrelated to the dispute.[54] An

assertion of general jurisdiction over the individual is permissible if the defendant's contacts with the forum are systematic and continuous enough that the defendant might anticipate defending any type of claim there.[55] A second jurisdictional situation arises where the facts of the dispute arise out of the defendant's contacts. A court may exercise jurisdiction over the defendant if the defendant has "minimum contacts" with the forum are such that he might anticipate defending that particular type of claim there.[56] The contacts relied upon may be isolated or occasional, so long as they are purposefully directed toward the forum.[57]

28. The specific jurisdiction situation is rather more problematic than that of general jurisdiction, as the nature and extent of the contacts, as well as their relationship to the claims asserted, must be carefully examined. The general requirement that must be satisfied for Due Process purposes is a sort of "foreseeability" that the defendant is on notice of fora where she may be called upon to defend a suit.[58] This "foreseeability" requirement allows the defendant to structure her activities so as to prepare for potential liability, or avoid states where she does not wish to assume liability.[59] A precise catalog of the activities that will render one amenable to suit in a particular jurisdiction remains elusive, but it appears clear from the Supreme Court's due process opinions that direct pecuniary gain from doing business in a jurisdiction greatly enhances the foreseeability of defending a suit in that jurisdiction. Assertion of jurisdiction over a defendant may be particularly facilitated if the cause of action arises out of a course of business dealings pursuant to an express contract;[60] and should the contract contain a choice of forum clause, so much the better: the defendant's acquiescence to jurisdiction is then virtually assured.[61]

29. The Supreme Court has also indicated that in some cases where an intentional tort is directed toward an individual or entity within a particular jurisdiction, the tortfeasor should anticipate defending a suit in that forum. The Supreme Court decision in *Calder v. Jones*[62] held that California jurisdiction over a Florida defendant was proper because the allegedly libelous statements directed at the defendant injured her in her home state of California. Some intermediate courts of appeal have seized upon this doctrine to formulate a so-called "effects test." Under this test, jurisdiction would be proper when some effect of a defendant's actions is felt within the forum state.[63] Other circuits have flatly rejected this test, observing that it flies in the face of much of the Supreme Court's due process jurisprudence.[64] These courts recognize that the standard cannot simply be that whenever an intentional tort is alleged, jurisdiction is proper in the plaintiff's home state because the harm will be felt there.

30. The opinion in *Calder* repeatedly emphasizes that the defendants knew that the plaintiff resided in California and that their newspaper's largest circulation was in that state.[65] Moreover, the definition of the intentional tort in *Calder* required actual malice or reckless disregard of the truth -- the standard set out by the Supreme Court in *New York Times v. Sullivan* for libel actions against newspaper publishers.[66] The Court in *Calder* refused to take the "chilling effect" of liability into account in the jurisdictional analysis, stating that to recognize such a new jurisdictional factor would be "double counting" -- the standard to prove the tort, they said, already takes First

Amendment concerns into account.[67] This reasoning seems sound if we consider that the facts necessary to allege actual malice or reckless disregard themselves indicate activity purposefully directed toward the defendant's place of residence. Thus, the libel standard encompasses the jurisdictional standard, but not every intentional tort will do so.

31. The Supreme Court has also offered a list of five jurisdictional "fairness factors" that may require a separate assessment, especially when the defendant's contacts with the forum are attenuated.[68] The factors to be weighed before subjecting the defendant to jurisdiction include the inconvenience to the defendant of defending in that forum, the forum state's interest in adjudicating the dispute, the plaintiff's interest in obtaining convenient and effective relief, the interstate judicial system's interest in efficient resolution of interstate conflicts, and the shared interest of the states in furthering substantive social policies.[69] Additionally, where jurisdiction over foreign nationals is at issue, the Supreme Court has indicated that potential interference with the procedural and substantive policies of other nations, as well as the impact on the foreign relations policies of the United States may constitute additional fairness factors for consideration.[70]

32. These due process considerations constrain the reach of state courts. Where federal courts are concerned, similar due process considerations apply, but arising under the Fifth Amendment constraints on the federal government, rather than the Fourteenth Amendment constraints on the states.[71] Under an unfettered Fifth Amendment jurisdictional analysis, Fourteenth Amendment concerns surrounding state sovereignty vanish, as there is no question of interstate comity when the sovereign in question is the federal government.[72] Due process considerations of fairness and affiliating contacts remain central in a federal jurisdictional analysis, but contacts inquiry may in theory consider contacts with the nation as a whole, rather than with any particular state.[73]

33. However, Fifth Amendment jurisdictional analyses are seldom unfettered, as the reach of federal courts is set by Congress within the limits of due process. Congressional authorization has been closely tied to service of process. In the majority of situations, Congress has instructed the courts to exercise no more jurisdictional authority than is permitted under the "long-arm" statute of the state in which the federal court is situated.[74] However, in "federal question" cases where the statute at issue authorizes nationwide service of process, federal courts may exercise jurisdiction to the nationwide limits of the Fifth Amendment.[75] Additionally, under Federal Rule of Civil Procedure 4 (k)(2), a district court may look to the nation as a whole to aggregate contacts if the jurisdiction conferred under the local long arm statute is insufficient and if jurisdiction would not lie in any other district.[76]

VI. Virtual Contacts

34. These jurisdictional criteria, though familiar to every first-year law student, have not necessarily produced recognizably coherent results when applied to real-space activity. A comprehensive

theory of personal jurisdiction has largely eluded commentators. Indeed, although we may discern the broad outlines the legacy of *International Shoe*, predicting the outcome of the "minimum contacts" test under a given set of transactions is something of a black art. This will undoubtedly be true for on-line transactions, and indeed, early cases dealing with jurisdiction in the milieu of proprietary computer networks demonstrate the difficulty that courts will have extending the indistinct criteria of minimum contacts into an electronic environment.

35. For example, in *Compuserve v. Patterson*[77], the United States Court of Appeals for the Sixth Circuit applied the minimum contacts test to an on-line trademark dispute and found proper jurisdiction where they almost certainly should have found none. The defendant in the *Compuserve* case had contracted with the national computer network Compuserve, which is headquartered in Ohio, to allow distribution of his software on the network.[78] The Compuserve user agreement, which was incorporated by reference into the software distribution contract, provided that the agreement would be governed by Ohio law.[79] The software was distributed from Compuserve's computers located in Ohio, although the majority of sales were to individuals located outside of Ohio. The defendant, however, was physically located in Texas.

36. Patterson subsequently learned that Compuserve was distributing software of its own under a name very similar to that of his product. Patterson contacted Compuserve, alleging that Compuserve's activities infringed his common-law trademarks for his own software, and demanded a monetary settlement of his claims.[80] Compuserve filed suit in federal district court in Ohio, seeking a declaratory judgment that they had not infringed Patterson's trademarks. Patterson moved to dismiss for lack of personal jurisdiction, and the district court, finding insufficient contacts to satisfy due process, granted the motion. The appellate court, however, reversed the dismissal.[81] In a profoundly flawed opinion, the Sixth Circuit found that Patterson's contacts with Ohio were sufficient to satisfy the state's long arm statute and the requirements of due process. The court particularly cited as contacts the presence of a service contract between the two parties, Patterson's communications regarding the alleged infringement, and the state-law foundations of Patterson's common-law trademark claims.[82]

37. However, the purported contacts on which the court relied melt away on closer scrutiny. The linch-pin of the court's analysis, the presence of a contract in the *Compuserve* case was entirely irrelevant to the due process calculation. The appellate court did not find that Patterson had sufficient contacts with Ohio to allow general jurisdiction; they found instead specific jurisdiction. Yet, the cause of action was Patterson's trademark claim against Compuserve, which did *not* in any way arise from either the software distribution or user contracts Patterson signed with Compuserve. The court acknowledged that Patterson's minimal sales in Ohio, taken alone, were not enough to satisfy minimum contacts with the state.[83] The court found jurisdiction proper only because it combined Patterson's Ohio sales with the contract -- even though the contract had nothing to do with the suit.

38. The court also suggested that sending a demand letter to an Ohio resident was a significant contact

on which jurisdiction in Ohio might be based.[84] Jurisdiction based on this type of contact is not unprecedented,[85] and may be appropriate where the threat of litigation arises from a business, such as a contractual agreement, purposefully directed toward a state. But as a general matter, sending a demand letter into a jurisdiction indicates of itself little if any purposeful availment of that jurisdiction's benefits -- and recall that the dispute in this case arose from Compuserve's unilateral activity, not from its relationships or agreements with Patterson. Reliance upon a demand letter itself creates perverse incentives in the litigation process. If such disconnected "contacts" were the basis for jurisdiction, then plaintiffs would surrender jurisdiction any time they notified another party of a dispute. Indeed, a potential plaintiff might lose a significant procedural advantage by notifying another party of a potential dispute, or by attempting to settle a dispute. One might then expect plaintiffs to cease notifying or offering to settle disputes, and rather to engage in preemptive filings of suit in a jurisdiction of the plaintiff's choice. A jurisdictional rule that discourages pre-litigation notification and possible settlements seems ill-considered at best, and hardly in keeping with the Supreme Court's due process jurisprudence.

39. Similarly, the court's reliance on the creation of common-law trademark rights in Ohio is highly questionable.[86] Such rights arise when goods or services are offered in commerce and the source of the goods becomes associated with a distinguishing mark. Given that Patterson had very few sales in Ohio, there is no particular reason to believe that any trademark rights he may have had arose in Ohio. They would presumably arise where software was sold, or where the name of his software was associated with its source of origin, and *not* where Compuserve happened to locate its computers. Because Compuserve is a nationwide network, Patterson's marks potentially might have gained recognition almost anywhere; indeed, under the facts of the case, recognition of the marks appears to have arisen a almost anywhere *besides* Ohio. The court expressly declined to decide whether Patterson might have been amenable to suit in all the jurisdictions where his software was sold or offered for sale, but those are precisely the jurisdictions where his common-law trademark would have arisen.

VII. Jurisdiction in Cyberspace

40. The *Compuserve* case indicates just how difficult jurisdictional analysis may be when computer networks are at issue. However, no matter how perplexing the determination of minimum contacts has been with regard to a proprietary computer system, its application to Internet activity may prove to be even more arcane. The court in *Compuserve v. Patterson* properly declined the question of whether the jurisdiction would be proper wherever the defendant's software happened to land, yet this question is relatively simple in the context of a proprietary system where the subscribers are known to the system owner. By contrast, the Internet is owned by no one, there are no subscription fees, and no reliable records of who is using the network, or of where they may be located. This poses severe problems for a due process analysis based on territorial contacts; anomalous results may be expected because the network's structural indifference to geographic position is incongruous with the fundamental assumptions underlying the *International Shoe* test.

Much of the Supreme Court's jurisprudence in this area appears to contradict the essential nature of the Net. Where jurisdiction from Internet contacts is at issue, physical presence of the defendant within the forum state will likely be the exception rather than the rule -- cybernauts do physically reside somewhere in real space, and if the defendant cybernaut physically resides within the forum, the law seems well settled that its courts can exercise jurisdiction over her. However, given the far-flung nature of the Net, far more defendants will reside outside any given plaintiff's preferred jurisdiction than will reside within it. A significant number of on-line disputes will therefore require an *International Shoe* analysis.[87]

41. Thus, personal jurisdiction over an Internet user will most frequently be premised on the user's contacts with the forum. Given the nature of on-line transactions, those contacts will in many cases be solely Internet-based contacts. As described above, the "minimum contacts" test requires the tribunal to inquire whether the defendant cybernaut has purposefully availed herself of the benefits of the forum state, such that she might reasonably foresee being haled into court there. In particular, pecuniary gain from the forum is assumed to signal that the defendant has "benefitted" in a concrete way from the laws and public services of the forum.

42. However, one must wonder how reliable an indicator pecuniary gain will be as to minimum contacts via Internet. At the present time, the majority of Internet users probably derive no pecuniary benefit from their on-line activity, yet their on-line activity may still give rise to a variety of legal disputes. Personal communications and discussion groups may be breeding grounds for a wide range of constitutional, contractual, and tort claims, but in the course of conduct that leads to the claim, little money changes hands. This situation is of course already changing; there is money to be made in cyberspace, and entrepreneurs are scrambling to claim their share. Clearly, as on-line commerce grows, many businesses will benefit financially from transactions conducted via the network.

43. Yet the business activity these on-line vendors conduct will, for the most part, not be directed toward a particular physical jurisdiction. Businesses will frequently be ignorant of a customer's physical location, and customers equally ignorant of the business'. If the transaction results in shipment of physical goods, then this veil of ignorance may be rent; the goods must end up somewhere. But the unique aspect of Internet commerce is that the Net allows not only negotiation and payment on-line, but also delivery of goods if the goods are digitized information products: software, pictures, movies, music, novels, data, and the like. Information-based services such as systems monitoring, education, data processing, or consulting can also be offered wholly on-line. Payment by credit card may reveal the customers' identity to a business, but not her location, and payment using anonymous "digital cash" is even less traceable.[88]

VIII. Purposeful Availment

44. The network's geographic insensitivity is similarly problematic with regard to Due Process' purposeful availment requirement. As outlined above, cybernauts neither know nor care about the

physical location of the Internet resources they access. In some very broad sense one might argue that an Internet user who accesses remote resources is "purposefully availing" himself of the benefits of the forum in which the resource is located; the laws and public services of that jurisdiction likely help to maintain the physical infrastructure of that resource, protect it from theft and vandalism, and facilitate its continued operation. But the remote user is entirely indifferent, and frequently ignorant, as to which jurisdiction is providing these benefits -- the resource could just as well be in one jurisdiction as another.[89] Thus, it is difficult to assert with a straight face that the remote user has purposefully or knowingly availed himself of *that* particular jurisdiction's benefits.[90]

45. It is similarly difficult to seriously assert that an Internet business should "reasonably anticipate" being hauled into court in a geographical location concerning which it was ignorant, or at least indifferent, with regard to contact. Recall that there is no feasible way within the Internet to screen or block client requests according to geographic location. This would seem to preclude any meaningful chance for an Internet host to avoid contact with a certain jurisdiction. It is not even feasible for on-line businesses to exclude users by geographic location by means of a password. There is no effective means to conduct such screening on-line, since as described above, there is no way within the Internet to verify the response -- in cyberspace, a password indicates *who* you are, not *where* you are. One court, attempting to enforce a geographically-based prohibition on-line, has suggested that passwords to the restricted web site could be given out by postal mail to addresses outside the prohibited region. But since this process is not automated, many of the advantages of using the Internet would be lost, much like forcing telephone carriers to abandon modern software switching and return to "pull and plug" switching by switchboard operators. Moreover, even if a human being gets every request manually, there is no way to coordinate the off-line response with the on-line usage of the password.

46. Such geographic indeterminacy of course works both ways. The process of on-line commerce is for all practical purposes double-blind; neither the purchaser nor the vendor can know precisely where the other is located. Thus, Internet users are unlikely to have an actual awareness of the jurisdictions that their on-line activities might touch. Of course, one might argue, the "reasonably anticipate" standard does not contemplate actual knowledge or anticipation of contacts, but constructive knowledge: even if the actor did not in fact anticipate the contact, he should have.[91] But this is equally problematic; construed this broadly, the criterion of reasonable anticipation becomes a sham, especially on the Internet. Because Internet activity can originate essentially anywhere, the broad form of the anticipation requirement would dictate that users might "reasonably anticipate" defending a lawsuit essentially anywhere.[92]

47. This position in fact appears to be the position of the Minnesota Attorney General's office, that she who ventures into cyberspace takes her chances as to where she may find herself defending a lawsuit. This jurisdictional theory closely resembles the "stream of commerce" theory articulated by a Supreme Court plurality in the *Asahi Metal* decision.[93] Under this analysis, placing goods into the "stream of commerce" would render the manufacturer amenable to suit wherever the

goods came to rest, as participants in a modern economy should be aware that their goods could come to rest almost anywhere.[94] This position may also derive some support from the Supreme Court's companion decisions in *Keeton v. Hustler Magazine, Inc.*[95] and *Calder v. Jones*.[96] In each of these cases, the sale of magazines within a forum state was found to render, respectively, the publisher or editor of the magazine amenable to suit there.

48. But the "stream of commerce" rationale failed to draw a majority in *Asahi*, and its application in many cases will lie at odds with the language of the Supreme Court's other Due Process holdings. The opinion in *World-Wide Volkswagen* flatly rejects a construction of personal jurisdiction that would subject manufacturers of physical products to suit wherever their products should happen to end up.[97] In that decision, the court declined to make automobiles travelling "agents for service of process" on the distributor, rendering him amenable to suit wherever they roamed.[98] Similarly, on the Internet, if amenability to suit travels with a user's packets, then it might be said that the user in effect appoints his data "as agents for service of process."

49. However, the analogy between moving packets and moving automobiles is somewhat obscured by the holding in *Calder v. Jones*. There the plaintiff raised similar arguments, using the World Wide Volkswagen phraseology with regard to the magazines: that they should not be transformed into his agents for service of process.[99] The court rejected that argument, and perhaps one might reason that packets of bits more closely resemble magazines than they do automobiles. But extending the holding of *Calder* or of *Keeton*, to the Internet may simply be taking a good joke too far. The publisher or editor in those cases was unlikely to have actual knowledge that their magazines were sold in, respectively, New Hampshire and California, but the distribution or subscription information was undoubtedly available if needed or requested.[100] The defendants in those cases could, at least in theory have structured their conduct so as to avoid those jurisdictions.

50. On the Internet, however, the fiction of such imputed knowledge is pushed to the point of intellectual bankruptcy. The fundamental principle of the Supreme Court's Due Process jurisprudence has been that the actor must be able to structure his primary conduct so as to avoid liability in a given jurisdiction. The structure of the network is such that there is no meaningful opportunity to avoid contact with a given jurisdiction -- except perhaps to stay off the Internet altogether. This "all or nothing" result in not consonant with the Supreme Court's in personam jurisprudence and almost certainly results from a poor analysis of both the characteristics of the Internet and of the federal functions of Fourteenth Amendment Due Process.

51. Where the jurisdiction of federal courts is concerned, interstate federalism concerns are absent, and the potential ambit of jurisdiction is potentially much greater. It is important to recall that, where authorized, federal courts in federal question cases may consider a defendant's contacts with the nation as a whole. In particular, the consequences of FRCP 4 (k)(2) may be profound as a matter of general jurisdiction. Recall that general jurisdiction is permissible on the basis of contacts unrelated to the cause of action, so long as the defendant has enough unrelated contacts with the

forum to make defending a suit there reasonable. It is quite conceivable that even where specific jurisdiction for on-line activities is lacking in any given district, general jurisdiction may be found with the nation as a whole.[101]

52. Consider, for example, the situation where a dispute arises with regard to some on-line service based outside the United States. The on-line business may lack meaningful or substantial specific jurisdictional contacts with any given portion of the United States. In such a situation, a district court may be allowed to aggregate nationwide contacts. Given the diffuse nature of the Internet, it is quite possible for the business to lack sufficient nationwide contacts related to the claim for jurisdiction to lie. However, the business' unrelated contacts may be substantial -- the Internet may make the business' advertising and service, as well as access to the business, available throughout the United States. Thus, even within the constraints of Fifth Amendment due process, Internet users may be legitimately called to account for federal infractions in unexpected venues.

IX. Confusion in the Courts

53. Unfortunately, the absurdity of the Fourteenth Amendment imputed knowledge fiction vis a vis the Internet has largely escaped the first courts to address the issue in published opinions. Beginning with the decision in *Inset Systems, Inc. v. Instruction Set, Inc.*[102], courts around the United States have begun deciding a series of on-line trademark disputes where the only contact of the defendant with the forum was a site accessible through the World Wide Web. In an opinion devoid of any meaningful due process analysis, the court in *Inset Systems* held that such contact was sufficient to authorize personal jurisdiction over the alleged infringer. According to the *Inset Systems* opinion, because the web site was accessible from Connecticut, the site owner had "purposefully availed" itself of the privilege of doing business in that state.[103] Or course, as of this writing, there are estimated to be approximately half a million web sites on the Internet; if one were to adopt the reasoning of the *Inset Systems* opinion, all half a million web site operators have "purposefully availed" themselves of the privilege of doing business in Connecticut -- even if they have never *heard* of Connecticut.

54. *Inset Systems* has been followed in a subsequent Internet trademark case that reaches similarly unfortunate results, but at least displays the virtue of more considered analysis. In *Maritz v. Cybergold*,[104] the plaintiff in a trademark dispute over the name of an on-line service filed suit in Missouri; the defendant had no contact with Missouri other than the accessibility of its out-of-state web site. In analyzing the defendant's contacts with the state, the court recognized that "the Internet is an entirely new means of information exchange, [and] analogies involving the use of mail and telephone are less than satisfactory . . . ."[105] Ironically, however, the court used an analogy to postal mail to hold that the defendant was transmitting its advertising into Missouri. According the to court:

> [I]f a Missouri resident would mail a letter to CyberGold in California requesting information from CyberGold regarding its service, CyberGold would have the

> option as to whether to mail information to the Missouri resident and would have to take some active measures to respond to the mail. With CyberGold's website, CyberGold automatically and indiscriminately responds to each and every internet user who accesses its website. Through its website, CyberGold has consciously decided to transmit advertising to all Internet users, knowing that such information will be transmitted globally. Thus CyberGold's contacts . . . favor the exercise of personal jurisdiction . . . .[106]

This analysis, of course, is precisely backward: because the network does not permit the user of a website to discriminate by jurisdiction, its contacts with any given jurisdiction are less, rather than more, purposeful.

55. Much of the mischief in this decision stems from the misapplication of the *Calder v. Jones* standard. The court in *Maritz*, in addition to its reliance on the *Inset Systems* decision, looked to a previous decision in *California Software Inc. v. Reliability Research, Inc*.[107], where allegedly libelous statements posted on a computer bulletin board were held sufficient to confer jurisdiction in the forum state where the plaintiff resided.[108] The court in the *California Software* decision had in turn relied upon the rule of *Calder* for the proposition that jurisdiction is proper where the plaintiff in a libel suit resides, because the damage of the intentional tort is felt there.[109] Because trademark infringement is tortious in nature, the court in *Maritz* extended the *Calder* rule to find jurisdiction in the plaintiff's home state, because the effect of the alleged tort was felt there.

56. However, the *Maritz* holding misconceives the standard of *Calder*, especially in an on-line setting.[110] The standard cannot simply be that whenever an intentional tort is alleged, jurisdiction is proper where the plaintiff resides because the harm will be felt there.[111] Rather, the standard of intent alleged must be one, such as for libel, that would encompass the allegations of purposeful direction necessary to satisfy the jurisdictional standard.[112] Thus, the libel standard encompasses the jurisdictional standard, and specific jurisdiction would be proper in an on-line libel suit such as *EDIAS v. BASIS*, where the court relied upon *Calder* and *California Software* to hold that allegedly defamatory statements via web, e-mail, and newsgroup were purposefully directed at the forum where the plaintiff had its principle place of business.[113] But such malicious behavior will not necessarily be present in the majority of commercial torts, such as trademark infringement -- trademark infringement may be negligent, or innocent, or even in good faith.

57. Thus, in *Maritz* and *Inset Systems* there is no reason to believe that the alleged infringer directed any tortious activities at the plaintiff or at the jurisdiction in which the plaintiff resided. To the contrary, the web sites in question were open to the world, and "mere untargeted negligence" is not enough for jurisdiction to lie.[114] This analysis is supported by the analysis in an additional domain name dispute, *Panavision International v. Toeppen*.[115] The dispute in *Panavision* involved domain name "squatting," in which the defendant was purported to have obtained domain name registrations that contained the plaintiff's trademarks, with the sole purpose of selling the

domain names to the plaintiff.[116] The defendant's sole contact with the jurisdiction was again the allegedly infringing web site. In *Panavision*, however, reliance on the *Calder* standard was proper due to the allegation of the plaintiff's "scam."[117] Since this practice was alleged to constitute a sort of commercial blackmail or extortion, the requirement of alleged facts approaching actual malice was satisfied.

58. The proper application of the *Calder* standard in *Panavision* is cold comfort in light of the improper application of the standard in *Maritz* and *Inset Systems*; taken together, the three cases could signal a trend toward indiscriminately applying *Calder*, properly or not. A glimmer of hope is provided by the opinion in yet another trademark dispute, *Bensusan Restaurant Corp. v. King*,[118] in which the court correctly declined to find jurisdiction where the only contact with the jurisdiction was web site accessibility. The court correctly noted that under a due process analysis, the creation of a web site that is accessible world-wide is no indication that the creator had purposefully availed himself of the benefits of a particular forum.[119] The court further held that actual foreseeability that the site might be accessed in the forum is by itself insufficient to satisfy due process.[120]

59. Similar reasoning led the district court in *McDonough v. Fallon McElligott, Inc.*[121] to reject web access as the sole basis for general jurisdiction. The suit involved misappropriation of a photographer's work; defendant moved to dismiss for lack of personal jurisdiction. In response to the plaintiff's allegation that accessibility to the defendant's web site within the forum established general jurisdiction, the court noted:

> Because the Web enables easy world-wide access, allowing computer interaction via the web to supply sufficient contacts to establish jurisdiction would eviscerate the personal jurisdiction requirement as it currently exists; the Court is not willing to take this step. Thus, the fact that Fallon has a Web site used by Californians cannot establish jurisdiction by itself.[122]

Such insightful reasoning by the courts in *Bensusan* and *McDonough* demonstrates that the judiciary is fully capable of correctly applying due process standards to cyberspace; unfortunately the courts prior to the *Bensusan* opinion have failed to do so, and have garnered a string of misguided followers.

X. Conclusion

60. Personal jurisdiction has been a confusing legal issue since at least the advent of the automobile, and jurisdictional quandaries have arisen with successive waves of technology. However, in the case of the Internet, such jurisdictional overreaching may threaten the most important aspects of this new medium. People familiar with the Internet know that one of the network's great benefits is that the average citizen can participate for a relatively small investment. In the past,

communicating with or catering to a national constituency required heavy capital outlays; the Internet makes nationwide communication and commerce accessible to citizens for as little as a few hundred dollars.[123] But the prospect of multijurisdictional liability may very well raise the price of participation beyond the average citizen's reach. Much of the network's democratizing influence may be lost if liability deters all but the most heavily capitalized entrepreneurs from pursuing all but the most highly profitable ventures. The average user simply cannot afford the cost of defending multiple suits in multiple jurisdictions, or of complying with the regulatory requirements of every jurisdiction she might electronically touch.

61. Proper resolution of the scope of state jurisdiction is therefore critical in order to realize the promise of this medium. The first few cases to address the issue suggest that courts may be inclined to overreach the limits of due process in order to exercise jurisdiction in on-line disputes. In particular, the apparent trend toward reliance on the standard of *Calder v. Jones* bodes ill for the prospect of developing an appropriate due process jurisprudence for Internet-related cases; a broad "effects test" is incompatible with the nature of the Net.[124] At the same time, the decision of the District Court in the *Bensusan* case demonstrates that the courts are capable of properly analyzing due process limitations in the context of networked computer communications. Thus, despite the disturbing current trend, there remains substantial reason for optimism regarding the proper exercise of jurisdiction in the Internet's new world without borders.

Footnotes

[**] Assistant Professor of Law, Seton Hall University.

[1] *See* M. Mitchell Waldrop, *Culture Shock on the Networks*, 265 SCIENCE 879, 880 (1994).

[2] *See* ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1995) (striking down federal Communications Decency Act).

[3] GA. CODE ANN. § 16-9-93.1 (1996).

[4] California Senate Bill SB-1533, 1995-1996 Reg. Sess. (Ca. 1995-1996), and S.B. 1034, 1995-1996 Reg. Sess. (Ca. 1996); *see also* Ilana DeBare, *State Trademark Bill Ignites Net Turmoil*, THE SACARAMENTO BEE, March 2, 1996 at F1.

[5] *See* Texas State Bar Advertising Committee, Interpretive Comment on Attorney Internet Advertising, March 6, 1996; Florida Bar News, Ethics Update, Jan. 1, 1996.

[6] *See* Mark Eckenwiler, *States Get Entangled in the Web*, LEGAL TIMES, Jan. 22, 1996 at S35.

[7] *Id*.

[8] *Id*.

[9] *See* Vinton G. Cerf, *Networks*, SCI. AM., Sept 1991 at 72.

[10] *See generally A Close-up of Transmission Control Protocol/Internet Protocol (TCP/IP)*, DATAMATION, Aug. 1, 1988 at 72; ED KROL & PAULA FERGUSON, THE WHOLE INTERNET FOR WINDOWS 95 29-31 (1995).

[11] *See* KROL & FERGUSON, *supra* note 10 at 26.

[12] *See* Nicholas Negroponte, *Products and Services for Computer Networks*, SCI. AM., Sept. 1991 at 106.

[13] *See* KROL & FERGUSON, *supra* note 10 at 17-20.

[14] *See* WILLIAM J. MITCHELL, CITY OF BITS 19 (1996) (discussing telepresence).

[15] KROL & FERGUSON, *supra* note 10 at 33.

[16] *Id*. at 86-92.

[17] *Id*. at 141.

[18] *Id*. at 8.

[19] *See id*. at 37. ("The pieces of a domain-style name . . . may not tell you anything about who maintains the computer corresponding to that address, or even (despite country codes) where that machine is located.") Additionally, the same machine may have many different domain names, and machines displaying the same domain are not necessarily on the same physical network. *Id*.

[20] *See* MITCHELL, *supra* note 14 at 8-9.

[21] *See* KROL & FERGUSON, *supra* note 10 at 37-38.

[22] *See id*. at 37; MITCHELL, *supra* note 14 at 9.

[23] *See* KROL & FERGUSON, *supra* note 10 at 209.

[24] *See* Eckenwiler, *supra* note 6, at 535.

[25] *See* KROL & FERGUSON, *supra* note 10, at 286.

[26] *See* MITCHELL, *supra* note 14, at 9.

[27] *See generally* Martin Hellman, *The Mathematics of Public-Key Cryptography*, SCI. AM., Aug. 1979, at 146; *see also* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

[28] See generally A. Michael Froomkin, Anonymity and its Enmities, 1995 J. ONLINE L. art. 4 <http://warthog.cc.wm.edu/law/publications/jol/froomkin.htm>.

[29] *See* MITCHELL, *supra* note 14, at 9-10.

[30] *See generally* KROL & FERGUSON, *supra* note 10, at 142.

[31] *See* WAYNE R. LAFAVE & AUSTIN W. SCOTT, JR., CRIMINAL LAW § 2.9(d) (2d ed. 1986).

[32] U.S. CONST. art IV, § 2.

[33] *See* UNIFORM CRIMINAL EXTRADITION ACT, 11 U.L.A. § 6 (1974).

[34] *See* WAYNE R. LAFAVE & JEROLD H. ISRAEL, CRIMINAL PROCEDURE § 16.1 (d) (2d ed. 1992).

[35] *Id.* § 16.1(d), 16.2(a). *See also* B.J. George Jr., *Extraterritorial Application of Penal Legislation*, 64 MICH. L. REV. 609, 622-23 (1966); Larry Kramer, Note, *Jurisdiction Over Interstate Felony Murder*, 50 U. CHI. L. REV. 1431, 1437 (1983).

[36] United States v. Thomas, 74 F.3d 701 (6th Cir. 1996).

[37] *Id.* At 709.

[38] *See*LAFAVE & SCOTT, *supra* note 31, § 3.5(b) at 220 (discussing knowledge element in criminal statutes).

[39] 355 U.S. 225 (1957).

[40] *See, e.g.*, United States v. Macuso, 420 F.2d 556 (2d Cir. 1970) (conviction of failure to register as a narcotics offender dismissed under *Lambert*).

[41] *See* LAFAVE & SCOTT, *supra* note 31, § 3.

[42] *Id.* § 5.1(d) at 415.

[43] *See* Hanson v. Denckla, 357 U.S. 235, 250-51 (1958) ("As technological progress has increased the flow of commerce between the states, the need for jurisdiction over nonresidents has undergone a similar increase."); Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476 (1985) ("[I]t is an inescapable fact of modern commercial life that a substantial amount of business is transacted solely by mail and wire communications across state lines, thus obviating the need for physical presence within a state in which business is conducted.")

[44] *See* Burnham v. Superior Court of California, 495 U.S. 604 (1990).

[45] *See* Hess v. Pawloski, 274 U.S. 352 (1927).

[46] *See* Hutchinson v. Chase & Gilbert Inc., 45 F.2d 139 (2d Cir. 1930).

[47] *See, e.g.*, Shaffer v. Heitner, 433 U.S. 186 (1977).

[48] *See* Harris v. Balk, 198 U.S. 215 (1905).

[49] 326 U.S. 310 (1945).

[50] *Id.* at 316.

[51] *See* Hanson v. Denckla, 357 U.S. at 251; World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 293 (1980).

[52] *See* Insurance Corp. of Ireland v. Compangnie des Bauxites de Guinee, 456 U.S. 694, 702-03 n. 10 (1982).

[53] *Id*. At 703.

[54] *See* Helicopteros Nacionales de Columbia, S.A. v. Hall, 466 U.S. 408, 414 n.9 (1984).

[55] *See International Shoe*, 326 U.S. at 318.

[56] *See id*. at 317-18.

[57] *See id*.; Burger King Corp. v. Rudzewicz, 471 U.S. at 473 (1985).

[58] *World-Wide Volkswagen*, 444 U.S. at 297.

[59] *Id*.

[60] *See Burger King*, 471 U.S. at 482.

[61] *See* The Bremen v. Zapata Off-Shore Co., 407 U.S. 1 (1972).

[62] 465 U.S. 783 (1984).

[63] *See, e.g.*, Core-Vent Corp. v. Nobel Industries AB, 11 F.3d 1482, 1486-87 (9th Cir. 1993).

[64] Several courts across the United States have previously recognized this in other contexts. *See, e.g.*, Far West Capital, Inc. v. Towne, 46 F.3d 1071, 1079 (10th Cir. 1995); Southmark Corp. v. Life Investors Inc., 851 F.2d 763, 772 (5th Cir. 1988) (rejecting broad "effects test" for personal jurisdiction); Wallace v. Herron, 778 F.2d 391, 394 (7th Cir. 1985) (same).

[65] 465 U.S. at 789.

[66] 465 U.S. at 790 (*citing* New York Times Co. v. Sullivan, 376 U.S. 254 (1964)).

[67] 465 U.S. at 790.

[68] *Burger King*, 471 U.S. at 477.

[69] *Id*.

[70] Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102, 115 (1987).

[71] *See* Omni Capital Int'l v. Rudolf Wolff & Co., 484 U.S. 97 (1987).

[72] *See* Hayeland v. Jaques, 847 F. Supp. 630 (D.C.Wis 1994).

[73] *See generally* 4 CHARLES A. WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 1067.1 (Supp. 1995).

[74] *Omni Capital*, 484 U.S. at 105.

[75] *See, e.g.*, Mylan Lab Inc. v. Akzo, 2 F.3d 56, 60 (4th Cir. 1993).

[76] *See, e.g.*, Eskofot v. E.I. DuPont de Nemours & Co., 872 F. Supp. 81 (S.D.N.Y. 1995).

[77] 89 F.3d 1257 (6th Cir. 1996).

[78] *Id*. at 1260.

[79] *Id.* at 1260-61.

[80] *Id*. At 1261.

[81] *Id*. at 1260.

[82] *Id*. at 1262-66.

[83] *Id*. at 1265-66.

[84] *Id*. at 1266.

[85] *See, e.g.*, Akro Corp. v. Luker, 45 F.3d 1541 (Fed. Cir. 1995); Nova Biomedical Corp. v. Moller, 629 F.2d 190 (1st Cir. 1980).

[86] *See Compuserve*, 89 F.3d at 1267.

[87] *See* Cynthia L. Counts & C. Amanda Martin, *Libel in Cyberspace: A Framework for Addressing Liability and Jurisdictional Issues in this New Frontier*, 59 ALB. L. REV. 1083, 1117 (1996).

[88] *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J. L. & COM. 395 (1996).

[89] *See* MITCHELL, *supra* note 14, at 117.

[90] *See* Eckenwiler, *supra* note 6.

[91] *See* Lea Brilmayer, *How Contacts Count: Due Process Limitations on State Court Jurisdiction*, 1980 SUP. CT. REV. 77, 92.

[92] *See Worldwide Volkswagen*, 444 U.S. at 296 (rejecting actual foreseeability because of the potential scope of liability).

[93] *See Asahi Metal*, 480 U.S. at 116-17 (Brennan, J., concurring in part). In *Asahi Metal* Justice Brennan articulated a very permissive standard for "purposeful availment" that would hold manufacturers liable in a forum if they were aware that their product was regularly marketed there. *Id*. at 117. Neither this standard nor Justice O'Connor's more restrictive standard for purposeful availment commanded a clear majority.

[94] 480 U.S. at 117.

[95] 465 U.S. 770 (1984).

[96] 465 U.S. 783 (1984).

[97] 444 U.S. at 296.

[98] *Id*.

[99] 465 U.S. at 789.

[100] *See Calder*, 465 U.S. at 783; *Keeton*, 465 U.S. at 789-90. In *Calder v. Jones* particularly, the Court appeared to regard the publication as a sort of poisoned arrow "expressly aimed" at the forum. 465 U.S. at 783.

[101] *But cf.* McDonough v. Fallon McElligott, Inc., 40 U.S.P.Q.2d(BNA) 1826 (S.D. Cal. 1996) (declining to find general jurisdiction solely on the basis of web presence).

[102] 937 F. Supp. 161 (D. Conn. 1996).

[103] *Id.*

[104] 40 U.S.P.Q. 2d (BNA) 1729 (E.D. Mo. 1996).

[105] *Id.* at 1734.

[106] *Id.*

[107] 631 F. Supp. 1356 (C.D. Cal. 1986).

[108] *See* 40 U.S.P.Q. at 1735 (*citing California Software Inc.*, 631 F. Supp. at 1363).

[109] *Id.* at 1361-62 (*citing* Calder v. Jones 465 U.S. 783, 791 (1984)).

[110] *Cf.* Counts & Martin, *supra* note 87, at 1123 (discussing the proper scope of the Calder "effects test" for cyberspace).

[111] Several courts across the United States have previously recognized this in other contexts. *See*, *e.g.*, Far West Capital, Inc. v. Towne, 46 F.3d 1071, 1079 (10th Cir. 1995); Southmark Corp. v. Life Investors, 851 F.2d 763, 772 (5th Cir. 1988) (rejecting broad "effects test" for personal jurisdiction); Wallace v. Herron, 778 F.2d 391, 394 (7th Cir. 1985) (same).

[112] *See supra* notes 65-67 and accompanying text.

[113] 1996 U.S. Dist. LEXIS 18279 (D. Ariz. Nov. 19, 1996).

[114] *See* Calder v. Jones, 465 U.S. at 789.

[115] 938 F. Supp. 616 (C.D. Cal. 1996).

[116] *Id.* at 618.

[117] *Id.* at 622.

[118] 937 F. Supp. 295 (S.D.N.Y. 1996).

[119] *Id.* at 301.

[120] *Id.*

[121] 40 U.S.P.Q.2d (BNA) 1826 (S.D. Cal. 1996).

[122] *Id.* at 1828.

[123] *See* KROL & FERGUSON, *supra* note 10, at 23.

[124] *Accord* Counts & Martin, *supra* note 87, at 1128.