

“Resisting Temptation: Why Government Does Not Belong In Cyberspace”

**by David Euchner
© 1999 Maywood Publishing Co.**

Table of Contents

Introduction	2
I. United States Courts Attempt to Rule in Cyberspace	5
II. Disputes in Cyberspace Can Be Resolved Without Government	15
A. Private Courts Can Resolve Disputes in Cyberspace	15
B. Enforcing the Judgments of Private Courts	19
III. New Intellectual Property Laws for a New Jurisdiction	23
Conclusion	30

Introduction

Where there are two people living in a society there will be disputes, and by extension a need for a means of resolving these disputes. Frequently we hear the polarization of the alternatives “we can have order or we can have anarchy”; yet these two concepts are not necessarily at odds. By definition anarchy means “without government,” not “without law and order.” In the traditional three-dimensional world, a minimal government (consisting of nothing more than one supreme court for a given jurisdiction of voluntary association) may be necessary in order to provide a “final arbiter” when different courts pronounce opposing judgments on the same subject matter. However, the final arbiter rule assumes a completely different morph in cyberspace, where borders may exist in the form of subnets instead of arbitrary lines drawn in the sand.

The first part of the paper will discuss the failures of the courts in the United States in finding jurisdiction for themselves over causes of action that occur completely outside of their control. First, owners of servers and telecommunications have the right and the ability to police their own private property without interference from those who would usurp others’ property by means of democracy, communism, or other forms of subjugation of the individual. Second, cyberspace operates wholly outside of the geographical boundaries established by governments, almost as if it were a “fourth dimension”, so it is ridiculous to expand the “minimum contacts” test for determining whether personal jurisdiction exists in a geographical location as enunciated

in *International Shoe v. Washington*.¹ Once it becomes more commonplace for commercial, recreational and other operations to exist outside of the physical world, parties to contracts will no longer wish to be governed by archaic judges basing their decisions on archaic laws. Instead of resorting to the courts within the jurisdiction of any government, contracts will include clauses for settling potential disputes by arbitration with a respected arbitrator ruling on such cases.

Once a judicial process is set up in cyberspace, next a system of enforcing the laws and the decisions of these courts must also be established. The primary claim against anarchism is that it is totally impossible to enforce rights without a unitary branch of government dedicated to that role. There are several flaws in this rationale. For purposes of this paper, most critical is the lack of any conceptual difference between an anarchist political system in which server operators agree on enforcement techniques and an international system in which nations sign treaties doing the same. One system operator may be unable to enforce the laws of his jurisdiction against the operator of another server, but this is no more dysfunctional an arrangement than the United States being unable to enforce its laws against the Canadian government. Ultimately, whether in cyberspace or in the physical world, there are only two options for a political system: individual freedom or a “new world order.” Every existing political system is a combination of the two; some value individual freedom more and some value totalitarian rule more, but both apologize for its dilution of its principle by accepting some premises of the opposite pole. Cyberspace manages quite well under the concept of individual freedom, and until a rational explanation can be offered for a government to extend its jurisdiction into cyberspace, all governments would serve the interests of progress and justice by allowing the individuals in cyberspace to police themselves.

¹ 326 U.S. 310 (1945).

Finally, and most importantly, a set of principles by which a private court will adjudicate disputes must be formed. For reasons demonstrated herein, the present system of protecting intellectual property is outmoded. For example, patent law was established in response to the Industrial Revolution, and copyright law became possible only because of the invention of the printing press. The Information Revolution is arguably more significant in the history of human invention than both the printing press and the Industrial Revolution combined. While the discovery of cyberspace and the means to channel it do not necessarily make patents and copyrights undesirable, they certainly make it unreasonable and impossible to protect cyberspace patents and copyrights through the legislation presently on the books. One ingenious alternative system to the present system of publishing and copyrights was devised by visionary software developer Theodore Nelson which he named "Project Xanadu."² The most common critics, most notably Pamela Samuelson,³ do not uncover real flaws in the Project Xanadu model but rather are motivated by an overprotection for the status quo and a fear of progress. Cyberspace is developing regardless of whether the legal community chooses to recognize that reality; therefore, the legal community should snap to attention and make any necessary reforms before government-created chaos looms over the Internet.

² The name "Xanadu" came from the Samuel Coleridge poem "Kubla Khan." Xanadu FAQ, <http://www.xanadu.com.au/xanadu/faq.html> (accessed 4/19/99).

³ Pamela Samuelson and Robert J. Glushko, "Intellectual Property Rights for Digital Library and Hypertext Publishing Systems." 6 Harvard J.L. & Tech. 237 (Spring 1993).

I. United States Courts Attempt to Rule in Cyberspace

The foundations of the doctrine of personal jurisdiction lie in the due process clause of the Fourteenth Amendment to the United States Constitution. In *Pennoyer v. Neff*,⁴ the Supreme Court held that a lawsuit could not be brought against a defendant in a jurisdiction unless the defendant was served with notice of proceedings in that jurisdiction.⁵ In 1945, the Court further explored the question of how much benefit a party must receive from the protection of a jurisdiction in order to be sued under the laws of that jurisdiction in *International Shoe v. Washington*.⁶ Though International Shoe's headquarters was located in the state of Missouri, it employed field sales personnel in the state of Washington who acted on behalf of the company within Washington's jurisdiction.⁷ Therefore, the Court created a "minimum contacts" standard in order to decide whether a corporate body could rightly be sued within the confines of *Pennoyer* as well as the long-arm statute of any given state.⁸

Though the "minimum contacts" test has been modified over the past half century to fit the cases that arise before the courts, it is still the primary precedent cited by any court deciding a case of jurisdiction over a person (individual or corporate) not residing in that given jurisdiction. The reason is simple: it provides a court with a proper means for employing a long-

⁴ 95 U.S. 714 (1877).

⁵ "Since the adoption of the Fourteenth Amendment to the Federal Constitution, the validity of such judgments may be directly questioned, and their enforcement in the State resisted, on the ground that proceedings in a court of justice to determine the personal rights and obligations of parties over whom that court has no jurisdiction do not constitute due process of law." *Id.* at 733.

⁶ 326 U.S. 310 (1945).

⁷ Personal service was made upon a sales solicitor who acted on the company's behalf in the state of Washington. *Id.* at 312.

⁸ "[D]ue process requires only that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'" *Id.* at 316.

arm statute with a view to bringing a non-resident defendant into court to answer for actions taken within that jurisdiction by the defendant (or its agents). The need for determining the scope of minimum contacts increases dramatically as technology develops and contacts within a jurisdiction become less physical and more abstract. Citizens of various states in this country are communicating with each other (as well as citizens of foreign nations) in cyberspace in an effort to transact business within one or more of those physical jurisdictions.

The American Bar Association has recognized this need and has gathered hyperlinks to articles by various legal writers on the subject of Internet law.⁹ However, all of these references are more recent than the judicial opinions on this subject matter on which they comment, demonstrating that the legal field acted far too late in understanding the ripeness of this issue.¹⁰ Despite the fact that there was little written or even discussed concerning infringements of intellectual property rights on the Internet, plaintiffs were not discouraged from bringing actions in the United States federal courts.¹¹ Without any judicial precedent on which they could rely or any academic theories to help translate use of the new technology into terms the judicial bar could understand, judges were left with little alternative to accepting the arguments presented in the better of the two briefs presented in the case at hand.

While the opinions on the subject are extremely reliant on precedent in a heretofore-unexplored area of determining personal jurisdiction, for the most part they are not lacking in clarity or reason. In *CompuServe v. Patterson*,¹² the Sixth Circuit was presented with the novel issue of whether a programmer whose software was sold through an Internet service provider

⁹ "ABA Project on Internet Jurisdiction." <http://www.kentlaw.edu/cyberlaw/> (date visited 4/19/99)

¹⁰ *Id.* See also John Perry Barlow, "The Economy Of Ideas." *Wired*, March 1994.

http://www.wired.com/archive/2.03/economy.ideas_pr.html (date visited 4/19/99). Barlow predicted not only that law would have to change to reflect the changes in technology, but also that the legal profession would resist modifications in the law until it would be too late.

¹¹ See, e.g., *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996) (relying on ... to determine personal jurisdiction).

(ISP) could be sued in the home state of the provider even though the defendant's only connection to that state is by electronic means.¹³ The United States District Court for the Southern District of Ohio dismissed CompuServe's suit for declaratory judgment on the basis that "the electronic links between the defendant Patterson, who is a Texan, and Ohio, where CompuServe is headquartered, were 'too tenuous to support the exercise of personal jurisdiction.'"¹⁴ In this case, Patterson entered into a "Shareware Registration Agreement" with CompuServe, allowing Patterson to sell his shareware on CompuServe's network in return for a 15% commission.¹⁵ Over the three-year period 1991-1994, Patterson sold his software according to this agreement.¹⁶

The Sixth Circuit reversed the District Court's ruling on the grounds that the Ohio long-arm statute "allows an Ohio court to exercise personal jurisdiction over nonresidents of Ohio on claims arising from, inter alia, the nonresident's transacting any business in Ohio."¹⁷ While electronic commerce was a new issue for the judiciary, the Supreme Court supplied sufficient precedent that a defendant could "purposefully avail" himself in a jurisdiction without ever entering that jurisdiction.¹⁸ Since Patterson was connected to CompuServe's servers in Ohio, those who came to transact business electronically with him on the CompuServe network were doing so in Ohio.¹⁹ Furthermore, the Court determined that the cause of action arose out of activity that occurred in Ohio because the software that he alleges suffered from dilution by

¹² 89 F.3d 1257 (6th Cir. 1996).

¹³ *Id.* at 1259.

¹⁴ *Id.*

¹⁵ *Id.* at 1260-1.

¹⁶ *Id.* at 1261.

¹⁷ *Id.* at 1262. This case was brought in federal court under diversity jurisdiction. *Id.* at 1261. Therefore, Ohio substantive law must apply. See *Erie R. Co. v. Tompkins*, 304 U.S. 64 (1938).

¹⁸ In particular, the Sixth Circuit relied on *Worldwide Volkswagen Corp. v. Woodson*, 444 U.S. 286 (1980) (holding that modern modes of communication could serve to relax limits on a court's jurisdiction); *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 476 (1985) ("So long as a commercial actor's efforts are 'purposefully directed' towards residents of another State, we have consistently rejected the notion that an absence of physical contacts can defeat personal jurisdiction there.").

CompuServe²⁰ was sold in Ohio and therefore any infringement of state common-law trademarks must have occurred in Ohio.²¹

Other courts applied the “minimum contacts” test similarly in finding that non-residents made a presence in the states where they were sued. These decisions were generally based on the rationale that even though action may have been taken exclusively on the Internet, these actions were either directed at affecting the complainants’ business in the states which later invoked jurisdiction over them²² or involved the transaction of business with residents of that state.²³ On the other hand, a court could not confer jurisdiction upon a party merely for setting up a web site which could be accessed in that state.²⁴ Thus courts use this polarity to determine whether a web site is “active” or “passive”:

At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. . . . At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. . . . The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. . . .²⁵

In making such a determination, courts also look to the cause of action in the case at hand; and a court is more likely to find jurisdiction over a party when the cause of action arises from that

¹⁹ 89 F.3d at 1264-1266.

²⁰ *Id.* at 1261.

²¹ *Id.* at 1267.

²² See *Panavision Int’l v. Toeppen*, 938 F. Supp. 616 (C.D. Cal. 1996) (defendant can be sued in California for usurping plaintiff’s registered trademark and then soliciting a cash payment in return for releasing the wrongful hold on the mark).

²³ See *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997) (transaction of business with 3,000 Pennsylvanians is sufficient for conferment of personal jurisdiction in that state).

party's contacts with the state.²⁶ Additionally, a long-arm statute can apply to a party who commits a tortious act on the Internet if the party's web site exchanges information with residents of the state seeking to assert jurisdiction.²⁷

Some courts have given extraordinarily strength to long-arm statutes by ruling that merely setting up a commercial web site that is accessible without restriction in a given jurisdiction can be sufficient for personal jurisdiction to be asserted against that party. In *Inset Systems, Inc. v. Instruction Set, Inc.*,²⁸ the defendant was found to have sufficient contacts in Connecticut simply by maintaining a web site which could be accessed by as many as 10,000 users of the Internet and posting a toll-free phone number on that web site which could be used by residents of Connecticut as well as within every other state. Though the holding itself is not unlike the finding of jurisdiction in other cases, it is extremely unusual in that the court did not require the plaintiff to make a prima facie showing that the defendant's web site was accessed by a resident of Connecticut.²⁹ Though not all courts follow this decision, some courts are carrying *Inset* farther and finding that even influencing business in another state can create sufficient action for invoking the "minimum contacts" standard if information is disseminated on the Internet. In *Telco Communications v. An Apple A Day, Inc.*,³⁰ a Missouri defendant who defamed the Virginia plaintiff by posting two press releases on a web site based in Missouri and making one phone call to a securities broker in Maryland was found to have made sufficient

²⁴ See *Bensusan v. King*, 937 F. Supp. 295 (S.D.N.Y. 1996) (resident of Missouri who legitimately operated club with same name as complainant took precautions to avoid likelihood of confusion, and thus could not be haled into another jurisdiction merely because his web site could be accessed there).

²⁵ *Zippo*, 952 F. Supp. at 1124.

²⁶ *Id.* at 1127.

²⁷ See *Maritz v. Cybergold, Inc.*, 947 F. Supp. 1328 (E.D. Mo. 1996) (dilution of plaintiff's trademark and loss of business in Missouri results from unrestricted accessibility of defendant's web site in Missouri).

²⁸ 937 F. Supp. 161 (D. Conn. 1996).

²⁹ The court's opinion does not contain any information regarding such a showing, rather it was content that the site *could* be accessed from Connecticut. Cf. *Maritz v. Cybergold, Inc.*, *supra* note 27, at 1330, in which a finding was made that the defendant's site was visited 311 times by residents of Missouri (though 180 of those hits were from Maritz employees).

contacts with Virginia for the conference of personal jurisdiction. As in *Inset*, the Virginia court in this case found that the press releases posted on the Internet served to advertise the defendant's business, and defendant admitted that they would not refuse to do business with a Virginian who requested such a relationship. Such an opinion allows *hypothetical* relationships to create jurisdiction, as opposed to the *actual* contacts that were required by the Supreme Court in *International Shoe*.

At no time do any of the courts writing opinions on this subject discuss the issue of whether it is proper for a court in a geographical location to assert personal jurisdiction over a person who has no contact with that jurisdiction; instead, they hide behind Supreme Court dicta such as “the confluence of the ‘increasing nationalization of commerce’ and ‘modern transportation and communication,’ and the resulting relaxation of the limits that the Due Process Clause imposes on courts' jurisdiction.”³¹ The courts treated a novel issue with an opportunity to extend the grasp of power, when they should have exercised extreme caution for fear of denying due process to the defendants. The plaintiffs in these cases could have brought their complaints to the courts of the home states of the respective defendants without creating such a dangerous extension of the “minimum contacts” standard.

By arguing that a state can hail anyone it wants into its courts simply because a web page can be accessed from its jurisdiction, the international community will be encouraged to use similar rationale against citizens and companies in the United States, and therefore, “all such Web-based activity, in this view, must be subject simultaneously to the laws of all territorial

³⁰ No. 97-542-A (E.D. Va. 1997).

³¹ *CompuServe, Inc. v. Patterson*, 89 F.3d at 1262, citing *McGee v. International Life Ins. Co.*, 355 U.S. 220, 223 (1957).

sovereigns.”³² Actions by the Court of Appeals of Minnesota have confirmed that some of the states assent to the proposition that the Attorney General can enforce state laws against web sites in foreign countries merely because citizens of that state can access them.³³ The actions of the courts of the United States could conceivably cause global chaos by initiating jurisdiction wars, which cannot be won by countries but can only be lost by parties. It may be appropriate for Ohio to hail Patterson into its courts to defend himself against CompuServe’s action for declaratory judgment if there is no other substantial alternative; but this should not act as a wall barring the exploration of fairer and more efficient alternatives.

Laws must conform to reality, not reality to existing laws of any given jurisdiction. Attempting to fit the discovery and exploration of cyberspace into a neat pocket of existing jurisprudence is as ridiculous as reconciling Galileo’s discovery that the earth revolves around the sun with the church dogma which held that it was the other way around. It is one thing to say that Patterson can be brought into an Ohio court for signing an agreement with CompuServe that he will put his software on CompuServe’s servers that are located in Ohio and deal with customers who essentially travel to Ohio to meet Patterson on CompuServe’s servers. However, it is an entirely different situation when a state thinks it can assert jurisdiction over everyone with an unrestricted web site.

All of the cases discussed previously involve defendants who are all residents of the United States but deny that the courts in those respective states have personal jurisdiction over them under F.R.C.P. 12(b)(2). In other words, had the plaintiffs brought these lawsuits in federal courts in the defendants’ home states, the defendants may not have made these arguments for

³² David Johnson and David Post, “Law and Borders – The Rise of Law in Cyberspace.” http://www.cli.org/X0025_LBFIN.html (accessed on 4/19/99).

dismissal. Moreover, the choice of forum is not at issue for purposes of conflict of laws, because even if the case does not involve federal law, the laws of most states are in conformity with each other. But what if the defendant is not a United States national and does not have “minimum contacts” with any United States jurisdiction as understood in *International Shoe*?

Consider the following hypothetical situation. Smith sells a software package called “Smith’s World” on his web site which is located in England, and Jones, a resident of Connecticut buys the software for \$10. The terms of this exchange required Jones to send a \$10 bill through the mail and in return Jones would download the program from Smith’s web site. Software Programmers, Inc., a corporation with headquarters in Boston, Massachusetts and exclusive owner of the federally-registered trademark “Smith’s World,” sells its software “Smith’s World” in each of the fifty states as well as in many foreign nations. Upon hearing of the competing software, SPI wants to sue Smith for a violation of the Lanham Act, but they do not have lawyers in England and the only commercial contact Smith has had in the United States is the \$10 sale to Jones in Connecticut. Consequently, SPI files in the District of Connecticut alleging dilution under the Lanham Act as well as state common-law unfair competition.

Though *Pennoyer* and *International Shoe* would compel a dismissal under Rule 12(b)(2) for lack of jurisdiction over the person, the District of Connecticut could rely on its decision in *Inset* and hold that Smith purposely availed himself of the benefits of the laws of Connecticut by marketing and selling his software in Connecticut. When presented with the argument that this is not an appropriate venue since any harm done to plaintiff would be done in Europe where the defendant sells 99% of his software, the District Court would quote from *Inset*: “Since the defendant [] is subject to personal jurisdiction in Connecticut, then for venue purposes, it is

³³ *State of Minnesota v. Granite Gate Resorts, Inc.*, 568 N.W.2d 715 (Minn. 1997) (holding that the Attorney General can enforce the state's gambling laws against a web site located in Belize merely because

deemed to reside in Connecticut. The court concludes, therefore, that the provisions of §1391(b)(1) having been complied with, Connecticut venue is proper.”³⁴ It is the conceivability of such a preposterous situation that should prompt the legal community from finding a suitable alternative before the preposterous becomes reality.

As if the above example does not sufficiently demonstrate the need for significant change in personal jurisdiction doctrine, what would the courts do when presented with true “hard cases”? Suppose an unidentified person known only to his accusers by his cybernym (online pseudonym) “grisham” scans a copy of John Grisham’s latest book into digital format and then posts it on UseNet newsgroups and e-mails it to everyone who posted to the newsgroup alt.fan.johngrisham.³⁵ Our hypothetical copyright infringer is extremely skilled at avoiding any connection between himself and any personal identification or geographical location, so John Grisham is left with no legal recourse for recovering the financial damage caused by the distribution of his book to his fans who no longer saw the need to buy it at the store. Such a case can and will happen, and authors, inventors, and commercial enterprises deserve a forum for receiving justice.

Presently, the recourse for such an action is to identify the person using the cybernym and then serve that person with notice that they will be hailed into a court in a geographical location. A recent example is that of Raytheon Corp. suing employees for disclosing proprietary information in Yahoo! chat rooms.³⁶ Since the employees were using cybernyms such as "Rayman-mass" and "RaytheonVeteran," Raytheon sought and won subpoenas from a court

Minnesotans can access the site).

³⁴ *Inset Systems*, 937 F. Supp. at 166.

³⁵ No newsgroup dedicated to John Grisham actually exists, which speaks volumes about the technological savvy of Grisham’s readers.

³⁶ Associated Press, “Case Raises Questions About Online Privacy,” April 6, 1999. <http://cnn.com/TECH/computing/9904/06/internet.privacy.ap/index.html> (accessed 4/19/99).

ordering Yahoo! to produce the names and addresses of the persons using those cybernims.³⁷ Advocates of privacy rights have encouraged companies such as Yahoo! to resist the subpoenas,³⁸ but Yahoo! includes in the terms of agreement with its message board users that they will comply with valid subpoenas.³⁹ When asked to comment on the issue, a spokesperson for America On-Line stated that when it is served with a subpoena, it gives the member two weeks to attempt to quash the subpoena and only then does AOL comply.⁴⁰

³⁷ *Id.*

³⁸ "'Companies should not disclose such information, even in response to a subpoena, without some due process,' said Marc Rotenberg, director of the Electronic Privacy Information Center. He said companies should aggressively fight such subpoenas." *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

II. Disputes in Cyberspace Can Be Resolved Without Government

A. Private Courts Can Resolve Disputes in Cyberspace

Cases such as these are brought arising from actions taken in cyberspace, with no ties to any geographical location except for the person controlling the transmission of the data. But though these actions occur nowhere in terms of physical location, they do occur somewhere – in cyberspace.⁴¹ Since cyberspace is a location, there is no reason why a court sitting in an area of cyberspace could not legitimately assert jurisdiction over activity occurring in that location. Some may argue that the establishment of new courts sitting in cyberspace will create unforeseen disasters because a cybercourt would have to choose which laws it would enforce and which methods of enforcing its decisions it will support. Those arguments will be answered in the following sections of this paper, but it is necessary to determine first what jurisdiction a cybercourt shall possess.

Government only exists where humans establish it. Cyberspace is so recently discovered that no government has had the opportunity to create a regulatory system over it that can be enforced, save for the data which can be seen and heard without the use of a computer. The United States Customs Service does not even attempt to find data that is smuggled across United States borders illegally.⁴² And even in the absence of government, the cybercommunity has managed to create rules that are suitable for its netizens and are followed by those netizens because of their appropriateness. The fact that there are rules in cyberspace at all without a government to establish them is proof of the theory that a government is not necessary to

establish law and order. The only problem is that geographical governments are unwilling to recognize that cyberspace is an entirely separate location which was not discovered by the agent of any government. None of the original settlers of the Internet stuck a national flag in the dirt similar to Neil Armstrong's planting of the American flag on the moon in 1969, and at present there still is no national flag flying over cyberspace. Instead, many netizens see their participation in the cybercommunity as a way to distance themselves from the governments where their physical bodies are located.

Without government, however, there must be some factor that can make a unilateral determination of jurisdiction over a dispute. There is only one factor that can lead to a unilateral determination of jurisdiction: *private ownership*. If one is the owner of a certain property, only that owner has the right of disposal and only that owner can make commitments of that property. There is no such thing as a "legitimate violation" of property rights; anyone whose property rights are violated is due compensation for those damages. A property owner can license use of some or all of that property and specify terms for an agreement, and the owner must be able to reclaim damages if those terms are not met. Every area of cyberspace is a place, and therefore should have an owner.

Sometimes an owner has absolute control over one's own property but nonetheless cannot fully utilize that property without the assistance of another. For example, I may own a channel on the Internet Relay Chat (IRC) UnderNet (an area of the Internet dedicated to IRC), but my use of the channel is dependent on my ability to access the channel. This requires me to pay a fee for access to the Internet, and then I must agree to the terms of use of the UnderNet server, which hosts my channel. Beyond that, both my Internet provider and the UnderNet

⁴¹ Johnson & Post, *supra* note 32.

⁴² *Id.*

server get their access to the Internet from the owners of a backbone. Either my Internet provider, the UnderNet server which hosts my channel, or the backbone owner may place other conditions upon my usage of the channel, such as a prohibition on obscene language or a mandate that I obey the laws of any applicable jurisdiction.

Presently, each owner establishes whichever rules the owner prefers, and anyone who uses that property must agree to the owner's terms and conditions. Sometimes, as with large corporate entities like Microsoft, AOL and Yahoo!, a user of the services is expected to agree to a formal contract by clicking "I AGREE" before proceeding into a cyberzone under their control. Other owners of smaller chat rooms, such as channel #MICROSOFT_IS_EVIL on the UnderNet, can kick and ban any user from its room simply for saying "Bill Gates is God" without giving the matter a second thought. There is no First Amendment protecting free speech in cyberspace, because there has to be a United States government with jurisdiction to grant that protection. Free speech is promoted in cyberspace, not because the United States Supreme Court says it has to be this way, but because each owner of a cyberzone understands that intellectual growth only comes from the free exchange of ideas.

However, most disputes arise where no party involved has the unquestioned authority of ownership, and there must be a singular way of determining who shall resolve the dispute. Many of these disputes arise out of a breach of contract claim; and jurisdiction over these disputes can be easily decided in a clause of the contract. For all other claims which do not arise out of a breach of contract, the case should be heard in the jurisdiction of the "least common denominator" (hereinafter "LCD") of ownership.⁴³ This means that the owner of the property

⁴³ The term "least common denominator" is usually used in mathematics for finding the smallest whole number which can be factored by the denominators of two or more fractions. For purposes of this discussion, LCD shall be defined as "the lowest point in a network infrastructure which provides Internet access to both parties to a dispute."

where the alleged action occurred should host proceedings, and if there is no such property then the host shall be the owner of the property which grants use privileges to both plaintiff and defendant.

One example of a small-scale implementation of LCD could be a copyright infringement complaint against a defendant who reproduced a protected work on an IRC channel (which is owned or controlled by neither party). The owner of the copyright and the infringer use different providers for their Internet access, but upon analyzing the network hierarchy the copyright owner can see that both Internet providers receive their access in turn from the same backbone provider. The copyright owner then has two options, either to file an action with the infringer's provider or to file with the LCD provider. On a larger scale, an LCD provider would be the only possible venue for two mammoth corporations who cannot resolve their dispute.

Many parties would rather submit their cases to an LCD provider for a hearing than to a court in the jurisdiction of the defendant not only because it may be an inconvenience to meet in the defendant's jurisdiction (though not quite as inconvenient as physically travelling to another point on the globe) but also because the laws of an LCD provider will tend to be more favorable to the plaintiff. Both parties to a dispute brought before an LCD provider have already agreed to obey its laws, if not directly then indirectly through the laws of their respective providers. On the other hand, the laws of the defendant's jurisdiction may be completely unfavorable to the plaintiff's cause of action, or the defendant's jurisdiction might simply be biased against foreigners or have a reputation for poor adjudication of cases. LCD providers, on the other hand, would have such large caseload that they could turn a sizable profit in this market; therefore, they will be extremely scrupulous in selecting the arbitrators who will adjudicate these cases.

B. Enforcing the Judgments of Private Courts

Private courts exist in the United States even today, but enforcement of those judgments is left to the government (if enforcement is available at all).⁴⁴ The acknowledged purpose of these courts is to minimize the costs of resolving disputes.⁴⁵ This admission raises an interesting question: if private courts minimize costs of litigation, and therefore government courts cause excessive costs, why should the government courts be used at all? It would not be correct to assert that the government's judges are more qualified for deciding these disputes, because in reality federal judges are selected based on their political contacts, whereas in the private sector judges are selected based on their ability and experience in deciding cases in a specialized area of the law.

For much the same reasons that private courts are more efficient and accurate than government courts, private law enforcers are also more efficient and accurate than police agencies employed by any level of government. The primary reason for the efficiency of private police is the ability to hold them accountable for their wrongful actions. Tort law allows a victim to sue not only the person who committed the wrong but also the prospective defendant's employer under the *respondeat superior* doctrine if the wrong occurred in the scope of the defendant's employment. On the other hand, government officials can only be sued for their wrongful actions under limited circumstances, and the agencies for which they work can only be

⁴⁴ See, e.g., Shannon P. Duffy, "Private Courts." *The Legal Intelligencer*, April 14, 1999. <http://www.mises.org/fullstory.asp?FS=%3Ch3%3EPrivate+Courts> (accessed 4/19/99) (describing the formation of a National Patent Board which would arbitrate patent cases but would not prevent the resort to appeal in a government court).

⁴⁵ *Id.*

sued if there is a procedure in place which violates (or should reasonably have been foreseen to violate) rights of the citizens.⁴⁶

Police agencies can contract with courts for the business of enforcing judgments. Since the courts are private, there is no obligation for the courts to give the contract to the lowest bidder; in fact, the court would not have to give any justification whatsoever for its decision to hire that agency. It should be noted that if the police agency is ineffective or violates the rights of netizens, the court which contracts for its business would not qualify as an employer under the *respondeat superior* doctrine and therefore would not be liable for its contractor's actions. Yet this does not mean that the court would escape without punishment. A court that earns a reputation for releasing attack dog police on the losers of judgments without any rational justification would find very quickly that it will lose all of its business.

Under the present system of government police protection, the citizens of a jurisdiction are coerced to finance the police force regardless of the effectiveness or fairness of that police force. There is no way for a citizen of the jurisdiction to opt out of that system. A private police agency in cyberspace, however, could finance itself by billing the party for the cost of bringing that party to justice. For example, a copyright infringer who is found liable for damages but attempts to evade payment of the judgment can be tracked by police and then billed additionally for the cost of the tracking. Obviously there would be no cost for enforcement if the loser of a case simply paid the damages which are assessed against him, and therefore a loser in a court action has incentive to follow the judgment of the court. Moreover, a police agency which

⁴⁶ Under 42 U.S.C. 1983, a private citizen can sue a police agency for a rights violation only if the action is committed "under color of state law," the use of force is totally unreasonable, and no other immunity privilege can be applied. See, e.g., *Board of County Commr's of Bryan County v. Brown*, 117 S.Ct. 1382 (1997) (county not liable for sheriff's hiring of nephew as deputy even though the nephew's rap sheet included offenses that clearly showed a propensity for violence); *City of Sacramento v. Lewis*, 118 S.Ct. 1708 (1998) (allegation that high-speed pursuit was undertaken with deliberate indifference to passenger's survival was insufficient to state substantive due process claim).

understands that it can be held liable for any costs of excessive force under *respondeat superior* theory will be extremely careful in its hiring and training practices.

As with judicial proceedings in geographical jurisdictions, a plaintiff might bring an action in a jurisdiction that has authority over the defendant, but the defendant does not appear or the defendant flees after an adverse judgment. This leaves the responsibility with the police for tracking the defendant, but the police cannot succeed in every single case. In such a situation, the court can call upon the cybercommunity to assist in finding the defendant and bringing him to justice. Penalties can include (but are not limited to) revoking existing privileges and prohibition on establishing new privileges on servers and networks, seizing assets on a server or network, and a notice disseminated throughout cyberspace that the defendant is a fugitive from justice. This does not prevent every wrongdoer from fleeing justice, but for some the inability to connect to the Internet is as great a hardship as the unavailability of food and shelter. If the defendant happens to find refuge with a renegade provider of services who refuses to turn his refugee in to the proper authorities, then the cybercommunity can embargo and ostracize that renegade provider as well. Just as the international community on Earth has punished Libya for harboring the suspects in the airline bombing over Lockerbie, Scotland for a decade, the community of law-abiding Internet providers can do the same to renegade who thinks that he is above the law.

Furthermore, while it is possible that large corporations such as backbone providers may deny their customers of their rights under contract, it is not in their interest to do so. The reason why corporations would avoid treating their customers unjustly is simple: it hinders their profits. Politicians in geographical nations do not worry if people's rights are violated, because not only are they usually immune from suit but they also profit from fighting wars. A corporation who

violates the rights of one of its customers loses that much business; but if the corporation makes a habit out of such practices then it can discover rapidly that its customers are finding ways around giving it any business at all.

III. New Intellectual Property Laws for a New Jurisdiction

This paper has already advocated the replacement of the present system of adjudication of cases dealing with cyberspace with a system of courts that need not follow the laws of any of the nations on Earth. The rationale for doing so is simply that the politicians of Earthly nations are using irrational means toward achieving the irrational goal of carving out their own sections of cyberspace for nationalistic purposes. So far cyberspace has successfully rejected many attempts by government to enter its space, but ultimately governments will invade unless the cybercommunity can demonstrate its ability to institute a rational code of ethics and laws and then successfully police those laws and resolve disputes based on those laws. Far from being an insurmountable challenge, the cybercommunity can embrace this opportunity to prove to the governments of Earth that governments are not necessary for the procurement of “law and order.”

Most areas of intellectual property require only minor modifications from the general acceptances of the western culture that intellectual property should be protected. The signatories to the Paris Convention (protecting industrial property) and the Berne Convention (protecting literary and artistic works) have accepted the premise that intellectual property such as copyrights, trademarks, trade secrets and patents should be protected from misappropriation and have instituted standards in their respective nations for such protection. Protection for trade secrets is usually provided in companies’ contracts with their employees, so a cybercourt would decide the issue on the breach of contract cause of action using a methodology similar to the state courts in the United States. Also, trademarks and service marks can be registered at any

level of jurisdiction in cyberspace by registers who, in return for payment, will vouch for the validity of the mark.⁴⁷

Protection for patents in cyberspace⁴⁸ is a potential source of legal pitfalls, not unlike protecting the rights of patent holders in nations that do not recognize those patents. For example, the owner of a server may decide that it is in the best interest of his community if he offers certain privileges to netizens who bring him useful inventions. This server owner may even enter into contractual agreements with the owners of other servers and telecommunications stating that all will respect the patents of inventors in their respective communities. However, the inventor who seeks patent protection from a server owner has an enormous advantage over the inventor who seeks patent protection from the United States or nations with similar laws. Whereas the United States Patent and Trademark Office is required by law to publish all patent applications and thereby give the plans for construction of the invention to anyone who is not obligated to obey United States law, a server owner may choose to keep the plans for construction undivulged. Thus, the inventor can enjoy the benefits both of patent protection in the jurisdictions that respect his patent and of trade secret protection everywhere.

The one sector of the intellectual property realm that requires a complete reconstruction is copyright. While the Copyright Act of 1976⁴⁹ is adequate for the protection of physical works such as sculptures and books, the popularization of the Internet has turned the law into a ring of fire that seekers and disseminators of information must leap through in order to achieve their worthwhile goals. Especially with regard to literary works, there is little financial incentive to

⁴⁷ Should the party registering the mark be sued for infringement by a pre-existing owner of the mark in that jurisdiction, the party accused of infringement can sue the register as a third-party defendant for breach of contract.

⁴⁸ It should be understood that any patents in cyberspace can only be granted to inventions that can exist solely in the form of information. If an invention cannot be converted into data completely, it is more appropriate to seek the patent protection of a geographical government.

⁴⁹ 35 U.S.C. 101 et seq.

pirate copyrighted works in physical forms such as paperback books. On the other hand, there is substantial educational incentive to disseminate a copyrighted work over the Internet when it does not already exist in digital form. The cybercommunity must be able to devise a method by which netizens will have easy access to any information they desire without denying the financial rewards to the authors who produce that work.

Theodore Nelson foresaw this need in 1960 (over a decade before the first Ethernet network was created) and envisioned a model for a cyberlibrary connected by hyperlinks, which he named “Project Xanadu.” Nelson believed that hypertext libraries must be standardized and commercially regulated if it is to prevent the software incompatibilities and broken links that plague the World Wide Web today.⁵⁰ Project Xanadu employs a technique called “transpublishing” which allows readers of a copyrighted work to quote as much as they choose without needing to concern themselves with re-publication burdens such as purchasing a license.⁵¹ Despite the readers’ expansive rights, the “transquotation” model does not deny the moral rights of the authors whose words are “transquoted”; instead, the context of the original quote is maintained by transquote symbols.⁵² Should a new document containing the transquote be created by a new author, a hyperlink would remain embedded in the transquote and a click on the hyperlink could bring the reader of the new document to the original document from which the transquote was taken.⁵³ Additionally, should the original document be modified in any way that affects the transquote that was taken by the author of the new document, the new document will also be updated automatically.⁵⁴

⁵⁰ Ted Nelson’s Home Page, <http://www.sfc.keio.ac.jp/~ted/XU/XuPageKeio.html> (accessed 4/19/99).

⁵¹ Transpublishing: An Easy Concept, <http://www.sfc.keio.ac.jp/~ted/TPUB/TPUBsum.html> (accessed 4/19/99).

⁵² Transquotation Demo, <http://www.sfc.keio.ac.jp/~ted/TPUB/TQdemo.html> (accessed 4/19/99).

⁵³ More Benefits of Transquotation, <http://www.sfc.keio.ac.jp/~ted/TPUB/tpubMoreBenefits.html> (accessed 4/19/99).

⁵⁴ *Id.*

Such a library would require a payment system for financial sustenance, but the financial resources for maintaining electronic libraries would be microscopic in comparison to maintaining thousands (maybe millions) of paper libraries all over the world.⁵⁵ According to Nelson, Project Xanadu would bring in revenues from users of the system as well as authors who rent storage space on the system.⁵⁶ After meeting expenses and keeping profits, the transpublisher would dispense royalties to authors, depending on how many times each author's documents were accessed by users.⁵⁷ In order to provide incentive for the creator of documents containing transquotations to original authors' materials, Nelson would qualify the creators of hyperlinks as authors (though authors in this class would only be eligible for a small fraction of the total royalty payments for that quote⁵⁸).

Wherever there is a visionary with a novel idea, there is also a critic seeking to prevent that vision from dismantling the status quo, and it is the role of critic which Pamela Samuelson plays in her academic contribution to the ironically-named 1993 Harvard Symposium on Electronic Communication and Legal Change.⁵⁹ All of her criticisms of Project Xanadu stem

⁵⁵ Nelson believes that only electronic commerce could succeed in Project Xanadu. Keio Formats, <http://www.sfc.keio.ac.jp/~ted/TPUB/TransPayMethods.html> (accessed 4/19/99).

⁵⁶ Samuelson, *supra* note 3, at 248.

⁵⁷ *Id.*

⁵⁸ Nelson explains the difference of royalty payments to original authors and authors of transquoted materials:

IT'S EXTREMELY DIFFERENT FROM ORDINARY REPUBLICATION

- The transquoter CANNOT MAKE MONEY from including transquoted material, since it is NOT REALLY IN THE NEW DOCUMENT; the benefit to the transquoter is to be able to present the material in some desired context of other contents.
- However, the transprovider can make money, by selling the quoted portions for very small amounts; these will add up significantly if pages are read very widely.
- The transquoter does not actually supply the quoted material, but provides pointers (TQstrings) which cause the quotation to be brought (or bought) from the original publisher.
- The transquoter pays nothing to the original publisher, since each reader will be downloading from the original publisher.
- No negotiation is necessary between original publisher and transquoter.
- The transquoter need not even contact the original publisher.

Transpublishing: Popular Misunderstandings, <http://www.sfc.keio.ac.jp/~ted/TPUB/tpub-pop-misunder.html> (accessed 4/19/99).

⁵⁹ Samuelson, *supra* note 3.

from a mistaken belief that Nelson just does not understand the way copyright law works, and he needs to modify his system in order to protect the rights which the existing copyright law protects. For example, she believes that the elimination of “fair use copying” would dismantle a necessary element of copyright law.⁶⁰ Nelson would agree with her except for the word “necessary”; he correctly sees the “fair use” doctrine as a burden on users of the copyrighted material without providing any benefit to the original publisher or copyright owner.⁶¹ Instead, Project Xanadu would offer substantial benefits to the transpublishers of copyrighted material, while also providing additional financial gains to original authors who would be able to receive none of these royalties under the “fair use” doctrine.

Samuelson also notes that a constructor of a hyperlink should be considered an “author” in the Project Xanadu system, since by traditional definition an “author” is the creator of expressive work and a hyperlink author is simply a builder of a bridge which connects two pieces of information.⁶² Samuelson is missing the point here. Nelson does not mean to give copyright protection to the creator of hyperlinks; he merely seeks to compensate them for the productive labor they provide to the library. The financial reward that the authors of hyperlinks earn is payment for services, just as an automobile operator would pay a toll before traversing the George Washington Bridge.

⁶⁰ *Id.* at 251-252.

⁶¹

- "Fair use" is a marginal method, a minor accommodation that loosens copyright law-- actually, sets it aside—to allow small re-uses as exceptions.
- Fair use meets some of the needs of republishers (if very modest), but it has no direct benefit to original publishers.
- Transpublishing offers publishers a new form of distribution and sale.
- Fair use is for short quotations only; transpublishing allows quotations of any length and quantity.
- Fair use does not require permission by the original publisher; transpublishing requires a specific permission method so that all parties clearly know what permission exists.

Transpublishing: Popular Misunderstandings, <http://www.sfc.keio.ac.jp/~ted/TPUB/tpub-pop-misunder.html> (accessed 4/19/99).

⁶² Samuelson, *supra* note 3, at 252. She notes that under 17 U.S.C. 102(b) “discoveries” are not copyrightable subject matter, and the Supreme Court has upheld the exclusion from copyright protection for facts in *Feist Publications, Inc. v. Rural Tel. Serv., Inc.*, 111 S.Ct. 1282 (1991).

Samuelson further assumes that Nelson has not properly analyzed whether the community of authors would accept publication of their work in such an environment, and yet she provides no additional data that would even suggest a conclusion in concert with her own. First, she expects authors to revolt against Project Xanadu for requiring a rental fee for the authors' works.⁶³ She must not be aware of the fact that this expense is covered by the authors in the present method of publication by the reduction of royalties. She also recognizes many reasons why authors may not fully capitalize on the benefits of Project Xanadu, such as lacking confidence in their work or inability to pay for the rental space.⁶⁴ First, anyone who could not afford the rental space (translated into U.S. currency, a 200-page book would probably cost about a half-dollar for one hundred years' rent) probably could not afford the paper on which they would have typed a manuscript. Second, an author who lacks confidence in his work would risk only a handful of pennies in publishing on Project Xanadu, rather than make appointments to meet publishers and hand out several paper copies hoping that one will accept the cost of publishing it.

The ignorance of her critique becomes ever so apparent when she makes the presumption that users in search of knowledge would only visit the document that tallied the most visits. If this were true, then there would be extreme harm done to scholars in every field, as doctors might attempt to circumvent a medical education in favor of practicing what they read from an old "ER" script. But it is patently obvious that this is an irrational fear, for those seeking knowledge exhaust all available sources before they are satisfied that they gathered all available information on the subject. Samuelson also believes that even if others correct a previously-published article with erroneous information, the article with the erroneous information will still

⁶³ Samuelson, *supra* note 3, at 256.

⁶⁴ *Id.*

be linked and therefore that author will receive royalties. First, each reader should have the benefit of deciding for himself whether the article is erroneous or just misunderstood without having Samuelson's "establishment" telling him right from wrong. Second, even if the article does contain completely wrong information and the article cannot be removed from the system, the present system of publication does not provide a mechanism for removing information which has already been disseminated to the public. One can only presume that Samuelson expects people to stop reading about Nelson's system merely after reading her article denouncing Project Xanadu.

Nelson foresaw not only the need for an efficient method of publishing literary works, but also the arguments made by those who would misunderstand and misconstrue his method. Those skeptics who, like Samuelson, would prefer to waste their time and money *attempting* to publish in print when they have guaranteed success in getting published on Project Xanadu are welcome to follow that prerogative. But Nelson's ideas should offer a clear demonstration that if copyright law can be transformed to suit the new technology, then it is possible to shape all intellectual property law to suit the cyberspace model.

Conclusion

A cyberspace with no government would not behave much differently from the international community does at the present. It is possible that the owners of one hundred different servers will have just as many different legal systems, and since they are owners of their property they have the right to dispense of that property as they see fit. The only other alternative to such a system is world domination by one man, whether that one man should be Adolf Hitler, Josef Stalin or Bill Clinton. Not even democracy can protect the rights of its citizens; after all, “democracy is four wolves and a sheep voting on what to eat for lunch.”⁶⁵ Especially in cyberspace, a location that was discovered without regard to any nation on Earth, individuals must be permitted to pursue their own happiness without worries about impending government invasions.

The cybercommunity has had terrific success at creating its own rules for behavior and enforcing those rules. Presently it is impractical to implement the judicial and enforcement systems that this paper advocates; but in the very near future those impracticalities will disappear. Legal scholars must accept the responsibility of advising providers of Internet services on this subject so that the cybercommunity will not slip into chaos merely because it has anarchy. In return for the education in jurisprudence, the Internet providers should teach the legal scholars how the technology of the Internet operates so that the legal community can help in crafting laws that fit the technology. And if the legal community can perform this task successfully, then each individual owner of property can consider whether the suggestions are adequate and rational and implement the laws deemed to be proper. Ironically, this process of

⁶⁵ This is an old libertarian proverb.

offering all owners the right to state the laws on their respective properties will meet with far greater success in unifying law across cyberspace than the force of government ever could.