# The Unexceptional Problem of Jurisdiction in Cyberspace

A caveat: I am here today as someone who has thought about jurisdictional issues, although not particularly in the context of cyberspace. My technological expertise is limited to a working knowledge of computers and my *Wired Magazine* subscription. As an outsider to the cyberlaw community, I offer with certain trepidation my conclusion that there is nothing about legal relations over computer networks that in any way challenges our conventional notions about how sovereign authority is allocated in the world.

At least at the outset, I am going to indulge in some analytic sloppiness in talking about "jurisdiction." The question of "jurisdiction" over Internet activity is in fact a series of related questions about civil and criminal judicial jurisdiction and choice of law under U.S., foreign, and international law, as well as questions about domestic and international enforcement of foreign judgments.<sup>1</sup>

Ultimately, I will limit my analysis to the fairly narrow question of how the United States' civil judicial jurisdiction law ("personal jurisdiction") applies to Internet activity. While this is certainly not the only important question to be answered, its resolution is of critical importance to many other questions, particularly those dealing with U.S. choice of law. For the most part, any time an American court is authorized to assert judicial jurisdiction, it will also be constitutionally permitted to apply its own laws to the underlying transaction.<sup>2</sup> This is

<sup>\*</sup>Allan R. Stein is a Professor of Law at Rutgers Law School in Camden, N.J. I am indebted to Perry Dane for his patient help and advice, and Tracy Siebold for her research assistance. I would also like to thank Linda Bosniak, Michael Dorf, Jay Feinman, Tamar Frankel, Richard Hyland, Vic Khanna, Larry Kramer, Michael Livingston, Nancy Moore and Linda Silberman for their helpful suggestions.

<sup>1.</sup> See Henry H. Perritt, Jr., Will the Judgment-Proof Own Cyberspace, 32 INT'L LAW. 1121 (1998). See also Henry H. Perritt, Jr., Jurisdiction in Cyberspace, 41 VILL. L. REV. 1, 9-13 (1996), for a thoughtful parsing of the difference between these discrete questions in the context of claims arising out of Internet activity.

<sup>2.</sup> See Allstate Ins. Co. v. Hague, 449 U.S. 302, 307 (1981) (upholding the right of a court to apply its own law to a claim as long as "the choice of its law is neither arbitrary nor fundamentally unfair"); Shaffer v. Heitner, 433 U.S. 186, 215 (1977) (suggesting that greater defendant connection

invariably true when jurisdiction is based on the underlying activity at issue in the lawsuit, that is, the category of "specific jurisdiction" applies to most cyberspace claims.<sup>3</sup> Thus, if a California court is permitted to assert jurisdiction over a New York defendant who has caused harm in California through the Internet, the court will also be permitted, although certainly not compelled, to apply California law to test the legality of a defendant's conduct.

At the outset, however, I want to paint with a broader brush in thinking about how sovereignty is allocated in the world. I will analyze how territoriality is imbedded in our notions of political sovereignty and how our conceptions of territoriality have accommodated technological change. I also critically evaluate the claim that cyberspace should be treated as a separate legal jurisdiction. Finally, I look at why legal claims arising in "cyberspace" can be sensibly understood within a territorial framework.

### I. Territoriality in Jurisdiction

Legal communities do not need to be organized around geography. Religious communities, for instance, are not bounded by geographic borders, and one can imagine a world in which legal rights were primarily defined aterritorially. That world, however, is not the one that we occupy.

As long as there have been political communities, they have primarily been organized around place. That is not to say that political communities are precisely defined by geography. Obviously the very notion of citizenship connotes a connection with a state not limited by the location of the citizen. For example, a U.S. citizen can live permanently in London, yet still fully participate in and be bound by the choices of the American polity. Nonetheless, her presence in London also unequivocally subjects her activities to British legal norms for any activity that she conducts in the United Kingdom. To be sovereign has largely meant to have authority over a place.<sup>4</sup>

4. See H.L.A. HART, THE CONCEPT OF LAW 24-25 (1994) (characterizing sovereignty as supremacy within a defined geographical territory and independence of other legal systems); accord Perry Dane, Maps of Sovereignty: A Meditation, 12 CARDOZO L. REV. 959, 996-97 (1991) (while

with a forum is required to sustain jurisdiction than to apply forum law). But see Phillips Petroleum Co. v. Shutts, 472 U.S. 797 (1985) (reversing application of forum law to claims of class members unconnected with the forum).

<sup>3.</sup> The term "specific jurisdiction" refers to the authority of a court to assert jurisdiction over a defendant for the limited purpose of adjudicating claims that have some important connection to the forum, in contrast to "general jurisdiction" which refers to the authority to hear all claims against a given defendant regardless of the claim's connection to the forum. See generally Arthur Von Mehren & Donald Trautman, Jurisdiction to Adjudicate: A Suggested Analysis, 79 HARV. L. REV. 1121, 1136-63 (1966). While, as discussed below, some courts have asserted jurisdiction over defendants where the claims were connected to defendants' electronic contacts with the forum, no court has found such contacts sufficient to support jurisdiction over claims unconnected with the forum. See Howard B. Stravitz, Personal Jurisdiction in Cyberspace: Something More is Required on the Electronic Stream of Commerce, 49 S.C. L. REV. 925, 934 n.76 (1998) (suggesting the courts have almost uniformly rejected attempts to assert "general jurisdiction" over defendants by virtue of Internet activity unrelated to plaintiff's claim).

In pre-technological society, this was, perhaps, inevitable. People could not easily communicate across distances, and coercive power to enforce legal rules was limited by the physical location of the law enforcer. For example, the Roman empire could extend no farther than the Roman army could march and maintain effective communication with Rome. Thus, the power of a sovereign to coerce compliance with legal rules by exercising physical dominion over person or property became the central organizing principle of jurisdiction. A state was said to have authority when it had the power to coerce compliance with its laws.<sup>5</sup> In the judicial jurisdictional context, this authority was implemented through service of process, a symbolic arrest of the defendant present in the territory.

### **II. Territoriality and Technological Change**

As people and transactions became more mobile, jurisdictional rules based solely on the current location of the defendant were strained. Courts increasingly had a need to assert authority over persons not currently within their borders, and improvements in communications and transportation rendered travel to a distant judicial forum less onerous than it once had been.<sup>6</sup>

The increase in mobility and communications was accompanied by another fundamental challenge to territoriality: the recognition of the corporate form. To the extent that a state's authority over a person was tested by the power of a state to exercise dominion over the defendant's body or property, corporations posed a problem.<sup>7</sup> The "person" of a corporation could not be located in a place other than, perhaps, the state of incorporation. If another state wanted to assert jurisdiction over the corporation, the most that could be said was that the corporation conducted activities, or owned property in that state. The "person" of the corporation was never present in the sense of being subject to the power of the state.

The principal innovation of jurisdictional doctrine in response to both developments was to look to the location of the relevant acts of the defendant and their effects over time, rather than the location of the defendant's body at the moment

<sup>territorial states do not exhaust the universe of legal community, "[1]egal orders take up space as well as time... [territory] can help draw the boundaries by which a legal community defines itself against other legal orders").
5. Pennoyer v. Neff, 95 U.S. 714 (1878). See generally Geoffrey Hazard, A General Theory</sup> 

<sup>5.</sup> Pennoyer v. Neff, 95 U.S. 714 (1878). See generally Geoffrey Hazard, A General Theory of State-Court Jurisdiction, 1965 SUP. CT. REV. 241, 253-62 for a discussion of the territorialist theories embraced by Pennoyer.

<sup>6.</sup> See generally Joseph Kalo, Jurisdiction as an Evolutionary Process: The Development of Quasi In Rem and In Personam Principles, 1978 DUKE L. J. 1147 (tracing relationship between jurisdictional evolution and economic development).

<sup>7.</sup> See Philip Kurland, The Supreme Court, the Due Process Clause and the In Personam Jurisdiction of State Courts: From Pennoyer to Denckla: A Review, 25 U. CHI. L. REV. 569, 578-86 (1958).

of litigation.<sup>8</sup> Thus, the modern court can assert jurisdiction over, and apply its own laws to, an absent defendant who caused harm within the forum state, either from within or without. This broader sovereign claim may be described as "neoterritorialist." Jurisdiction continued to be tied to place, but was measured by a more complex relationship with the defendant than simply the location of his body.<sup>9</sup>

The transition from territorialist jurisdictional rules based on presence to neoterritorialist ones based on acts and effects expanded the number of states that had legitimate claims on the underlying activity. Indeed, as emphasized by the Supreme Court in the *Burnham v. Superior Court*<sup>10</sup> decision, the expansion of "long-arm" jurisdiction did not come at the expense of cruder territorial authority. While the courts have tinkered with how much a defendant has to affiliate himself with a state before the state may legitimately exercise judicial authority over him, the evolution of jurisdictional doctrine has largely been a process of enlarging the number of states with claims over a given transaction.

## III. The Legal Pluralist Case for an Independent Cyberspace Jurisdiction

A neoterritorialist approach raises some interesting problems in accommodating all of the conflicting sovereign claims on cyberspace activity. Since "local" activity of typing on a computer keyboard can literally have global effects, the courts are going to have to sort out the authority claims of potentially numerous states. Those conflicts I will address in the next section.

The remarkable claim for a separate cyberspace legal regime is not that cyberspace activity is subject to multiple claims of authority, but rather that it requires the abandonment, or at least compromise, of sovereign claims. It calls for "holes" in territorial sovereignty.<sup>11</sup>

<sup>8.</sup> See International Shoe Co. v. Washington, 326 U.S. 310 (1945) (defendant's contacts with forum prior to litigation justify assertion of jurisdiction over it). While used in the choice of law, rather than personal jurisdiction context, such a neoterritorial approach is also evident in the RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (1987) (a state has "jurisdiction to prescribe law with respect to (1) (a) conduct that, wholly or in substantial part, takes place within its territory; (b) the status of persons, or interests in things, present within its territory; (c) conduct outside of its territory that has or is intended to have substantial effect within its territory.").

<sup>9.</sup> The abandonment of "power" as the exclusive test of jurisdiction was facilitated in the United States by the duty of states to enforce out-of-state judgments under the Full Faith and Credit Clause, Article IV, Section 1 of the U.S. Constitution. By virtue of that obligation, a state judgment could be given effect even if the state lacked power over the defendant or her property at the time it exercised jurisdiction.

<sup>10. 495</sup> U.S. 604 (1990) (sustaining constitutionality of assertions of jurisdiction based solely on service of process upon the defendant within the forum).

<sup>11.</sup> See, e.g., David R. Johnson & David G. Post, The Rise of Law on the Global Network, in BORDERS IN CYBERSPACE 13 (Kahin and Nesson eds., 1997): "Many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of cyberspace as a distinct 'place' for purposes of legal analysis and recognizing a legally significant border between cyberspace and the 'real world.'...' Crossing into cyberspace is a meaningful act that would make application of a distinct "law of cyberspace" fair to those who

Advocates of "cyberlaw" envision a judicial recognition of cyberspace as its own legal space, governed by its own legal order. When confronted with a claim arising in cyberspace, courts would defer to the law of cyberspace, much as medieval century courts incorporated and deferred to the "law merchant" in the case of transnational commercial disputes.<sup>12</sup>

Such deference requires the displacement of a state's legal norms. At the end of every digital connection are people, and their bodies would be the normal jurisdictional predicate. States have historically asserted authority when either a defendant committed a wrongful act in its territory, or a plaintiff suffered the consequences there. Thus, in order for there to be a separate jurisdictional zone of cyberspace, the state in which the computer user is present must agree to pull back its own regulatory fabric to make room for another to operate.

Such "holes" are not unprecedented. The Religious Freedom Restoration Act of 1993<sup>13</sup> and the Free Exercise Clause of the U.S. Constitution are prominent examples of the displacement of the sovereign prerogative in recognition of and respect for other legal orders. Indeed, in some sense, conflict of laws represents a choice by the forum-state to put aside its own claims of legislative authority in deference to another regulatory regime.

Legal pluralists see this accommodation not simply as a preference for freedom over state authority, but as an inevitable concession by states that they do not hold a monopoly on authority nor the ability to create legal meaning. They share that sovereignty with other norm-generating groups that exist within their territory.<sup>14</sup> Harold Laski viewed this concession as an act of self-preservation. In order to maintain its legitimacy, the state must take account of and accommodate other legal communities in which state citizens participate:

We have nowhere the assurance that any rule of conduct can be enforced. For that rule will depend for its validity upon the opinion of the members of the State, and they belong to other groups to which such rule may be obnoxious. If for, example, Parliament chose to enact that no Englishman should be a Roman Catholic, it would certainly fail to carry the statute into effect. We have, therefore, to find the true meaning of sovereignty not in the coercive power possessed by its instrument, but in the fused good-will for which it stands.<sup>15</sup>

pass over the electronic boundary. Cf. Joel R. Reidenberg, Governing Networks and Rule-Making in Cyberspace, in BORDERS IN CYBERSPACE, supra, at 88 ('inetwork communities also develop distinct sovereign powers. Infrastructure organizations acquire attributes of traditional territorial sovereigns'').

<sup>12.</sup> See Johnson & Post, supra note 11, at 22-34. For a critique of the law-merchant analogy, see Jack Goldsmith & Lawrence Lessig, Grounding the Virtual Magistrate (visited Oct. 7, 1998) < http://www.law.vill.edu/ncair/disres/groundvm.html >, arguing that recognition of law merchant was facilitated by a broader acceptance of natural and common law. Goldsmith and Lessig assert that a modern consensus of legal positivism, the premise that law is produced by a sovereign, makes the proposed acceptance of a sovereign less "cyberlaw" impossible.

<sup>13. 42</sup> U.S.C.A. § 2000bb (West. Supp. 1998). The statute was held unconstitutional on grounds not relevant here in City of Bourne v. Flores, 117 S. Ct. 2157 (1997).

<sup>14.</sup> See Robert M. Cover, Nomos and Narrative, 97 HARV. L. REV. 4 (1983).

<sup>15.</sup> See Harold J. Laski, Studies in the Problem of Sovereignty 12 (1968).

Thus, we cannot summarily dismiss the possibility of a community of Internet users laying claim to a certain degree of legal autonomy from territorial sovereignty, much as an Indian Tribe or religious community might.<sup>16</sup> States do, and sometimes must, make room for other legal orders to operate within their territorial sovereignty.

Can cyberspace claim such a status? Advocates for cyberlaw perceive geographical boundaries as inapposite and archaic.<sup>17</sup> "Netizens" are engaged in a global activity in which the location of hardware or even people seems unimportant. The vocabulary of the Internet consistently implies the negation of the molecular world. Users "visit" websites without getting on a plane or clearing customs. Internet identities are disembodied, with no necessary relationship to participant's bodies. People enter chat "rooms" that have no physical location and participate in discussions that defy both time and space.<sup>18</sup> The very phrase "cyberspace"<sup>19</sup> suggests the displacement of the molecular world. Indeed, cyberspace evokes a sense that the real activity is not occurring in physical space, but in some ethereal fifth dimension.<sup>20</sup>

Cyberspace does render place less important in many respects.<sup>21</sup> The relations formed from Internet communication are largely nongeographic. Communications on the Internet are between people of uncertain location and identity. An e-mail can be sent and read from anywhere on the planet. A browser cannot determine the physical location of a web site that it accesses, and a website does not ascertain the physical location of a browser accessing it.<sup>22</sup> The "site" itself

VOL. 32, NO. 4

<sup>16.</sup> See Dane, supra note 4, at 959.

<sup>17.</sup> See, e.g., Johnson & Post, supra note 11, at 10-11 ("Because events on the Net occur everywhere but nowhere in particular . . . no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws."); Reidenberg, supra note 11, at 85-86 ("transnational information flows on the [global information infrastructure] undermine theses foundational borders and erode state sovereignty over regulatory policy and enforcement"); William S. Byassee, Jurisdiction of Cyberspace; Applying Real World Precedent to the Virtual Community, 30 WAKE FOREST L. REV. 197, 199 (1995) ("[a]ctivity in cyberspace . . . creates new relationships among individuals that differ from their analogues in the more usual, physical existence . . . In a very relevant sense, cyberspace is a new, and separate jurisdiction."); HOWAKD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTER (1993).

<sup>18.</sup> See WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE AND THE INFOBAHN (1995) for a discussion of the numerous ways in which cyberspace transforms human relations.

<sup>19.</sup> The term "cyberspace" is generally credited to science fiction author William Gibson in his novel Neuromancer. See RHEINGOLD, supra note 17.

<sup>20.</sup> Cf. Johnson & Post, supra note 11, at 13:

Because events on the Net occur everywhere but nowhere in particular, are engaged in by online personae who are both "real" (possessing reputations and capable of performing services and deploying intellectual assets) and "intangible" (not necessarily or traceably tied to any particular person in the physical sense), and concern "things" (messages, databases, standing relationships) that are not necessarily separated from one another by any physical boundaries, no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws.

<sup>21.</sup> See generally MITCHELL, supra note 18.

<sup>22.</sup> See Johnson & Post, supra note 11, at 6-7.

is not a place, but simply text and programming code served up on demand from a computer. The code may be located on a server in a location unknown to the author of the page who has leased Internet access from a commercial provider that maintains hardware in numerous locations. Internet communications are routed to, from, and through places largely unknown and irrelevant to the users. For the most part, place in cyberspace has been reduced to a mere metaphor.

So, it is quite appropriate to ask whether place has been rendered similarly irrelevant as a political organizing principle, at least as to activities conducted over the Internet. For two reasons, my answer is that it has not. As I will argue in the next section, in spite of all of its space-defying qualities, claims arising on the Internet are susceptible to a fairly coherent resolution under existing jurisdictional doctrine.

Moreover, whether or not the Internet is a community, or a series of communities for some purposes,<sup>23</sup> it is not a political community. It is not the sort of community that creates legal norms, that sovereigns make space for, or that people fight wars of liberation over.<sup>24</sup> States are pressed to accommodate the autonomy of some nonterritorial communities because those groups are sovereign in a significant respect—they generate a legal order by which their members live.<sup>25</sup> Such a claim cannot credibly be maintained for users of the Internet. Unlike religious communities, there is little other than a wire that binds all of its participants. There is no shared authority, ideology, history, or even culture. People log on to shop, entertain, communicate, research, or rant. It connects fascists and libertarians, Barbie fans and Barney haters, porn lovers and nuclear physicists. The vastness and diversity of the Internet belies its characterization as a polity. It evokes the universe of telephone users, not the Nation of Islam.

Advocates of cyberlaw cite the comity that states accord other states in occasionally applying foreign law in its own courts.<sup>26</sup> Thus, they imagine a state deferring

<sup>23.</sup> Howard Rheingold, in particular, has written extensively about the virtual communities formed over computer networks. RHEINGOLD, *supra* note 17. Accord Byassee, *supra* note 17, at 200-03 (arguing that interest groups formed over the Internet constitute virtual communities); Dan Burk, *Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermarks*, 1 RICH. J. L. & TECH. 1, 6 (1995) ('' cybernauts' who traverse this digital landscape find that virtual relationships with other electronic pilgrims blossom into collaboration, friendship, and even romance. Virtual communities coalesce from all corners of the globe to exchange information and reinforce shared values.'').

<sup>24.</sup> Advocates of "legal pluralism," the view that territorial states do not exhaust the universe of law-making communities, recognize that not all assemblages have what Perry Dane has described as "juridical dignity": sufficient sovereign integrity to command respect from territorial states. Dane suggests some non-exhaustive criteria for determining that status: members of the group are committed to its legal authority; the group follows a distinctive legal order differentiated from the rest of the world; the group follows a general legal order, not simply a single rule; the group historically has had a juridical identity; and the group is bounded by borders, usually geographic—"boundaries by which a legal community defines itself against other legal orders." Dane, *supra* note 4, at 992-98. Cyberspace would appear to fall short of a polity under every criterion.

<sup>25.</sup> See supra note 24 and accompanying text.

<sup>26.</sup> Johnson & Post, supra note 11, at 25.

to the law of the Internet, much as an American court might defer to French law in adjudicating a tort committed in France.<sup>27</sup> But comity precisely captures the quality absent in cyberspace; the sense of a state's encounter with another's legitimate authority. It is the sense of sovereign courtesy that the King of France accords the King of England.<sup>28</sup> It is the pragmatic recognition by the state that its population is occasionally bound by the authority of other institutions.<sup>29</sup> Whatever connections the Internet facilitates among its users, it has no claim of authority over them. Whatever difficulties territorial states have in regulating elusive Internet behavior, there is no Internet sovereignty with which they must reckon.

This is probably more true now than it was even a few years ago. The early users of the Internet (a.k.a. "geeks") arguably did (and may still) regard it as a semi-sovereign community. The rhetoric of that era is replete with references to the "anarchy" of the Internet and its freedom from governmental control,<sup>30</sup> "netiquitte," and the responsibilities of Internet users to comply with the self-imposed norms of proper behavior.<sup>31</sup> Few would dispute that this utopian, pioneering spirit has given way to a more mainstream integration of the Internet into the broader economy and culture. Microsoft and Netscape are not "netizens."

Hal Abelson, Professor of Computer Science at the MIT Media Lab, compares the concept of cyberspace to early television audience's belief in a place called "TV Land." Just as the public came to appreciate that there was no such place as "TV Land," our understanding of cyberspace as a discrete place, separate from the molecular world, will eventually give way to a more sophisticated understanding of the Internet as an extension of the broader culture and economy.

It's not a different place anymore. It's our place... People used to talk in the '50's about the folks out there in 'TV Land.' All right, there's no TV Land, and there's no Cyberspace. There's just the real world... Can you remember back all the way, gosh, two years ago when people thought you weren't supposed to put any advertising on the network? And now that's just so taken for granted, you don't even question that.<sup>32</sup>

29. See LASKI, supra note 15, at 12.

VOL. 32, NO. 4

<sup>27.</sup> Id.

<sup>28.</sup> I don't mean to suggest that such "courtesy" is limited to relations between territorial sovereigns. Comity connotes respect and cooperation with another authority, perhaps partly out of concern for reciprocal respect in the future. Such a concern is equally valid in regard to non-state authorities. Perry Dane posits that such respect is not simply to reinforce the legitimacy of territorial authorities, but "is also an act of self-definition, and even self-legitimation . . . [for example] [w]hen the United States recognizes some autonomy for religious communities, it confirms the logic and limits of its own identity as a secular state." Dane, *supra* note 4, at 986-87.

<sup>30.</sup> See, e.g., RHEINGOLD, supra note 17, at 7-8.

<sup>31.</sup> See, e.g., BRENDON P. KEHOE, ZEN AND THE ART OF THE INTERNET (1993). This early primer on Internet basics devotes almost as much space to being a good "net.citizen" as it does laying out technical information. Some of Kehoe's rules include: "Being a good net.citizen includes being involved in the continuing growth and evolution of the Usenet system;" limit your e-mail signature to 4 lines; don't post personal messages to a newsgroup; and avoid inciting flame wars by intemperate comments. *Id.* at 32-39. *Cf.* Burk, *supra* note 23 (discussing communities formed by "electronic pilgrims").

<sup>32.</sup> National Public Radio: Morning Edition (Radio Broadcast, April 2, 1996. Transcript #1837-7).

There is a related transformation in the way we experience the Internet, which may also account for some initial perceptions that cyberspace is a "place" distinct from the molecular world, due its own legal order. The tired metaphors of "surfing the web" and "visiting a web site" at one time reflected the way in which cyberspace captured the human and perhaps legal imagination.<sup>33</sup> The claim for Internet sovereignty makes a lot more sense if cyberspace is experienced as some out-of-body activity instead of as simply viewing information on a computer monitor.<sup>34</sup> Just as the culture of the Internet becomes permeated by real-world culture, the technology of the Internet falls into place as yet another source of information in the real world. As we master and understand the technology, we demystify it. We experience it as a medium, not as a place.

Advocates of cyberlaw insist that the Internet is, or has the potential to become, a functional political community.<sup>35</sup> They point to the emergence of various non-governmental rules and standards on the Internet, such as America Online's privacy policy, Counsel Connect's copyright rules, Microsoft's Web-rating system, as well as availability of the "Virtual Magistrate," an on-line dispute arbitration service.<sup>36</sup>

But such examples are inapposite. When Internet service providers, such as CompuServe or America Online, draft and enforces rules of Internet behavior, they are engaged in the kind of private ordering that governments encourage and facilitate every day. Such rules are produced not by a political community, but by private actors contracting under the authority of existing legal regimes.<sup>37</sup> As

I look back on those reactions with the embarrassment similar to that felt by someone who thought there were people inside the first radios. Today, when I log onto a foreign webpage, I experience it simply as accessing information authored (perhaps) by someone abroad. I may have some residual sense of making an electronic connection with a computer located in another country (where the server may or may not be located), but the content now is far more important to me than the medium. The experience is far more akin to reading a foreign magazine than exploring a distant place.

34. Cf. A. Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U. PA. L. REV. 709, 860-79 (1995) (discussing power of metaphor in shaping legal attitudes toward data encryption).

35. See, e.g., Johnson & Post, supra note 11, at 22 ("Experience suggests that the community of online users and service providers is up to the task of developing a self-governance system.").

<sup>33.</sup> I suspect my own experience is not unique. When I first invoked a hyperlink on a webpage, I experienced a rush of excitement, as though I was passing through some space/time portal. The metaphor of "surfing" seemed apt; as I jumped from site to site with the click of the mouse, I could almost hear the "woosh." Similarly, the first time I connected with an offshore webpage, I experienced amazement tinged with a touch of the anxiety I felt as a child playing with the telephone that perhaps I had inadvertently dialed Japan. I *really* felt as though in some sense I was present in another country. The metaphor of "visiting" a web page did not seem a stretch at all.

<sup>36.</sup> Reidenberg, supra note 11, at 90-91.

<sup>37.</sup> See Morris R. Cohen, The Basis of Contract, 46 HARV. L. REV. 553, 586 (1933). The law of contract, then, through judges, sheriffs, or marshals puts the sovereign power of the state at the disposal of one party to be exercised over the other party. It thus grants a limited sovereignty to the former . . . [T]he ability to use the forces of the state to collect damages is still a real sovereign power and the one against whom it can be exercised is in that respect literally a subject. From this point of view, the

Professor Jack Goldsmith has pointed out, private contract will help to order some behavior in cyberspace, but it will not obviate the need to sort out territorial regulatory claims.<sup>38</sup> Unlike the law of sovereigns, the scope of such private ordering is limited to persons who have consented to the particular rules in question. Even as to them, enforcement is dependent on a state authority that will hold them to their promises. CompuServe depends on territorial sovereigns to enforce their service agreements; there is no other Internet authority or community to give effect to their contracts.<sup>39</sup> Similarly, cybercourts simply represent private arbitration agreements. Their only authority is derived from the authority of governmental courts that will enforce their decrees, much as they might enforce any other contractual provision. Not only will this type of private ordering not fill a jurisdictional void, its effective operation is completely dependent on the power and authority of a state. We are left with the same thorny conflict of laws question of which state has authority over Internet actors and which kind of contracts should be enforced.

Similar to private contractual ordering is the rule-making that occasionally emerges from some cyberspace groups to redress group-specific conduct. For instance, a player in a Multi-User Dungeons (MUD) role-playing game may have its character "act" violently toward other characters.<sup>40</sup> While the group may have practical problems enforcing norms against such behavior,<sup>41</sup> there is apparently enough cohesion among the community of players to generate norms prohibiting such behavior.<sup>42</sup>

It is easy to overstate the significance of such rule-making. First, the domain of the community is limited to the particular MUD or discussion group; the norms generated by the group do not represent the law of the Internet. Second, the norms are not legal rules; they do not order people's behavior in any manner outside the game and do not conflict with any legal order established by a territorial sovereign. No one claims that the National Football League is a polity because

42. See id. at 217-18.

law of contract may be viewed as a subsidiary branch of public law, as a body of rules according to which the sovereign power of the state will be exercised as between the parties to a more or less voluntary transaction.

<sup>38.</sup> See Jack L. Goldsmith, Against Cyberanarchy, 65 U. CHI. L. REV. 1199 (1998). In particular, Goldsmith argues that private ordering cannot provide "mandatory rules" that people do not contract over, such as contractual capacity and tort and statutory duties. *Id*.

<sup>39.</sup> See, e.g., CompuServe Inc. v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997) (upholding CompuServe's right to eject spammers under its service contract).

<sup>40.</sup> See, e.g., Julian Dibell, A Rape in Cyberspace, THE VILLAGE VOICE, Dec. 21, 1993, at 36; Josh Quittner, Johnny Manhattan Meets the Furry Muckers, WIRED MAGAZINE, Mar. 1994. Byassee, supra note 17, at 217-18.

<sup>41.</sup> While the system operator of the game may bar the offending player from logging on, it is currently relatively easy to circumvent such "banishment" by logging in under a new identity. *Id.* at n.103 (noting that in one case of banishment for "virtual rape" the offending party was able to re-register under a different name).

it generates rules concerning pass interference. The question is whether such groups can ever have, in Perry Dane's phrase, juridical dignity. Would a sovereign ever recognize and defer to the group rule in lieu of its own law? Imagine a discussion group norm of toleration and free expression in the face of solicitations of child pornography. Would a court ever defer to the group norm of toleration and dismiss a criminal prosecution?

Perhaps the most intriguing evidence of capacity for self-governance is the recent initiative to privatize regulation and administration of Internet domain names.<sup>43</sup> The Department of Commerce announced in July 1997, plans to shift control over the registration and maintenance of domain names from the federal government to the private sector,<sup>44</sup> and various Internet stakeholders have been attempting to reach consensus on the structure of a private, not-for-profit corporation that would oversee and set policy for domain name registration.<sup>45</sup>

Under the government plan, as outlined in a June 1998 White Paper, the new oversight board would have responsibility for: 1) setting policy for allocation of IP numbers; 2) overseeing operation of the authoritative Internet root server system (the master table which assigns domain names to IP numbers); 3) deciding whether new top level domain names should be added to the system; and 4) coordinating "the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet."<sup>46</sup>

Whether or not the efforts are ultimately successful, the new organization will bring no more legal order to Internet activity than does current government oversight. The primary, and arguably exclusive, function of the organization will be to maintain connectivity, not to regulate Internet activity or content.<sup>47</sup> Thus most, if not all, of the legal norms at stake in current litigation will be unaffected. Indeed, the one "substantive" right potentially affected by domain name registration—claims by registered trademark owners that their marks have been illegally

<sup>43.</sup> Domain names makes it possible to access an Internet address by a familiar name (www. coke.com) rather than by entering a long series of IP address numbers (128.8.114.43). The IP address is obtained by looking up the domain name in a table provided by Domain Name Servers. This only works if everyone agrees where the master lookup table is kept, and what the rules are for obtaining a listed domain name.

<sup>44.</sup> See Statement of Policy on Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (June 10, 1998) [hereinafter White Paper]. The actual registration and maintenance of high-level domain names was performed up to that point under government contract by Network Solutions, Inc., a private U.S. corporation. *Id.* at 31,742.

<sup>45.</sup> See generally Amy Harmon, We, the People of the Internet, N.Y. TIMES, June 29, 1998, at 81; John Borland, Domain Debate Highlights Net's Growing Pains (visited Oct. 7, 1998) < http:// www.techwebcom/wire/story/domnam/TWB19980831S009>; Kristi Essick, New Domain System Gearing Up (visited Oct. 9, 1998) < http://www.computerworld.com/home/news.nsf/ignet/ 9808252domain>.

<sup>46.</sup> White Paper, 63 Fed. Reg. at 31,749.

<sup>47.</sup> One possible exception may be the potential ability of the organization to reject the registration of offensive domain names.

appropriated as domain names by others—is specifically excluded from the jurisdiction of the new organization.<sup>48</sup>

The debates over domain name registration have been reportedly plagued by questions of who has authority to set Internet policy and what the content of that policy should be.<sup>49</sup> Commercial interests have apparently been pitted against various technical experts.<sup>50</sup> After months of heated discussion, the only consensus that emerged was about the structure of the new organization.<sup>51</sup> Imagine then, the prospect of agreeing on the kind of substantive values at stake in current litigation: intellectual property rights, reputational rights, and norms of decency weighed against various claims of freedom.<sup>52</sup> Imagine further what it would take for a territorial state to put aside its own normative judgment about how those values should be balanced and defer to that law. Even if some organization drafts an "Internet Code," a state would not displace its own law absent, at a minimum, a fairly compelling case for the Code's legitimacy. This is the case for comity that cannot be sustained. It is unimaginable that a state would defer to such a code absent evidence that it was, in fact, the law of the Internet, i.e., that it

49. See Douglas Hayward & John Parry, Internet Domain Name Plan Falters (July 1, 1997) (visited Oct. 9, 1998) <a href="http://www.techweb.com/se/directlink.cgi?WIR1997070105.html">http://www.techweb.com/se/directlink.cgi?WIR1997070105.html</a>; Domain Name Debate Moves to Europe (visited Oct. 19, 1998) <a href="http://www.wired.com/news/news/politics/story/13447.html">http://www.wired.com/news/news/ politics/story/13447.html</a>; Harmon, supra note 45.

50. Id.; John Borland, Domain Debate Highlights Net's Growing Pains (visited Oct. 7, 1998) < http://www.techweb.com/wire/story/domnam/TWB19980831S0009 > .

51. See id.; Kristi Essick, New Domain System Gearing Up (visited Oct. 7, 1998) < http:// www.computerword.com/home/news.nsf/idgnet/9808252domain >.

52. Cf. Elizabeth Wasserman, Magaziner Wags a Finger at Domain Name Forum (visited Oct. 9, 1998) < http://www.thestandard.net/a...\_display/0,1270,1203,1203,00.html > :

[John] Postel [director of the Internet Assigned Numbers Authority] emphasized that he does not want the new entity saddled with any vexing issues other than domain names. "I would not like an organization focusing on domain names to get involved in any of those other issues," he said, listing off such quagmires as tax policy, privacy and content regulation.

Postel appears more realistic than some cyberlaw advocates who fall prey to a libertarian fallacy that the commitment to free flow of information is a universal, transcendent value:

If there is one central principle on which all local authorities within the Net should agree, it must be that territorially local claims to restrict online transactions in ways unrelated to vital and localized interest of a territorial government should be resisted. . . . This central principle . . . makes clear that the need to preserve a free flow of information across the Net is as vital to the interests of the Net as the need to protect local citizens against the impact of unwelcome information may appear to be from the perpective [sic] of a local territorial jurisdiction.

Johnson & Post, *supra* note 11, at 27. While a free flow of information may be vital to the "interests of the Net," there is no basis for asserting that this libertarian value should trump local protective values. In other words, there is no meta-principle that prevents a government or any local authority from considering "vital and localized" its interest in preventing the exposure of its members to objectionable information disseminated over the Internet. More importantly, if a local territorial jurisdiction is thus "misguided," it is unimaginable to suppose they might then put aside their own judgment and defer to the contrary libertarian preference of the "Internet community."

VOL. 32, NO. 4

<sup>48. &</sup>quot;Nothing in the domain name registration agreement or in the operation of the new corporation should limit the rights that can be asserted by a domain name registrant or trademark owner under national laws." White Paper, 63 Fed. Reg. at 31,750.

provided a legal order that Internet users generally followed, and/or that it was promulgated by an organization that exercised legitimate authority.<sup>53</sup> An Internet that maintained a true legal order might command deference, but it would be a radically different institution than exists today.

That is not to say that there will not be international conventions that establish uniform norms among the signatories for such issues as intellectual property protection, Internet gambling,<sup>54</sup> or even the distribution of pornography. Such uniformity would, no doubt, be useful. Uniformity inevitably alleviates conflicts of law. However, such lawmaking would be squarely within existing jurisdictional paradigms—it is lawmaking by territorial sovereigns.

In short, the claim for deference to the norms of the Internet is undermined by the absence of a norm-generating Internet community. Moreover, as I will attempt to demonstrate in the next section, such deference will not be propelled by the difficulty of resolving competing territorial sovereign claims over Internet activity. At least in respect to personal jurisdiction questions arising out of cyberspace controversies, the courts seem capable of applying existing jurisdictional paradigms to resolve jurisdictional conflicts.

# IV. Internet Activity Does Not Challenge Existing Jurisdictional Paradigms: The Example of Civil Judicial Jurisdiction in Cyberspace

The question of personal jurisdiction over cyberspace activity is in one sense far more conventional than legislative jurisdiction, or choice of law. While we can imagine (although barely) that the world community might choose to recognize different, independent legal standards to govern cyberspace activity, such cyber laws would still have to be enforced in conventional courts. There is no Internet judicial authority that can resolve disputes without the consent of the litigants.<sup>55</sup> Thus, while there may be some real conflicts between California law and cyberlaw, there is no comparable conflict between California courts and cybercourts.

On the other hand, on both a practical and conceptual level, resolving personal jurisdiction issues is crucial to our assessment of whether cyberspace challenges existing jurisdictional paradigms. To the extent that our conventional tools work

<sup>53.</sup> Even if an Internet Code did represent the actual legal norms of Internet users, many of the problems currently in litigation involve the real-world consequences of Internet behavior, such as defamation and loss of business profits, including injury to persons that conducted no relevant Internet activity. These people would expect, and be entitled to, the protection of territorial laws regardless of Internet practice.

<sup>54.</sup> Interstate conflicts over Internet gambling should be largely eliminated by a bill outlawing gambling over the Internet recently introduced in Congress. H.R. 4427, 105th Cong. (1997).

<sup>55.</sup> As discussed above, the emergence of "cybercourts" on the Internet does not represent a viable substitute for existing judicial authority; the jurisdiction of such services is limited to the consent of the parties. Accord Perritt, supra note 1, Jurisdiction in Cyberspace at 99. Absent the authority to compel participation by nonconsenting litigants, cybercourts cannot provide an effective dispute resolution function for most controversies. Moreover, given the absence of any central Internet authority, it is hard to imagine how true judicial authority could ever emerge.

for determining the extent of California's judicial authority, we have gone a long way toward settling the extent of California's legislative authority.<sup>56</sup> Does cyberspace confound our sense of how sovereign authority is allocated? The personal jurisdiction cases suggest that it does not.

The Internet is a medium. It connects people in different places. The injuries inflicted over the Internet are inflicted by people on people. In this sense, the Internet is no different from the myriad of ways that people from one place injure people in other places, whether by the movement of dangerous products across borders, the multistate broadcast of defamatory information, or the breach of a contract established over the telephone.<sup>57</sup> Since the replacement of strict territorialism with neoterritorialism, such interstate activity no longer confounds the courts. There is a rich and complex body of law to test the legitimacy of sovereign claims to regulate and redress interstate claims.

The doctrinal challenge posed by cyberspace is that actions in one place can have both intended and unintended consequences all over the globe. There is, in fact, little ability of an Internet user to take advantage of cyberspace without losing control of where actions will have consequences.<sup>58</sup> The contents of a webpage or news-posting can be accessed globally.

Jurisdiction is further complicated by the nature of claims arising out of cyberspace activity. Injuries inflicted electronically will not normally have physical manifestations. While it is conceivable that an Internet communication could damage a specific computer (a computer virus for instance), most of the injuries inflicted in cyberspace, such as intellectual property and defamation claims, are difficult to locate in a particular place. Reputations are deemed to be injured for

<sup>56.</sup> The relationship between choice of law and personal jurisdiction is a complex one, and subject to much debate among conflicts scholars. While it is clear that there is considerable overlap between the power of a state to assert jurisdiction and its decision to apply its own law to the dispute, scholars disagree about which requires greater connection with the forum. Compare, e.g., Linda J. Silberman, Shaffer v. Heitner: The End of An Era, 53 N.Y.U. L. REV. 33, 88 (1978) ("if a court has the power to apply its own law, it should have the power to exercise jurisdiction over the action") (emphasis in original) with Robert Allen Sedler, Judicial Jurisdiction and Choice of Law: The Consequences of Shaffer v. Heitner, 63 IOWA L. REV. 1031, 1033 (1978) (arguing that state should be able to apply its own law whenever there are sufficient contacts with the forum to sustain its jurisdiction). In general, there will be more jurisdictions that might legitimately assert jurisdiction over, than apply its law to, a given case. However, this is largely a function of a state's choice of law doctrine rather than constitutional compulsion. If anything, the Supreme Court appears more tolerant of a particular choice of law than expansive assertions of jurisdiction. See cases listed in note 2, supra.

<sup>57.</sup> Accord Lawrence Lessig, The Zones of Cyberspace, 48 STAN. L. REV. 1403, 1404 (1996): ... the legitimacy of regulation turns upon effects. If the net has an effect on that half of the cybercitizen that is in real space, if it has an effect upon third parties who are only in real space, then the claim of a real space sovereign to regulate it will be as strong as any equivalent atom induced effect.

<sup>58.</sup> Johnson & Post, supra note 11, at 6-7.

judicial jurisdiction purposes wherever defamatory information is disseminated.<sup>59</sup> Intellectual property is deemed to be stolen wherever the misappropriated information is viewed.<sup>60</sup> Both are artificial constructs. Ideas do not occupy physical space, and the law's attempt to so locate them strains existing jurisdictional doctrine, even in the molecular world.<sup>61</sup>

The intersection of these two characteristics, global connectivity inflicting intangible injury, thus creates some difficult, although not intractable, doctrinal challenges.<sup>62</sup> In order to answer the challenge, we must consider the existing jurisdictional framework. I limit my analysis to a small slice of that framework— when are U.S. courts constitutionally permitted to assert jurisdiction over absent defendants? This constitutional standard is both more expansive and more limited than other countries' sense of their own extraterritorial authority.<sup>63</sup> Even in the domestic context, it may be further limited by a given state's choice to not extend their jurisdiction to the outer constitutional limits.<sup>64</sup>

The touchstone of the constitutionality of an assertion of jurisdiction over an out-of-state defendant is whether a defendant has "purposefully availed" himself of the benefits and protections of the forum state.<sup>65</sup> While that language may

62. Interestingly, in one regard these cyber-injuries are less jurisdictionally problematical than many conventional claims. Perhaps coincidentally, both defamation and intellectual property claims have been largely federalized. Thus, unlike parties pursuing claims governed by state law, a plaintiff seeking to redress the typical cyber-injury will get minimal choice of law advantage by "forum shopping." Statutes of limitations may vary, but otherwise, the law is not apt to vary much between forums. While jurisdiction may still be used tactically to secure a relatively convenient or sympathetic forum, such conduct is typically less problematic than forum shopping to secure favorable law.

63. See generally Friedrich Juenger, Judicial Jurisdiction in the United States and in the European Communities: A Comparison, 82 MICH. L. REV. 1195 (1984); Russell J. Weintraub, An Objective Basis for Rejecting Transient Jurisdiction, 22 RUTGERS L.J. 611 (1991).

64. See, e.g., Longines-Wittnauer Watch Co. v. Barnes & Reinecke, Inc., 209 N.E.2d 68, cert. denied, 382 U.S. 905 (1965) (Illinois manufacturer of defective hammer which injured New York resident not subject to jurisdiction under New York long-arm statute since "tortious act" as defined in statute was committed in Illinois).

65. Although not critical to most claims that are apt to arise out of cyberspace activity, there is some unresolved ambiguity in whether the purposeful availment must itself give rise to, or simply be related to, the underlying claim in order to sustain a forum's assertion of "specific jurisdiction" over a defendant. Consider the following case. Defendant extensively solicits business in New York over the Internet, specifically targeting New York consumers. Plaintiff, however, has never seen a computer, and buys defendant's product in New Jersey after seeing it in a store there. It is unclear

<sup>59.</sup> Keeton v. Hustler Magazine, Inc., 465 U.S. 770 (1984). Conflicts doctrine more specifically localizes the governing law. The Restatement of Conflicts provides that the plaintiff's domicile will normally provide the governing law in the case of a multistate defamation. THE RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 150 (1971).

<sup>60.</sup> Vanity Fair Mills, Inc. v. T. Eaton Co., 234 F.2d 633, 639 (2d Cir. 1956), cert. denied, 352 U.S. 871 (1956).

<sup>61.</sup> See, e.g., Calder v. Jones, 465 U.S. 783 (1984); Keeton, 465 U.S. 770 (upholding jurisdiction to redress nationwide defamation of plaintiff on the basis of de minimis contacts by defendant with forum). Judicial difficulty with locating intangible property may have contributed to the Court's rejection of quasi in rem jurisdiction in Shaffer, 433 U.S. 186. See Andreas F. Lowenfeld, In Search of the Intangible: A Comment on Shaffer v. Heitner, 53 N.Y.U. L. REV. 102, 122-24 (1978).

suggest some constitutionally required "exchange" of benefits for burdens, in fact the standard appears to be tied to the premise that a defendant's amenability to jurisdiction must be the product of his own volition. "Purposeful connection" better captures the sense of the cases than "purposeful availment."<sup>66</sup>

In particular, courts have relied on a distinction between "targeted" interstate activity that has an intended consequence in the forum, and "local" activity that may have out-of-state consequences but was not designed to have that effect. To the extent that personal jurisdiction serves to allocate authority between sovereigns, this is a sensible distinction; it allows for exercise of extraterritorial authority only when the forum *ex ante* had a regulatory claim on the underlying conduct differentiated from all other states.<sup>67</sup> Similarly, to the extent that limits on personal jurisdiction are designed to prevent unfair surprise to a defendant, the targeted/ untargeted distinction provides some measure of predictability to jurisdictional rules.

The key Supreme Court guideposts on this question are provided by two cases. In *Worldwide Volkswagen v. Woodson*,<sup>68</sup> a New York car dealership sold an allegedly defective car to New York residents who subsequently moved to Arizona. On their way to Arizona the car was rear-ended in Oklahoma, causing severe injuries to the plaintiffs. The plaintiffs attempted, unsuccessfully, to subject the dealership to jurisdiction in Oklahoma.

66. See Burnham v. Super. Ct. of Cal., 495 U.S. 604, 622-27 (1990) ("benefits" received by defendant from his presence in state do not compensate him for burden of jurisdiction). Accord Allan R. Stein, Styles of Argument and Interstate Federalism in the Law of Personal Jurisdiction, 65 TEX. L. REV. 698, 736 (1987) (criticizing contract-like justification for assertions of personal jurisdiction) [hereinafter Stein, Styles of Argument].

Scholars have debated whether such a test is a consequence of some innate right of individuals to be free from a sovereign's authority without their consent, or whether it is derivative of some principle of intersovereign allocation of authority. Compare Robert D. Brussack, Political Legitimacy and State Court Jurisdiction: A Critique of the Public Law Paradigm, 72 NEB. L. REV. 1082, 1095 (1993) (jurisdiction legitimated by consent of defendant); Linda J. Silberman, Can the State of Minnesota Bind the Nation?: Federal Choice-of-Law Constraints After Allstate Insurance Co. v. Hague, 10 HOFSTRA L. REV. 103, 112-13, 117-19 (individual may not be subjected to authority of state unless he volitionally affiliates himself with it) with Lea Brilmayer, How Contacts Count: Due Process Limitations on State Court Jurisdiction, 1980 SUP. CT. REV. 77, 86 (jurisdictionally significant contacts are those that evidence a state regulatory interest in the underlying cause of action). See Stein, Case Three, supra note 65, at 630-34 (contrasting conceptual underpinnings of different scholars participating in Jurisdiction Symposium). My position, that it is a function of intersovereign allocation of authority, is set forth in Stein, Styles of Argument, supra.

67. See Stein, Styles of Argument, supra note 66, at 749-51.

68. 444 U.S. 286 (1980).

whether defendant will be deemed to have "purposely availed" itself with New York for purposes of plaintiff's claim. *See* Helicopteros Nacionales de Colom. v. Hall, 466 U.S. 408, n.10 (1984) (plaintiff's concession that case must be treated as an assertion of general jurisdiction obviates need to determine whether specific jurisdiction may be asserted over claims that are related to, but do not arise out of defendant's contacts with the forum); Allan R. Stein, *Case Three: Personal Jurisdiction*, 29 New ENG. L. Rev. 627, 629 (noting lack of Supreme Court guidance on what constitutes specific jurisdiction) [hereinafter Stein, *Case Three*].

The Supreme Court held that the mere act of selling a mobile product in New York was insufficient to subject the seller to jurisdiction in the place of injury. Mere foreseeability of injury is insufficient.<sup>69</sup> Rather, the defendant must "purposefully avail" itself of the privilege of conducting business in a forum before it is amenable to jurisdiction.<sup>70</sup> The car dealership was not responsible for, nor did it benefit from, the car's transport to Oklahoma.<sup>71</sup> Defendants must be able to have some level of control over where they are amenable to jurisdiction.<sup>72</sup>

*Volkswagen* is in one sense directly analogous to at least some forms of Internetbased claims. Purely "local" conduct causing remote injury cannot be the predicate for jurisdiction elsewhere unless the defendant sought out the connection with the distant forum. Clearly, the doctrinal action is going to be in assessing whether Internet communications are essentially "local" activities. Is an Internet participant engaged in local activity that has global consequences, or is she an interstate actor who purposefully seeks out global connections?

The problem in resolving that question is that there is no bright line separating "local" from global activity. Actions that have consequences elsewhere could be characterized as either local or global depending on the criteria employed. The control criterion suggested by *Volkswagen* is question-begging. It is true that once the dealership sold the car in New York it lacked any control over where the car would cause injury. But the dealer could have limited, or avoided altogether, its exposure to Oklahoma jurisdiction by limiting the warranty to use in New York, or by not selling such a mobile product. It is not that the dealer lacked any control over where its products caused harm; it simply lacked an effective means of selling cars in New York while controlling the consequences of that act elsewhere. Implicit in the Court's holding is the conclusion that subjecting the dealer to suit in Oklahoma would unreasonably burden the sales activity in New York, an activity that was worth protecting.

An instructive contrast is provided by the Court's less familiar treatment of jurisdiction over intentional torts. In *Calder v. Jones*,<sup>73</sup> a reporter and editor for the *National Enquirer* were subjected to jurisdiction in California for writing and editing a defamatory story about actress Shirley Jones, a California resident. The defendants' only presence in California was unrelated to the story,<sup>74</sup> and they did not benefit from the paper's distribution there. They were as indifferent to where the product ended-up as the dealership in *Volkswagen*. They certainly had no control over where the paper was distributed. The Court, nonetheless,

74. Id. at 785-86.

<sup>69.</sup> Id. at 296-97.

<sup>70.</sup> Id. at 297.

<sup>71.</sup> Id. at 299.

<sup>72.</sup> Id. at 297.

<sup>73. 465</sup> U.S. 783 (1984).

held that defendants had sufficiently affiliated themselves with California by knowingly defaming a California resident in a publication that they knew would be distributed in California.<sup>75</sup>

The logic of *Volkswagen* might have suggested that defendants could claim that their "local" activity of producing a story in Florida had California consequences beyond their control and that subjecting them to jurisdiction in California unreasonably burdened their ability to write in Florida. Instead, the court treated the defendants as interstate actors. That could be because the Court imputed the newspaper's connection with California to the defendants. The courts have similarly imputed jurisdictional contacts of a manufacturer to upstream component-part-makers.<sup>76</sup> But it was also significant that the Court viewed the defendants' behavior as "targeted" on California, as though they had fired a gun in Florida that hit its target in California. Intentional injury to an out-of-state plaintiff cannot reasonably be characterized as "local" behavior; the very purpose of the defendants action was to inflict injury in California. Conversely, there was no legitimate local activity that was burdened by subjecting defendants to California jurisdiction. The focus of defendants' actions on California gave that state authority to regulate California-specific conduct.

Although running a webpage or posting a news message could well be characterized as global, rather than local behavior, courts have generally resisted subjecting defendants to jurisdiction solely on the basis that their communication was accessed from the forum state, even where the plaintiff is a resident of the forum.<sup>77</sup> Just as the Supreme Court was unwilling to burden the sale of automobiles with the responsibility of defending claims wherever the automobile caused injury, most lower courts have been largely unwilling to burden Internet activity with the threat of global jurisdiction.<sup>78</sup>

A review of the Internet jurisdiction cases to date suggests a judicial sensitivity to the contrast between *Volkswagen* and *Calder*. The nature of the claim asserted

quoting Hearst, 1997 WL 97097 at \*1. Accord Weber, 977 F. Supp. at 333.

VOL. 32, NO. 4

<sup>75.</sup> Id. at 790.

<sup>76.</sup> Asahi Metal Indus. Co. v. Super. Ct. of Cal., 480 U.S. 102 (1987) (Brennan, J. concurring) (manufacturer of tire valve purposefully availed itself of California market by selling valves to manufacturer of tires distributed in California); Gray v. Am. Radiator & Standard Sanitary Corp., 176 N.E.2d 760 (1961) (manufacturer of boiler component subject to jurisdiction where boiler was distributed).

<sup>77.</sup> See, e.g., Weber v. Jolly Hotels, 977 F. Supp. 327 (D.N.J. 1997); Hearst Corp. v. Goldberger, 1997 WL 97097 (S.D.N.Y. Feb. 26, 1997); Edberg v. Neogen Corp., 1998 WL 458249 (D. Conn. 1998) (defendant's single sale of product in forum alleged to infringe Connecticut plaintiff's patent did not support jurisdiction, notwithstanding defendant's maintenance of a webpage advertising its products).

<sup>78.</sup> See Scherr v. Abrahams, 1998 WL 299678, \*4 (N.D. Ill. 1998):

District courts do not exercise jurisdiction [on the sole basis of an informational web site] because 'a finding of jurisdiction . . . based on an Internet web site would mean that there would be nationwide (indeed, worldwide) personal jurisdiction over anyone and everyone who establishes an Internet web site. Such nationwide jurisdiction is not consistent with traditional personal jurisdiction case law. . . .'

is critical to the courts' assessment of whether a defendant has, through Internet activity, sufficiently affiliated himself with the forum-state to confer personal jurisdiction. Specifically, the distinction between 'targeted' impact versus unintended consequences on the forum appears to be crucial.<sup>79</sup>

The cases to date fall into three general categories. The most common category appears to be Lanham Act claims to redress defendant's allegedly illegal appropriations of plaintiff protected trademark on a webpage. For instance, in *Bensusan Restaurant Corp. v. King*, a Kansas City nightclub named "The Blue Note" advertised its club on its webpage, and the owner of the New York jazz club of the same name sued in New York to redress its trademark claim.<sup>80</sup> The court denied jurisdiction over the defendant, holding that defendant did not specifically target its conduct toward New York. The mere foreseeability that New Yorkers might access defendant's site did not sufficiently affiliate defendant with New York to satisfy due process.<sup>81</sup> Nor was it significant that defendant knew of, and indeed referred to, the famous New York club on its webpage.<sup>82</sup>

Cases like *Bensusan* directly implicate the tension between *Volkswagen* and *Calder*; defendant's webpage has a foreseeable but nontargeted impact in the forum. Unlike *Volkswagen*, plaintiffs in these cases normally pursue the litigation in their home forum, a far more foreseeable forum than the place of injury in which the *Volkswagen* plaintiffs filed. Unlike the defamation claim asserted in *Calder*, trademark infringement claims do not require proof of intent to harm, or even that defendant knew he was appropriating a protected mark.<sup>83</sup> Most of these courts are unwilling to burden Internet actors with the cost of defending litigation in every forum in which their actions have consequences, and accordingly find *Volkswagen* to be the more compelling precedent.<sup>84</sup>

82. Id. at 297-98.

<sup>79.</sup> See, e.g., Bensusan Restaurant Corp. v. King, 937 F. Supp. 295, 301 (S.D.N.Y. 1996), aff'd, 126 F.3d 25 (2d Cir. 1997); Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 418 (9th Cir. 1997). Accord Stravitz, supra note 3, at 937-38 ("Under Calder knowledge that a plaintiff will suffer maximum and foreseeable harm in the forum state is critical to the jurisdictional calculus . . . The harm must be targeted . . . ").

<sup>80. 937</sup> F. Supp. at 301.

<sup>81.</sup> Id.

<sup>83.</sup> J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 25:1, 25-6 (1996).

<sup>84.</sup> See, e.g., Hearst, 1997 WL 97097 (alleged appropriation of New York plaintiff's protected mark on defendant's web page does not subject defendant to New York jurisdiction); Cybersell, Inc. 130 F.3d at 414 (Florida defendant's infringing use of Arizona plaintiff's mark on its home page does not subject defendant to jurisdiction in Arizona); Bensusan, 937 F. Supp. at 295 (use of New York plaintiff's protected mark on Missouri plaintiff's web page does not subject defendant to jurisdiction in New York); Patriot Systems, Inc. 1998 WL 668625 (D. Utah 1998) (website advertising allegedly infringing software does not subject defendant to jurisdiction in forum). Cf. Transcraft Corp. v. Doonan Trailer Corp., 1997 WL 733905, \*8-10 (N.D. Ill. 1997) (maintenance of webpage that includes picture of infringing product does not subject defendant to personal jurisdiction in forum). For a discussion of the substantive federal trademark implications of Internet activity, see Burk, supra note 23, at 19.

Only where a defendant specifically directs his conduct toward the forum has jurisdiction been consistently sustained. Thus "domain squatters," who reserve commercially familiar domain names in the hope of selling them back to the commercial enterprise, are treated differently than mere trademark infringers.<sup>85</sup> The domain squatter was principally motivated by the impact his action would have on the defendant, thus his behavior is reasonably characterized as "targeted" at the defendant's domicile. In contrast, someone who simply uses a protected mark on his web page is not necessarily attempting to affect the plaintiff, even if his behavior predictably has that effect.<sup>86</sup> He is thus analogous to the dealer in *Volkswagen*.

Some trademark infringement cases have gone the other way, and the appellate courts will need to provide clearer guidance. A minority of courts have upheld jurisdiction in the plaintiff's home forum merely on the basis of defendant's appropriation of plaintiff's mark on a webpage accessible from the forum.<sup>87</sup> Contrary to the conclusion of some commentators,<sup>88</sup> this judicial split does not represent chaos in the law of Internet jurisdiction. This is a fairly narrow, albeit important dispute.

The minority of courts that find jurisdiction are, in my view, simply wrong. A forum is rarely privileged to assert jurisdiction simply because it is the plaintiff's domicile. The Supreme Court has repeatedly emphasized that the critical jurisdictional inquiry is the nature of the defendant's connection with the forum.<sup>89</sup> It is hard to see why the plaintiff's domicile should have greater significance in a trademark infringement case than in any other. Moreover, untargeted national

<sup>85.</sup> See, e.g., Panavision Int'l, L.P. v. Toeppen, 989 F. Supp. 616 (C.D. Cal. 1996) (domain squatter is amenable to jurisdiction in plaintiff's domicile).

<sup>86.</sup> See authorities cited in note 64, supra; Hearst and Bensusan are distinguishable from another New York decision upholding jurisdiction in a trademark infringement action against a Georgia Internet service provider. See Am. Network, Inc. v. Access Am., Inc., 975 F. Supp. 494 (S.D.N.Y. 1997). In American Network, the defendant had successfully solicited six customers for its business and had mailed software to them in New York. The court emphasized that its jurisdictional claim was not justified "simply because its home page could be viewed by users [in New York]." 1d. at 498-99. Cf. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997) (upholding Pennsylvania jurisdiction over California defendant for trademark infringement where defendant contracted with 3000 Pennsylvania customers, including seven Pennsylvania Internet Service Providers to provide Usenet access).

<sup>87.</sup> See Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996) (upholding jurisdiction over Massachusetts defendant that used protected mark in its domain name); Hasbro, Inc. v. Clue Computing, Inc., 994 F. Supp. 34 (D. Mass. 1997) (upholding Massachusetts jurisdiction over Colorado defendant that touted prior business done on behalf of Massachusetts corporation, and used Massachusetts plaintiff's protected mark on its webpage). Cf. Superguide Corp. v. Kegan, 987 F. Supp. 481 (W.D.N.C. 1997) (trademark owner subject to personal jurisdiction in declaratory judgment proceeding on the basis of its maintenance of a webpage accessible to residents of the forum, absent proof that defendant had little actual contact with forum residents).

<sup>88.</sup> See, e.g., Robert W. Hamilton & Gregory A. Castanias, Tangled Web: Personal Jurisdiction and the Internet, 24 LITIG. 27 (1998).

<sup>89.</sup> See Keeton, 465 U.S. 770, 780.

advertising has generally been held insufficient to subject a defendant to jurisdiction in the plaintiff's domicile.<sup>90</sup> Maintenance of a webpage certainly represents no greater purposeful activity toward the forum.

The second category of Internet cases involve breaches of contractual obligations formed as a result of Internet solicitation. Using the targeted/untargeted distinction, the contract cases are easy and consistent. Where a party has allegedly breached a contractual obligation formed through Internet solicitation, the subsequent direct dealings between the parties provides the "targeted behavior," thus mooting the cyber-source of the relationship.<sup>91</sup> While the Courts may, as in the mail-order context, protect the one-time customer from onerous jurisdictional responsibilities,<sup>92</sup> there is nothing special about contracts formed over the Internet.

The targeted/untargeted distinction also accounts for the interest of some courts in whether an actionable webpage is read-only, or is interactive.<sup>93</sup> On one level, such a distinction seems silly and technologically naive. At some level, all webpages are interactive. A web browser sends a wealth of information to virtually every webpage server, including the Internet Protocol address and the server name of the browser.<sup>94</sup> Whether it additionally receives other data from the browser should not, per se, be jurisdictionally significant, notwithstanding cases

92. See Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985) (suggesting that consumers would not be subject to jurisdiction in seller's forum in disputes arising from mail-order purchases, notwithstanding holding that operator of Burger King franchise was subject to jurisdiction in franchisor's home state).

93. See Park Inns Int'l Inc. v. Pacific Plaza Hotels, Inc., 5 F. Supp. 2d 762 (D. Ariz. 1998) (hotel reservations made by Arizona residents through defendant's web page renders page jurisdictionally significant contact with forum); *Hasbro*, 994 F. Supp. at 45 (Interactivity of web site enhances jurisdictional significance, "encouraging and enabling anyone who wishes, including Massachusetts residents, to send e-mail to the company."); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (link on web page allowing browsers to e-mail author, and subscribe to his newsletter, the "Drudge Report," renders web page significant contact with District of Columbia in defamation action brought by White House official).

94. See GEORGE ECKEL, BUILDING A LINUX WEB SERVER 274 (1995). Moreover, even apparently "passive" websites have the capability of collecting additional information about a browser through the use of "cookies," a file placed on the browser's hard drive which identifies the user to the webpage and may record information about the browser's prior contacts with the webpage, including the links that the browser explored. See Chip Bayers, The Promise of One to One, WIRED MAGAZINE, vol. 6.05 at 130, 184 (May, 1998).

<sup>90.</sup> See, e.g., IDS Life Ins. Co. v. SunAmerica, Inc., 958 F. Supp. 1258, 1268 (N.D. Ill. 1997) (nationwide advertising and nontargeted webpage do not constitute jurisdictionally significant contact with Illinois). See generally ROBERT C. CASAD, JURISDICTION IN CIVIL ACTIONS § 74 (2d ed. Supp. 1997).

<sup>91.</sup> See, e.g., Resuscitation Techs., Inc. v. Continental Health Care Corp., 1997 WL 148567 (S.D. Ind. Mar. 24, 1997); cf. Digital Equip. Corp. v. AltaVista Tech., Inc., 960 F. Supp. 456 (D. Mass. 1997) (Massachusetts has jurisdiction over defendant that allegedly breached trademark licensing agreement with Massachusetts plaintiff); CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996); Hall v. LaRonde, 66 Cal. Rptr. 2d 399 (Ct. App. 2d Dist. 1997) (California has personal jurisdiction over New York licensee of software designed by California company).

to the contrary.<sup>95</sup> What is jurisdictionally significant is whether that information puts a defendant on reasonable notice that his conduct will have a consequence in a particular place. Even the exchange of e-mail does not necessarily provide such notice since domain names do not necessarily correspond with geography.<sup>96</sup> On the other hand, if a browser has supplied the webpage with a name and address, it would not be unreasonable to characterize the defendant's conduct as targeted.<sup>97</sup>

A third category of cases involve attempts to enjoin illegal activity that could harm forum residents. For instance in *State v. Granite Gate Resorts, Inc.*,<sup>98</sup> the court upheld jurisdiction over a civil injunction proceeding brought by the Minnesota Attorney General against Nevada defendants that announced an Internet gambling service accessible to Minnesota residents. The complaint alleged that defendant was defrauding Minnesota residents in suggesting that they could legally gamble from home through the defendant's planned Internet casino website. These cases are not necessarily captured by the subsequent negotiations principle articulated above, since judicial intervention may be in anticipation of such contact, and the defendant could operate the casino without knowing the location of the gamblers. While the defendant in *Granite Gate* was charged with an intentional wrong, unlike defamation cases, the defendant's behavior was not targeted at a particular place.

This type of case may be the most problematic. Since there is no way currently to limit webpage access to browsers located in particular geographic locations,<sup>99</sup> the only way to prevent the threatened injury is for the court to enjoin the dangerous conduct globally.<sup>100</sup> Cases like this thus raise the tail-wagging-the-dog specter of a state with a relatively tangential interest in imposing its regulatory norms globally. These are complex questions, but not made particularly more difficult

<sup>95.</sup> See Hasbro, 994 F. Supp. at 34. In Hasbro, the mere capacity of the webpage to receive e-mail was considered important, notwithstanding the absence of evidence that anyone from the forum actually used that feature. But see Scherr v. Abrahams, 1998 WL 299678 (N.D. III. May 29, 1998) (link on webpage allowing browser to send e-mail to defendant does not render website sufficiently interactive to be deemed targeted at Illinois consumers).

<sup>96.</sup> Cf. Johnson & Post, supra note 11, at 6-7.

Accord Zippo, 952 F. Supp. at 1119 (upholding jurisdiction in trademark infringement action where defendant knowingly processed 3000 Pennsylvania subscriptions to its Internet news service).
 98. 568 N.W. 2d 715 (Minn. Ct. App. 1997).

<sup>99.</sup> See Johnson & Post, supra note 11, at 6-7.

<sup>100.</sup> Preventing the kind of fraud alleged in *Granite Gate* would be much easier than enjoining the actual gambling activity. A court could certainly enjoin the out-of-state defendant from suggesting that Minnesota residents could gamble with impunity, and could impose a "void where prohibited by law" disclaimer without stepping on other sovereign's toes. It would be more difficult for a court to enjoin the gambling itself without interfering with the defendant's right to conduct legal gambler. Perhaps a fair accommodation would be to require the casino to obtain addresses from each gambler prior to each gambling session, and then prohibit the casino from dealing with known Minnesota residents.

by the digital medium.<sup>101</sup> The courts have grappled with comparable problems in policing offshore economic behavior that has anticompetitive effects in the United States.<sup>102</sup> In the gambling context, the same conflict would arise if the defendant offered in nationally distributed advertisement to accept wagers by phone or mail. This is not unique to the Internet context.

If there is a hard case out there peculiar to cyberspace, it is the Internet version of *Calder v. Jones.*<sup>103</sup> Suppose a news posting defames a public person<sup>104</sup> (as I am quite confident thousands of news postings do every day). If the author wrote in reckless disregard of the truth, her behavior is actionable under *Sullivan v. New York Times.*<sup>105</sup> Under *Calder*, it might also be considered "targeted behavior," at least if the message is read in the forum state.<sup>106</sup> It is conceivable that the courts will distinguish *Calder* on the ground that the publisher's extensive contacts with the forum were imputed to the reporter in a way that the news reader's activity could not reasonably be imputed to the news poster. But it would not be a gross misreading of the case for courts to conclude that the mere foreseeable injury

104. Private defamation should be easier, at least to the extent that it is based on a negligent misstatement of fact. While such negligent, private-person defamation is distinguishable from *Volkswagen* in that only one person could be the victim of the conduct, I would expect courts to characterize it as "local" behavior having an unintended interstate consequence, thus denying jurisdiction in the plaintiff's state.

105. 376 U.S. 254 (1964).

106. The lower courts' construction of *Calder* is varied. Some courts have required only minimally additional connections with the plaintiff's domicile where the writing has been foreseeably disseminated in the forum; *see*, *e.g.*, Gordy v. Daily News, L.P., 95 F.3d 829 (9th Cir. 1996) (defendants, a New York reporter and newspaper, subject to California jurisdiction for publication of allegedly defamatory statements concerning California domicile notwithstanding existence of less than twenty California subscribers to the Daily News); Sinatra v. Nat'l Enquirer, Inc., 854 F.2d 1191 (9th Cir. 1988) (Swiss clinic subject to California jurisdiction where its employees in Switzerland wrongly told a reporter for a nationally distributed newspaper that plaintiff had been a patient in the clinic and defendant had advertised its clinic in California publications). Others have distinguished *Calder*, and have declined to assert jurisdiction where the defamation in question did not concern events occurring in the forum. *See*, *e.g.*, Reynolds, Jr. v. Int'l Amateur Athletic Fed'n, 23 F.3d 1110, 1120 (6th Cir. 1994) (defendant not subject to jurisdiction in plaintiff's Ohio domicile for issuing press release in England asserting that plaintiff used performance-enhancing drugs since, unlike *Calder*, defamation did not concern activities in Ohio, was not based on Ohio sources, defendant did not circulate the report in Ohio, and plaintiff's career was not ''centered in Ohio.'').

<sup>101.</sup> Accord Goldsmith, supra note 38 (arguing that containing the "spill-over effects" of extraterritorial regulation is the central challenge for modern choice of law doctrine).

<sup>102.</sup> Hartford Fire Ins. Co. v. California, 509 U.S. 764 (1993).

<sup>103.</sup> See. e.g., California Software Inc. v. Reliability Research, Inc., 631 F. Supp. 1356 (C.D. Cal. 1986); Telco Communications v. An Apple A Day, 977 F. Supp. 404 (E.D. Va. 1997) (issuance of press release to third party, who then posted it on the Internet, subjected defendant to jurisdiction in Virginia, where posting was accessible); Edias Software Int'l, L.L.C v. Basis Int'l. Ltd., 947 F. Supp. 413, 420 (D. Ariz. 1996), in which the court asserted jurisdiction over defendant on the basis, inter alia, of defendant's global defamation of plaintiff through e-mail and its webpage; "[plaintiff] allegedly felt the economic effects of the defamatory statements in Arizona." *Id.* However, defendant had numerous other contacts with Arizona.

to the plaintiff's reputation in her domicile provides an adequate justification for asserting jurisdiction over the defendant.<sup>107</sup>

Such a principle is a lot easier to swallow in the molecular world than in the digital one. Outside of the Internet, a defendant has to go pretty far out of her way to disseminate libel beyond her home. She has to dial an out-of-state phone, appear on a broadcast, or mail a letter. On the Internet, simply clicking on the reply icon will disseminate the message globally.<sup>108</sup> A resident of New York or even France<sup>109</sup> could find themselves defending in a California court with frightening ease.<sup>110</sup>

One response, of course, is that this result is the cost of engaging in intentional torts. People who live in cyberspace shouldn't cast aspersions. The problem is that we only know after an adjudication whether the defendant in fact engaged in tortious behavior.<sup>111</sup> The line between constitutionally protected conduct and an intentional tort is arguably more subtle in defamation than in any other context. The availability of summary judgment or a judgment on the pleadings certainly mitigates the problem, <sup>112</sup> but a defendant ultimately exonerated from substantive

109. A foreign defendant may have marginally better protection against such jurisdictional assertions. First, if the defendant does not own assets in the United States, it may be difficult or impossible for the plaintiff to collect on the judgment; there are currently few treaty obligations to enforce United States judgments in other countries. See Perritt, supra note 1. The Supreme Court also suggested in Asahi Metal Indus. Co. v. Super. Ct., 480 U.S. 102, (1987) that the enormous inconvenience to a foreign defendant of litigating in the United States may sometimes render jurisdiction constitutionally invalid even where the defendant has purposefully availed itself of the benefits of the American forum.

110. Accord Counts & Martin, supra note 107, at 1128-1130 (ease of global dissemination of alleged liable makes it inappropriate to permit jurisdiction "in any random state in which a cyberspace message may be read").

111. Where the facts supporting jurisdiction overlap with the facts supporting substantive liability, courts typically defer fact-finding until trial and simply require that plaintiff set forth a prima facie case for jurisdiction at the motion stage. Ultimately, jurisdiction must be supported by a preponderence of evidence. See 5A CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE & PROCE-DURE § 1357 (2d ed. 1990).

112. See Anderson v. Liberty Lobby, Inc., 477 U.S. 242 (1986) (plaintiff has heightened burden in defamation case to establish prima facie case that there is "clear and convincing evidence" that defendant acted with "actual malice").

VOL. 32, NO. 4

<sup>107.</sup> But 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, 1124 (1996) (Calder requires purposeful direction of the libel into the forum, not merely that the effects of the defamation were felt in the forum).

<sup>108.</sup> I'm sure everyone has their favorite unintentional "Reply-To" story. My favorite involved Professor Larry Kramer of N.Y.U. Law School. Professor Kramer was leaving town for vacation, and instructed his e-mail program to reply to all e-mails with the message that he would be back in the office in January. Unfortunately, he forgot that he was a subscriber to the Federal Courts and Civil Procedure e-mail discussion groups. Every time someone posted a message to those groups, Kramer's e-mail responded. When his automatic response was received by the discussion group server, he was automatically sent a copy of his own automated response, thus creating an infinite loop. Several hundred law professors were slammed with thousands of messages from Kramer announcing that he would be back in the office in January. It took every ounce of maturity I could muster to resist posting a question to the groups asking if anyone knew when Professor Kramer would be back in the office.

liability could still incur substantial jurisdictional liability. Such a prospect could well chill robust debate on the Internet, where potential defendants would typically lack the resources to defend out-of-state litigation. Because of a possible chilling effect, the courts briefly experimented with subjecting libel claims to more exacting jurisdictional standards than other torts,<sup>113</sup> but ultimately abandoned that approach in *Calder v. Jones*.<sup>114</sup>

Assuming the courts are not prepared to revisit that approach, there is still room to read *Calder* narrowly and reject the proposition that a defamation plaintiff's domicile has an automatic claim of authority over a defendant. Such a resolution would be consistent with the Lanham Act cases, most of which do not heavily weigh the domicile of the infringed plaintiff in deciding jurisdiction. At the most, however, the Internet defamation cases simply require some fine tuning and sensitivity to context, not any fundamental paradigm shift.

In short, while not a model of clarity, the personal jurisdiction cases to date suggest the courts are well on their way to working out a more-or-less coherent approach to the allocation of judicial authority over cyberspace controversies. As courts become more familiar with the technology, we can expect more sophisticated refinements. This suggests that the new technology of cyberspace does not, in general, confound our basic jurisdictional instincts.

### V. Conclusion

The title of this article is quite deliberate. Jurisdiction in cyberspace is not unproblematic. My point is that it is not uniquely problematic. The world is increasingly a complicated place and sorting out the regulatory claims of competing sovereigns has never been easy business. The Internet geometrically multiplies the number of transactions that implicate more than one state. But it is a problem of quantity, not quality. The cases to date suggest some workable standards by which to measure jurisdiction. As of yet, there is not true consistency in the decisions, but that is nothing new for the law of jurisdiction.

<sup>113.</sup> See, e.g., Curtis Pubg. Co. v. Birdsong, 360 F.2d 344 (5th Cir. 1966).

<sup>114.</sup> See Calder, 465 U.S. at 790-91.

13. Publication Ti	Ge	14. Issue Date for Circulation Data Be	iow .
Internati	onal Lawyer	Summer 98 32/2	
5.	Extent and Nature of Circulation	Average No. Copies Each Lasue During Preceding 12 Months	Actual No. Copies of Bingle Iss Published Nearest to Filing De
a. Total Number	of Copies (Net press run)	15,957	15,651
b. Paid and/or Recuested	(1) Sales Through Dealers and Carriers, Street Vendors, and Counter Sales (Not mailed)	-0-	-0-
Circutation	(2) Paid or Requested Mail Subscriptions (Include advertise's proof copies and exchange copies)	13,217	12,986
c. Total Paid and (Sum of 15b)	In Requested Circulation	13,217	12,986
d. Free Distribution (Samples, con	on by Mall splimentary, and other tree)	1,329	1,318
e. Free Distributio	on Outside the Mell (Carriers or other meane)	-0-	-0-
. Total Free Distr	ibution (Sum of 15d and 15e)	1,329	1,318
g. Total Distributio	an (Sum of 18c and 150)	14,546	14,304
h. Copies not	(1) Office Use, Leftovers, Spoled	1,411	1,347
Distributed	(2) Returns from News Agents	-0~	-0-
. Total (Sum of 1	\$9, 16h(1), and 15h(2))	15,957	15,651
Percent Paid and (15c / 15g x 100)	for Requested Circulation	902	90%
6 Publication of a Publication	Statement of Ownership required. W3 be printed in the	issue of this publication.	·
	Title of Editor, Publisher, Bustrette Manager, or Owner		Cate

Ronald Kadlec, Hanager, Hail Service R Maller 9.28.48 ading information on this form

I certify their all information furnished on this torm is true and complete. Londerstand that anyone who furnishes fattes or mis or who omits material or information requested on the torm may be subject to criminal sanctore (including lines and imprise (including includes changes and only provides).

Instructions to Publishers

Complete and the one copy of this form with your postmaster annually on or before October 1. Keep a copy of the completed form for your records.

 Be sure to furnish all circulation information called for in item 15. Free circulation must be shown in items 15d, e, and f. 4. If the publication had second-case authorization as a general or requester publication, this Statement of Ownership, Management, and Circulation must be published; it must be privated in any issue in October or, if the publication is not published during October, the first laws private later October.

5. In item 18, indicate the date of the issue in which this Statement of Ownership will be published.

6. Item 17 must be signed.

Failure to file or publish a state ment of ownership may lead to suspension of second-class authorization.

P8 Form 3525, September 1995 (Reverse)

1. Publication Title	2. Pi	otes	ton	Non	ber	_			3. Pling Date
International Lawyer (ISSN: 0020-7810)		5	8	ı	-	8	6	0	10-1-98
4. Issue Frequency	5. N	mbe		-	P.d	deh	nd A	munity	5. Annuel Subscription Price
Quarterly		For	ur						\$12.00
7. Complete Malling Address of Known Office of Publication (Not printer)	(Street, cl	ty: co	anny.	stite	, and	5 ZV	ψđ)		Contect Person Ronald Kadlec
750 N. Lake Shore Drive, Chicago, IL 6061	1-4497								(312)988-6304

### 9. Full Names and Complete Maching Addresses of Publisher, Ector, and Managing Editor (Do not leave blank) Evolution (Name and complete micros address)

American Bar Association, 750 N. Lake Shore Drive, Chicago, IL 60611-4497

#### Editor (Name and complete mating address)

Peter Winship, Southern Methodist University, School of Law, Dallas TX 73275

Monaging Editor (Name and complete mating address)

### Norman Gross, 750 N. Lake Shore Drive, Chicago, IL 60611-4497

ull Name	Complete Molting Address
American Bar Association	750 N. Lake Shore Drive
	Chicago, 1L 60611-4497
Known Bondhatien, Mongagess, and Other Becurity Hold Holding 1 Percent or More of Total Amount of Bonds, More Other Securities. It Anno. Hore box	Nris Overing er pages, or 
Holding 1 Percent or More of Total Amount of Bonds, Morts Other Securities, It none, check box	Piges, of
Holding 1 Percent or More of Total Amount of Bonds, Morts Other Securities, It none, check box	project, or thome
Holding 1 Percent or More of Total Amount of Bonds, Morts Other Securities, It none, check box	project, or thome
Holding 1 Percent or More of Total Amount of Bonds, Morts Other Securities, It none, check box	project, or thome
	project, or thome

(See Instructions on Reverse)

 Has the changed burns Preceding 12 Months (Publisher must sub
 Has Changed burns Preceding 12 Months (Publisher must sub
 PS Form 3526, September 1995 (See In nga with this state nt)