International Jurisdiction in Cyberspace:Which States May Regulate the Internet?

Stephan Wilske[*]

Teresa Schiller[**]

There is no dark side of the moon.

(Pink Floyd)[1]

I. Introduction

A. The Evolution of a Global Internet

The Internet's growth over the last years has been large and dramatic.[2] An American idea that began in 1969 as an obscure military experiment, the Internet is now becoming a global community. The first international connections from the United States were established to England and Norway in 1973.[3] By the end of 1995, more than 4.5 out of 6.6 million hosts were located in North America, with the rest spread out among connected networks in about one hundred other countries.[4] The portion of the Internet outside North America is meanwhile growing at an accelerated

speed. It now reaches 60 million users in 160 countries, with the number doubling each year. The number of domains rose from 120,000 to 488,000 from 1995 to 1996.[7] European users are expected to double every year, reaching 100 million in 2001.[8] Internet users in Asia currently number 3 million, and the total is expected to reach 25 million to 30 million by the end of the decade.[9] Meanwhile, even Mongolian herdsmen can go into libraries where the Internet is accessible through a combination of digital radios and satellite links.[10] And North Korea, one of the world's most secretive societies, recently began publishing English reports on the Internet.[11] While the vision of a global Internet community has a great deal to offer, different legal, cultural, political, and economical sensitivities must be faced.[12] In particular, jurisdictional questions have become increasingly complex with the explosion in Internet usage and technology. Some courts and enforcement agencies in America advocate broad exercises of jurisdiction. As countries with stricter laws choose to adopt this approach, however, American citizens may find they are facing the blade of a double-edged sword.[13]

B. The Regulation of Cyberspace

The rapid growth of the group known as "cyberspace"[14] users will be accompanied by a growth of regulation. As long as cyberspace was a playground for a small fraction of highly educated people, paid for by large institutions, the myth of an unregulated, independent space could grow.[15] Part of the happy mythology of the network holds that it is a self-regulating entity, controlled by no government—one of the few instances in history of successful anarchy.[16] This was never completely true since most countries have long-standing laws that regulate speech and commerce, irrespective of the medium.[17]

It should not have been surprising that with its expansion the Net became relevant to the "real" world. Legal reality intruded upon the world of Internet: Where terms like "rape in cyberspace,"[18] "cybertorts,"[19] "cybercrime,"[20] and "cyberterrorism"[21] are created, the cry for regulation is not far away.[22] Regulation finally came to the surprise of "Netizens," not just from the national level.[23] When CompuServe, Inc. blocked access by its subscribers in the United States and around the world to two hundred discussion groups after a federal prosecutor in Germany had indicated that they might violate German pornography laws,[24] users realized that "cyberspace doesn't belong to a single country,"[25] but to a whole range of countries with diverse legal concepts.

Many other States have expressed an interest in regulating the Internet. Chinese officials announced in January 1996 that they wanted to stop "detrimental information" from entering the country via the Internet.[26] The French Government is said to have complained to CompuServe that there is too much English on the Internet.[27] Britain's "Home Office is currently examining how the Internet can be regulated."[28] "The Malaysian government has proposed a bold new legal framework, popularly known as the `cyberlaws,'"[29] which extends beyond the shores of Malaysia. The director of policy and planning at the Singapore Broadcasting Authority, the government's regulatory body for the Internet and broadcast media, said: "In cases where a libelous act has been committed, whether or not it is done on the internet or any other public medium, the laws of Singapore still apply."[30]

Meanwhile, it is hard to maintain that the Net is some kind of free city in the sky.[31] Politics and pornography are not the only reasons why governments want to control the Internet. There are financial aspects, such as taxation,[32] intellectual property rights,[33] trade,[34] and gambling.[35] As governments need to control their revenues, the desire to control the Net grows.[36] One question of importance is certainly still the question of how to regulate cyberspace.[37] More and more important, however, becomes the question of who has authority to regulate cyberspace.[38] As individual countries begin to regulate cyberspace, their decisions reach far beyond national borders. Can one country be so influential in regulating the Net that the consequences are felt around the world? How far may a country go? Or, as *The Economist* preferred to formulate the question in the aftermath of the *CompuServe* case: "When Bavaria wrinkles its nose, must the whole world catch a cold?"[39]

This analysis covers bases of international jurisdiction in cyberspace. It identifies criteria which enable a State to

prescribe rules for cyberspace, to subject violators of these rules to the process of its courts, and eventually to enforce these rules. Domestic multijurisdictional cases are analyzed, not for their correctness under U.S. law, but for their precedential value for international multijurisdictional cases.

The focus of this analysis is to show that States are not impressed by an alleged "independence from geographical constraints" resulting from the "electronic nature of the message transmission"[40] or by a presumed failure of "territorially-based laws" to reach persons "whose geographical jurisdictions span legal jurisdictions."[41] As the focus is on the competence of the State to exercise jurisdiction, collateral consequences for the individual, such as the possibility to pursue a lawsuit in a variety of different jurisdictions, will be of only subordinate interest for this analysis.[42]

II. International Law of Jurisdiction

Under international law, a State is subject to limitations on its authority to exercise jurisdiction in cases that involve foreign interests or activities.[43] International law, however, does not impose hard and fast rules on States delimiting spheres of national jurisdiction. Rather, it leaves States wide discretion in the matter. Nevertheless, the existence of limits is undisputed. Every State has an obligation to exercise moderation and restraint in invoking jurisdiction over cases that have a foreign element, and they should avoid undue encroachment on the jurisdiction of other States.[44] A State that exercises jurisdiction in an overly self-centered way not only contravenes international law, but it can also "disturb the international order and produce political, legal, and economic reprisals."[45]

Traditionally, three kinds of jurisdiction are distinguished: jurisdiction to prescribe, or legislative jurisdiction; jurisdiction to adjudicate, or judicial jurisdiction; and jurisdiction to enforce, or executive jurisdiction.[46] Jurisdiction to prescribe is the first step in many analyses. Jurisdiction to adjudicate does not apply in the absence of jurisdiction to prescribe unless the forum State is willing to apply the law of a foreign State. For jurisdiction to enforce, States also regularly need jurisdiction to prescribe. These distinctions can be important in determining the limits of a country's jurisdiction under international law. Depending on the nature of the jurisdiction being exercised, the requisite contacts with a State necessary to support the exercise of jurisdiction differ.[47] The three types of jurisdiction however, are often interdependent, and their scope and limitations are shaped by similar considerations.[48] The following analysis of the international law of jurisdiction is based on the assumption that the relevant provisions of the *Restatement (Third) of Foreign Relations Law of the United States* correctly restate the consensus of the community of nations.[49]

A. Jurisdiction to Prescribe

1. Bases of Jurisdiction to Prescribe

Jurisdiction to prescribe means a State's authority to make its substantive laws applicable to particular persons and circumstances.[50] International law has long recognized limitations on the authority of States to exercise jurisdiction to prescribe in circumstances affecting the interests of other States. In principle, it was accepted that a State had legislative jurisdiction to regulate activities within its territory, as well as the conduct of its nationals abroad.[51] Yet, there is wide international consensus that not even the links of territoriality or nationality suffice in all instances for the exercise of jurisdiction to prescribe.[52] For instance, according to Article 34 of the Vienna Convention on Diplomatic Relations, diplomats are exempted from most dues and taxes.[53]

Restatement section 402 summarizes bases of jurisdiction which indicate a legitimate interest of a State to assert jurisdiction to prescribe as follows:

Subject to section 403, 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 its territory that has or is intended to have substantial effect within its territory;

(2) the activities, interests, status, or relations of its nationals outside as well as within its territory; and

(3) certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests.[54]

These principles are known as the territoriality principle, the nationality principle, the effects principle, and the protective principle.[55]

The broad bases of jurisdiction restated by section 402 are limited by section 403 which imposes a general requirement of reasonableness:

(1) Even when one of the bases of jurisdiction under [section] 402 is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connection with another state when the exercise of jurisdiction is unreasonable.[56]

Section 2 of section 403 enumerates different factors which have to be evaluated in determining the reasonableness of assertion of jurisdiction.

(2) Whether exercise of jurisdiction over a person or activity is unreasonable is determined by evaluating all relevant factors, including, where appropriate:

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

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

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

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

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

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

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

(h) the likelihood of conflict with regulation by another state.[57]

When the prescriptions of two States are in conflict, each State has an obligation to evaluate its own as well as the other State's interest in exercising jurisdiction. A State should defer to the other State if that State's interest is clearly greater.[58]

Another basis of internationally-recognized jurisdiction—universality jurisdiction—is described in section 404 of the Restatement:

A state has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism, even where none of the bases of

jurisdiction indicated in [section] 402 is present.[59]

2. Application in Cyberspace

a. Territoriality Principle

"The territoriality principle is by far the most common basis for the exercise of jurisdiction to prescribe, and it has been generally free from controversy."[60] This principle would allow a State to order service providers who operate on its territory to obey its regulations. It would further allow barring access to certain Web sites from machines operating within the State's territory. States insist, in fact, on their sovereignty to control activities which happen in their territory even if these activities are not limited to the national territory,[61] and even if control might be ineffective.[62] Under international law, States can even incur international responsibility if they allow their territory to be used for unlawful activities directed against other States.[63]

In the *CompuServe* case, German law was held applicable to bar access for German users to certain news groups. The consequence was that "German law is dictating what American citizens can read and view."[64] This effect, however, was incidental. It was caused by the inability of CompuServe to tailor its services to the laws of each country in which it operates. There is no need to invoke the reasonableness limitation in this case. No State can seriously be expected to make the application of its penal laws depend on the software of a service provider operating in its territory.[65] Not even CompuServe expected to conduct business in Germany free from the application of German laws.[66] Meanwhile, it seems as though special filtering software could systematically map out specific addresses that contain certain kinds of content.[67]

Under the territoriality principle, it was also permissible for France to force the French campus of Atlanta's Georgia Institute of Technology to translate its Web site into French.[68] The Institute found itself in a Paris courtroom in early 1997. Its Web site displaying course offerings on its French campus was hosted on a French server. Thus, under a 1994 French law, the Web site was required to be in the French language.[69] Similar language laws apply in Quebec.[70]

The territoriality principle, however, would not allow extraterritorial application of national law. An Islamic country, for instance, could legally force a local service provider to comply with a regulation banning access of local users to Salman Rushdie's *Satanic Verses*. But this principle would not cover an order to remove the controversial novel from the Net in general. Therefore, the attempt of a U.S. agency official in August 1996 to apply the Helms-Burton Act to Internet links from Austria to Iran[71] was unlawful under international law.

A U.S. case, *American Library Ass'n v. Pataki*,[72] also demonstrates the limits of the territoriality principle, not on the State versus world level, but on the state versus U.S. level. The court overturned a New York state law protecting children from receiving obscene and indecent material. The practical effect of that statute was that Internet users, in-state or not, were responsible for any posting of such material that New York children could access. According to the court, "Internet users have no way to determine the characteristics of their audience that are salient under the New York ActCage and geographic location."[73] The court determined that the Internet, "analogous to a highway or railroad," was an instrument of interstate commerce and was therefore governed by the Commerce Clause.[74]

b. Nationality Principle

The right of a State to regulate the conduct of its citizens or nationals anywhere in the world is, like territorial jurisdiction, basically noncontroversial.[75] For example, more and more States are outlawing child sex tourism. This makes sexual intercourse with a child punishable for the adult even if the act is tolerated or legal in the country where the act is committed.[76] Insofar as Germany makes even its nationals residing abroad subject to its prohibition against the dissemination of child pornography,[77] it is acting in accordance with international law.

The nationality principle is applicable to juristic as well as to natural persons.[78] As the German branch of CompuServe

Inc., for example, is chartered as a German company, it is subject to German law.[79]

In addition to the territoriality principle, therefore, service providers will in many cases also be subject to jurisdiction under the nationality principle.

c. Effects Principle

The effects principle can be invoked when an act committed in one State causes injury in the territory of another State. Jurisdiction is grounded in the fact that the injurious effect, although not the act or omission itself, occurred in the territory of the State.[80] Controversies may particularly arise where the conduct was lawful where carried out. This principle has been a major source of controversy in antitrust cases where it was invoked to support regulation of activities abroad by foreign nationals because of the economic impact of those activities in the regulating State.[81] As a basis for jurisdiction however, it is increasingly accepted[82] even when its excessive application, especially by the United States, is criticized.[83]

(1) General Approaches

(a) United States v. Thomas

Probably the first cyberspace case where the effects principle was invoked was *United States v. Thomas*.[84] Even though this case is a domestic one, it is important because it addresses some of the issues arising in international cross-border cases. The defendants operated a computer bulletin board system from their home in California. They loaded on their bulletin board images depicting bestiality, oral sex, incest, sadomasochistic abuse, and sex scenes involving urination. Access to the files was limited to members who were given a password after they paid a membership fee and submitted a signed application form that requested the applicant's age, address, and telephone number. An undercover agent was accepted as a member. When the agent downloaded explicit material in Memphis, Tennessee, the defendants were indicted in federal court in Tennessee on several criminal violations.

The defendants challenged the venue in Tennessee, claiming that the criminal actCthe transportation of the materialCdid not occur in Tennessee, but in California. The Sixth Circuit concluded that "the effects of the Defendants' criminal conduct reached the Western District of Tennessee, and that district was suitable for accurate fact-finding."[85] Accordingly, the court found that venue was proper in that judicial district.

During the same month that the Thomases were sentenced in Tennessee, Mr. Thomas was indicted for similar criminal charges in Utah federal court. He argued unsuccessfully that the charges should be dismissed based on collateral estoppel and double jeopardy, stemming from the Tennessee conviction.[86]

With the same theory used by Tennessee and Utah prosecutors, which focussed on where materials were accessed, the defendants could have been indicted in Saudi Arabia, where standards concerning indecency are probably even stricter than in the U.S. At least insofar as international jurisdiction is concerned,[87] it is not clear whether the downloading of files in a certain country makes the sender's activities subject to foreign jurisdiction. However, in Tennessee's *United States v. Thomas*, the defendants knew the jurisdiction in which their files were being accessed, and the downloading could not occur without their approval. The case is no precedent for jurisdiction over a sender's activities based on the random downloading of files that happen to be illegal in certain jurisdictions.

(b) Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.

Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc. [88] is the first published international case addressing multijurisdictional issues in cyberspace. Here, a careful analysis of the scope of the court's jurisdiction was presented. In this trademark case, a publisher offered and distributed sexually explicit photos to netizens, including U.S. customers, from a Web site in Italy. Customers had to subscribe to his service and pay a monthly fee; therefore, the

publisher was aware that his material was entering specific jurisdictions, such as the U.S. The court held that distribution of the materials in the United States was a violation of a fifteen-year-old U.S. court order prohibiting the use of the trademark, "Playmen," in magazines distributed in the United States. It stated:

> The Internet is a world-wide phenomenon, accessible from every corner of the globe. [Defendant] cannot be prohibited from operating its Internet site merely because the site is accessible from within one country in which its product is banned. To hold otherwise "would be tantamount to a declaration that this Court, and every other court throughout the world, may assert jurisdiction over all information providers on the global World Wide Web."[90]

Even though the court concluded that it could not prescribe conduct on the global Internet, it was entitled to prohibit access to the computer sites in the United States.[91] Thus, the defendant was enjoined from offering his magazine to customers residing in the United States.

Insofar as a State limits the domestic effects of a Web site perceived as dangerous to its citizens, it is in accordance with international law. However, that State is not permitted to outlaw the activity completely unless it has jurisdiction based on territoriality, nationality or universality.

The *Playboy Enterprises* Court's differentiated analysis, which considers both national interests and the interests of other nations, is a good model for Internet cases in the international context.

(c) Florida Attorney General

In the matter of jurisdiction over Internet communications, the Florida Attorney General has chosen to throw up his hands and look to the federal government for the regulation of Internet gambling activities.[92] Florida residents are placing bets at "virtual casinos" through the Internet, but their activities cannot be tracked because of the companies' complex encryption techniques and location in foreign jurisdictions.[93] According to the Florida Attorney General, the task of cracking the encryption codes and regulating the Internet is suited, not for the "patchwork attention" of individual states, but for the federal government.[94]

(d) Minnesota Attorney General

On the other end of the spectrum, the broadest approach has been taken by Minnesota Attorney General Humphrey, who circulated a memorandum, entitled "WARNING TO ALL INTERNET USERS AND PROVIDERS," asserting broad jurisdiction over any Internet activity having an effect on Minnesota.[95] The memo
randum argued in favor of personal jurisdiction over anyone "[w]ho transmit[s] information via the Internet knowing that information will be disseminated in Minnesota . . . ."[96]

The Attorney General pointed to the state's general criminal jurisdiction statute, which makes it a crime when a person who, while outside the state, causes a crime to "result" in the state or causes another to commit a crime within the state.[97] He drew an analogy to a classic scenario of international criminal jurisdiction.[98] Just as Minnesota has jurisdiction over someone outside the state who fires a rifle at someone in the state, the argument goes, so Minnesota has the power to enforce its laws against purveyors of on-line fraud.[99] He described the illegality of gambling activities initiated outside the state but made available to Minnesota residents. He also described the correctness of regulation over Native Americans on a reservation who purchased space for political advertisements in a newspaper circulated within Minnesota. The Attorney General stated, "the[se] . . . principles of Minnesota law apply equally to activities on the Internet. Individuals and organizations outside of Minnesota who disseminate information in Minnesota via the Internet and thereby cause a result to occur in Minnesota are subject to state criminal and civil laws."[100]

This approach is broader than that taken in *Playboy Enterprises*,[101] because the sender's knowledge and approval of distribution in a particular jurisdiction is assumed. However, to understand the legal difficulties created by this broad allegation of jurisdiction, it is important to have a closer look at the variety of ways in which the Internet can be used

to disseminate information.

(2) Specific Approaches

(a) E-mail

E-mail is similar to its conventional paper counterpart in that it allows individuals to correspond with one another. Like every other medium, it can be used for criminal activities.[102] Armed with the intended recipient's unique user name and address, the sender of e-mail can compose a message that will be deposited into the recipient's mailbox. The message becomes available to the recipient when she next comes on-line.[103] In principle, e-mail messages are no different from letters and phone calls, as long as the international character of the communication is known to the sender.[104] Whereas it is more or less obvious that an address like "uchicago.edu" belongs to a user who resides in the United States, the address is not always so clear as to the user's residence. An address at a major commercial Internet service could be associated with a user in the United States or abroad.[105] That fact, in turn, raises serious questions about the reasonableness of jurisdiction if the sender is not aware of the recipient's country.

The effects principle is not controversial with respect to acts such as shooting a gun or sending libelous publications across the border.[106] In these cases, the transnational character of the act is normally obvious for the actor. But where the sender of an e-mail message is not aware that the message is received in another country, the situation is different. In this case, there is no link of the activity to the territory of the regulating State and no connection between the regulating State and the sender of the message. The activity is not characterized here by any international contact. The assertion of jurisdiction to prescribe is therefore limited to situations in which it is known or at least foreseeable that substantial effects will occur in another State.

(b) Bulletin Boards

Messages posted to public bulletin boards pose similar questions of jurisdiction. A writer posting messages containing anti-Semitism, racism, or hatred in any form knows or ought to know one thing: copies of the message will ultimately be distributed to Internet sites all over the world. Does this subject a non-German to the German prohibition on importation and distribution of Nazi propaganda[107] on the denial of the Holocaust?[108]

According to the Attorney General of Minnesota there should be no doubt that it does. But his analysis is too short sighted. It imposes an unreasonable burden on the sender of a posting to be aware of criminal liability for his posting in hundreds of different jurisdictions when he cannot control the distribution. Furthermore, it would be technically difficult to exclude certain jurisdictions from the distribution of such postings in such a situation.

According to press reports, many German neo-Nazis have found shelter in the "electronic fortresses" of Bulletin Boards.[109] Hundreds of extreme rightists are reported to be going on-line, using the Internet to access material illegal in Germany—such as anti-Semitic and Holocaust revisionist treatises—and communicate their views of intolerance. Participants appear to know that their activities are prohibited by German penal law. Assuming they know that they are communicating within an identifiable circle of people centered within a particular jurisdiction, the communication resembles more personalized e-mail messages. This is especially true if the group uses a language, such as German, which is not the common Net language. Arguably, the effects in this case are linked closely to a certain country. Consequently, jurisdiction within Germany would be in accordance with international law.

(c) World Wide Web

The Web, a vast decentralized collection of documents containing text, visual images, and even audio clips, poses the greatest problems for international jurisdiction. The Web is designed to be inherently accessible from every Internet site in the world. Information on a Web page resides passively on a particular computer until fetched by a human reader. Even when a Web site's computer can determine the geographical location of the prospective reader's Internet site, that does not disclose the location of the human reader. For instance, a Minnesota resident could place a telephone call to an Internet host in Toronto and browse a Web page through that host without disclosing his Minnesota location.

"Given that simple fact, it is impossible for the owner of a Web site to prevent access by users in a given jurisdiction."[110]

Even if the distributor of *Sports Illustrated Online Swimsuit Edition* is aware that his files are especially attractive for Internet users in Islamic countries where they might be considered indecent, it seems unreasonable to subject this distributor to the decency laws of these countries. The link of the offer to the territory of the regulating State is not obvious. The connection between the regulating State and the distributor is not very convincing. First of all, the distributor will in most cases not even be interested in having his offer spread to exotic countries without a real demand for his products. Additionally, the international commununity would not recognize a State's pure political or ideological interest in regulating the Internet on a global level.

This might be different where the distributor is targeting a certain country with extra efforts. A U.S.-based distributor of Nazi material, prohibited in Germany, could post this material on the Net. He could then start advertising for his Web site by sending flyers indicating how to download the material via regular mail to Germany. Even under these circumstances, offering the material on-line for downloading does not exactly resemble the shipping via regular mail because the sender does not know who precisely gets access to his material. But with these extra efforts the distributor targets a certain country as if he were dropping the material from an airplane. Despite the scattering, most material will arrive at its destination.

It seems to be reasonable and justifiable that a country that is targeted in the described way regulates this conduct, thereby subjecting individuals to its laws.[111] The conduct, however, has to be clearly recognized as criminal by international standards. So the effects principle might under certain circumstances even allow jurisdiction over Web site distributors.

In a U.S. case of targeting, *Panavision International, L.P. v. Toeppen*,[112] the California federal court used an "effects" analysis to determine that it had jurisdiction over an Illinois defendant who used a California company's trademark in a Web site address for the purpose of extorting money. The defendant allegedly searched for trademarks that had not been registered as Internet domain names, registered such trademarks himself, and then demanded money to relinquish his rights.[113]

The court determined that general jurisdiction did not exist over the defendant; he was domiciled in Illinois, and he only travelled to California twice a year.[114] The court found that his activities were not "substantial, systematic, or continuous."[115]

Regarding specific jurisdiction, the court used a three-part test:

> (1) [t]he nonresident defendant must do some act or consummate some transaction with the forum or perform some act by which he *purposefully avails himself* of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws[;] (2) [t]he claim must be one which *arises out of or results from* the defendant's forum-related activities [; and] (3) [e]xercise of jurisdiction must be *reasonable*.[116]

In determining that the defendant had purposefully availed himself of the forum, the court first looked at the nature of the cause of action. It decided that tort theory and an "effects test" should be used, rather than contract theory.[117] The court decided to examine the effects of the defendant's alleged actions because of his intentional targeting of a California company. The court referred to *Data Disk, Inc. v. Systems Technology Assoc.*,[118] in which the court looked at whether communications were intended to cause injury in California.[119] It stated that
the defendant intended to interfere with the plaintiff's business, knowing that the injury would be borne in California, and "expressly aimed his conduct at California."[120] The court distinguished several Internet-related cases[121] because they dealt with defendants who had "legitimate businesses and legitimate legal disputes"; by contrast, the defendant was merely "running a scam directed at California."[122]

The court used a "but for" standard for the second part of the test to find that the defendant would not have been injured but for defendant's registration of the trademarks.[123] For its analysis of the third prong of the test, the court referred to seven factors[124] for measuring whether jurisdiction would comport with "fair play and substantial justice."[125] The court held, under a tort theory, that jurisdiction over the defendant was presumptively reasonable because he had aimed his activities at California residents.[126] Because the defendant failed to overcome the presumption of reasonableness, the court held that the third prong of the test was met.[127]

The reasoning of the court is persuasive, and it would be equally persuasive in an international case. Extorting money from the owner of a trademark has substantial effects in the victim's State. Thus the exercise of jurisdiction to prescribe by this State is reasonable.

d. Protective Principle

The protective principle, found in *Restatement* section 402(3), allows a State to protect its own governmental functions.[128] International law recognizes the right of a State to punish a limited class of offenses committed outside its territory by persons who are not its nationals. "Nearly all states assume jurisdiction over aliens for acts done abroad which affect the security of the state . . . ."[129] These offenses must be generally recognized as criminal by the international community. This is the case for offenses like espionage, counterfeiting of the State's seal or currency, or falsification of official documents.[130] Furthermore hackers who play "wargames" and intrude in national security data systems, or endanger the systems with worms[131] or through other means, face subjection to the jurisdiction of the affected State.[132] Douglas Barnes, a member of the Austin Cyberpunks, even expects that this principle will be invoked against international software piracy rings.[133] The protective principle does not support application to foreign nationals of laws against political expression.[134] Considerations of national security, however, helped the House of Lords, in *Joyce v. Director of Public Prosecutions*,[135] to decide that "an alien who left the country in possession of a British passport owed allegiance and was guilty of treason when he subsequently broadcast propaganda for an enemy in wartime."[136]

States are authorized to prescribe rules to outlaw the above mentioned crimes in cyberspace. Expatriated citizens, and even aliens who oppose a certain regime, cannot be sure that participation in public news groups is not subject to regulation of their native State. This does not necessarily conflict with international human rights. To the contrary, Article 20 of the International Covenant of Civil and Political Rights of December 19, 1966 states:

> 1. Any propaganda for war shall be prohibited by law.
>
> 2. Any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.[137]

To avoid treaty violations due to different concepts of freedom of speech, the United States' adherence to international human rights treaties is regularly accompanied by reservations specifying that the treaty should not promise change in existing U.S. law or practice.[138]

e. Universality Principle

Universality provides for jurisdiction over a crime which customary or conventional law labels so egregious as to be of universal concern. Unlike the other principles of jurisdiction, universality does not require a direct connection such as the place of the offense, the nationality of the offender, or the effects of the offense on the prescribing State. The required connection is more abstract. Universal jurisdiction over the specified offenses is a result of universal condemnation of those activities. They are subject to universal jurisdiction as a matter of customary law or as a matter of international agreements. In the latter case, it remains to be determined whether universal jurisdiction over a particular offense has become customary law for States not party to such an agreement. The doctrine was developed centuries ago to address the piracy that menaced international trade and justified its application by deeming the pirate

hostes humani generi—the enemy of all mankind.[139] Meanwhile, section 404 of the *Restatement* correctly reflects the consensus of the international community.[140] It criminalizes piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and certain acts of terrorism. One might wonder whether any of these crimes might be committed in cyberspace. However, according to Article III
of the Convention on the Prevention and Punishment of the Crime of Genocide of December 9, 1948, the following acts shall be punishable under the universality principle:

> (a) Genocide;
>
> (b) Conspiracy to commit genocide;
>
> (c) Direct and public incitement to commit genocide;
>
> (d) Attempt to commit genocide;
>
> (e) Complicity in genocide.[141]

Whoever cruises the Net for a while will not have many difficulties discovering Web sites which at least give rise to a statutory interpretation of "[d]irect and public incitement to commit genocide."[142] Especially in regions where war is being waged, it should also be possible to prove that people are serious about hate messages—that is they really want genocide to happen. These acts may be outlawed by any State—even without one of the earlier discussed bases of jurisdiction to prescribe.

The acts listed in Article III of the Genocide Convention are also listed in Article 4, section 3 of the Statute of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law in the Territory of the Former Yugoslavia.[143] Article 7 of the Statute of the International Tribunal for Yugoslavia states the individual responsibility for aiding and abetting in the planning, preparation, or execution of crimes outlawed by this statute.[144] Thus, violating the statute not only subjects a perpetrator to the jurisdiction of all member states of the United Nations, but also to the jurisdiction of the organization itself.

B. Jurisdiction to Adjudicate

Jurisdiction to adjudicate is defined as a State's authority to subject persons or things to the process of its courts or administrative tribunals, whether in civil or in criminal proceedings, whether or not the State is a party to the proceedings.[145] It requires a sufficient or reasonable relation with the forum State.[146] The *Restatement* formulates this criteria in section 421 as follows:

> (1) A state may exercise jurisdiction through its courts to adjudicate with respect to a person or thing if the relationship of the state to the person or thing is such as to make the exercise of jurisdiction reasonable.[147]

The fact that an exercise of jurisdiction to adjudicate is reasonable does not mean that the forum State has jurisdiction to prescribe in respect to the subject matter of the action. "Conversely, there may be circumstances in which a State has jurisdiction to prescribe but jurisdiction to adjudicate is absent or doubtful."[148] Especially in criminal cases, jurisdiction to adjudicate is rarely exercised in the absence of jurisdiction to prescribe by the same State, because courts rarely apply the criminal laws of other States.[149]

According to subsection (2) of section 421, a state's exercise of jurisdiction to adjudicate is generally reasonable, if at the time jurisdiction is asserted:

> (a) the person or thing is present in the territory of the state, other than transitorily;
>
> (b) the person, if a natural person, is domiciled in the state;

(c) the person, if a natural person, is resident in the state;

(d) the person, if a natural person, is a national in the state;

(e) the person, if a corporation or comparable juridical person, is organized pursuant to the law of the state;

(f) a ship, aircraft or other vehicle to which the adjudication relates is registered under the laws of the state;

(g) the person, whether natural or personal, has consented to the exercise of jurisdiction;

(h) the person, whether natural or juridical, regularly carries on business in the state;

(i) the person, whether natural or juridical, had carried on activity in the state, but only in respect of such activity;

(j) the person, whether natural or juridical, had carried on outside the state an activity having a substantial, direct, and foreseeable effect within the state, but only in respect of such activity; or

(k) the thing that is the subject of adjudication is owned, possessed, or used in the state, but only in respect of a claim reasonably connected with that thing.[150]

In international criminal cases, jurisdiction to adjudicate depends almost exclusively on presence of the accused. In international civil cases, the principle of "*actor sequitur forum rei*" [Plaintiff follows defendant to the latter's forum] can be regarded as a principle accepted virtually everywhere.[151] It is important to note that the international law standard for civil cases—reasonableness—differs significantly from the U.S. "minimum contacts" standard, which was crafted in *International Shoe v. Washington* and serves as the basis for deciding jurisdictional questions in the U.S.[152] Transitory presence, for example, is not a sufficient basis for the exercise of jurisdiction to adjudicate under international law[153] even though "tag" jurisdiction is in accordance with U.S. law.[154] One federal court even held that the temporary presence of a person within the airspace of a state while on board a commercial aircraft established jurisdiction.[155] As a matter of principle, international law requires closer pre-litigation contacts between the defendant and the forum State than would be necessary in domestic cases.[156] This is due to the fact that a foreign nation presents a higher sovereignty barrier than another state within the United States. U.S. courts generally agree upon this concern for other nations' sovereignty.[157]

International cyberspace cases that call for international law principles relating to jurisdiction, however, are rare. For guidance, then, we extrapolate from interpretation of the "minimum contacts" standard in domestic cases. That interpretation is a starting point for determining how to apply "reasonableness" in the international context.

Internet-related questions involving jurisdiction have been most common in U.S. courts, primarily because of the multijurisdictional character of the country. U.S. courts have taken various approaches to this jurisdictional issue. It is helpful to separate these approaches into two categories: moderate and expansive. The moderate approach is more consistent with the "reasonableness" standard of international law and is a better model for international multijurisdictional cases.

1. Moderate Approach

Nine domestic courts so far have taken a moderate approach that is consistent with an international "reasonableness" standard. One court refused to find jurisdiction based solely on the existence of a Web site where it was not established that the Web site was accessed by citizens of the forum state.[158] Another court refused to find jurisdiction where the contents of a Web site were unrelated to the cause of action.[159] In the other seven cases, the accessibility of a Web site within the state was not an adequate basis for jurisdiction.[160] In two out of these seven cases, jurisdiction

based solely on Internet advertising was denied.[161] In four cases, more than Internet advertising was involved.[162] The courts upheld jurisdiction because of numerous intentional contacts to the forum state. In a final case, jurisdiction was denied where the only contact with the forum state was the location of a database.[163]

a. Smith v. Hobby Lobby Stores, Inc.

In a domestic case with an international twist, an Arkansas federal court refused to find jurisdiction over a Chinese company based on an on-line advertisement. *Smith v. Hobby Lobby Stores, Inc.*[164] involved liability for wrongful death from a house fire allegedly caused by a Christmas tree. The Chinese company manufactured the trees and distributed them to an Arkansas company. The plaintiffs claimed in part that the defendant had significant contacts with Arkansas through Internet advertising.[165] The defendant's advertisement was contained in an on-line Hong Kong trade magazine and the distributor received a monthly hard copy of the magazine. The defendant claimed that its name was not part of the Internet address and that the advertisement was not directed toward Arkansas and probably never even found its way to Arkansas.[166] The court agreed with the defendant's additional assertion that a finding of jurisdiction would result in worldwide jurisdiction. Citing *CompuServe*[167] and *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*,[168] the court stated that the alleged contact with Arkansas was insufficient because the defendant did not contract to sell goods or services to any state citizens over the Internet.[169]

It would have been clearly out-of-bounds for the judge to base jurisdiction on a Web site that was probably never even accessed by Arkansas citizens. The more interesting question, therefore, is whether evidence of access by a forum state, and, in turn, prospective plaintiffs is a workable test for jurisdiction.

b. McDonough v. Fallon McElligott, Inc.

In *McDonough v. Fallon McElligott, Inc.*,[170] a California federal court held that the existence of a public Web site used by Californians could not, by itself, establish jurisdiction.[171] The plaintiff, a California sports photographer, sued Missouri defendants on copyright claims for reproducing a photo of basketball player Charles Barkley for use in a magazine and submission to a national advertising awards contest.[172] The plaintiff argued that the Web site's accessibility by Californians allowed him to sue the defendant for issues wholly unrelated to the content of the Web site. This argument, however, was rejected.[173] The Court stated, "because the Web enables easy world-wide access, allowing computer interaction via the [W]eb to supply sufficient contacts to establish jurisdiction would eviscerate the personal jurisdiction requirement as it currently exists."[174] Also, the defendants' alleged contacts with California—advertising, the use of independent contractors, and nationwide distribution of the magazine—were not sufficiently related to the reproduction of the photo to warrant personal jurisdiction.[175]

In fact, a contrary decision, if applied on the international level, would have disturbing consequences for the international order—and the domestic case load—if any foreign company could be haled into a U.S. court based simply on the accessibility of its Web site. No U.S. company with a Web site could complain then, if as a countermove, it found itself subjected to some exotic jurisdiction on the other side of the world, even if its business was a Mom-and-Pop convenience store servicing a six block radius in Smalltown, America.

c. Hearst Corp. v. Goldberger

In *Hearst Corp. v. Goldberger*,[176] the New York federal court opposed nationwide jurisdiction over the Internet as contradicting traditional notions of fair play. The plaintiff, owner of *Esquire* magazine, sued a New Jersey attorney for using the Internet domain name, "ESQWIRE.COM," to advertise legal information services to New Yorkers. The services were not yet available at the time of the advertising. The Web site was accessible to, and visited by, New Yorkers.[177] Expressly declining to follow other courts' more expansive notions of jurisdiction over the Internet,[178] the court stated:

Where, as here, defendant has not contracted to sell or actually sold any goods or services to New Yorkers, a finding

of personal jurisdiction in New York 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 nor acceptable to the Court as a matter of policy.[179]

The court likened the defendant's Web site to a national magazine advertisement that targeted New York, which would be insufficient to establish jurisdiction.[180] Likewise, "ESQWIRE" e-mails sent to New York residents were insufficient because they were analogous to letters or telephone calls.[181] Jurisdiction for a tortious act committed in New York did not exist because the alleged "offer for sale" was posted on the Internet, and was not made within the state.[182] Neither did jurisdiction exist for a tort committed from outside the state because the defendant did not derive enough revenue from New York.[183]

The *Hearst* court obviously saw the international implications of a contrary decision. It wanted to avoid setting a precedent that would permit international jurisdiction over operators of foreign Web sites in every dispute involving New York residents.

d. Bensusan Restaurant Corp. v. King

Although *Bensusan Restaurant Corporation v. King*[184] differs factually from *Hearst*, the two are similar because jurisdiction in New York was denied in both. In *Hearst*, New Yorkers were likely to be interested in the advertised services, although these services were not yet available. In *Bensusan*, by contrast, few New Yorkers were likely to be interested in flying to Missouri for an evening in a jazz club.

The New York federal court in *Bensusan* held that the creation of a Web site, without more, was not sufficient for personal jurisdiction.[185] The plaintiff alleged that the defendant violated its trademark for a New York jazz club, "The Blue Note," by using the name for his Missouri club and posting a similar logo and information about the club on a Web site with unrestricted access.[186] To obtain tickets to the club, a person would call the Missouri telephone number listed on the Web site and pick up the tickets in Missouri.[187] Thus, except for accessing the Web site, the whole transaction would occur in Missouri. Refusing to extend the "stream of commerce" concept,[188] the court stated, "[c]reating a site, like placing a product into the stream of commerce, may be felt nationwide—or even worldwide—but, without more, it is not an act purposefully directed toward the forum state."[189] The court found that the creation of the Web site did not amount to targeting New York for business: "The mere fact that a person can gain information on the allegedly infringing product is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product in New York."[190] *Bensusan* distinguished *CompuServe, Inc. v. Patterson*,[191] in which an Internet user "specifically targeted" Ohio by subscribing to a network service based there, entering into a separate agreement with the service to market his software, advertising through the service, and sending his software to the service.[192]

Bensusan, as well as *Hearst*, reflects a cautious judicial approach which seems to have not only domestic, but also international multijurisdictional, cases in mind.

e. CompuServe, Inc. v. Patterson

CompuServe, Inc. v. Patterson[193] goes a step beyond *McDonough, Hearst* and *Bensusan* because it describes a factor needed beyond the mere existence of computer communications for personal jurisdiction: a contract. The Sixth Circuit allowed an out-of-state subscriber to be sued in Ohio because of his electronic communications directed toward the state.

The defendant, who owned a software company and lived in Texas, contracted with the Ohio-based CompuServe to market his software to other CompuServe subscribers nationwide.[194] The agreement was entered into in Ohio and was subject to Ohio law.[195] The defendant transferred thirty-two software files to CompuServe and advertised them on the

system.[196] When CompuServe began to market similar software on-line, the defendant accused the company of trademark infringement.[197]

In its jurisdictional analysis, the court determined that the defendant had purposefully availed himself of the state through three years of repeated contacts with the state and his use of CompuServe both to provide and market his software in Ohio and elsewhere.[198] The court also stated:

> Admittedly, merely entering into a contract with CompuServe would not, without more, establish that Patterson had minimum contacts with Ohio. By the same token, Patterson's injection of his software product into the stream of commerce, without more, would be at best a dubious ground for jurisdiction. Because Patterson deliberately did both of those things, however, and because of the other factors that we discuss herein, we believe that ample contacts exist to support the assertion of jurisdiction in this case, and certainly an assertion of jurisdiction by the state where the computer network service in question is headquartered.[199]

The court concluded:

> [Defendant] has knowingly made an effort—and, in fact, purposefully contracted—to market a product in other states, with Ohio-based CompuServe operating, in effect, as his distribution center. Thus, it is reasonable to subject [him] to suit in Ohio, the state which is home to the computer network service he chose to employ.[200]

Consistent with its holding that computer communications alone were insufficient to warrant jurisdiction, the court declined to extend its holding of jurisdictional sufficiency to, for example, an Ohio suit by CompuServe against a "regular subscriber" living in another state "even if the subscriber is a native Alaskan who has never left home."[201] It also declined to extend the holding to a suit in an Ohio court by a party from a third state over a computer virus, or to a suit in any state where the defendant's software was purchased or used.[202]

This well-reasoned decision, which does not overemphasize electronic contacts, might also be a model for international multijurisdictional cases.

f. EDIAS Software Int'l, L.L.C. v. BASIS Int'l Ltd.

In a similar case, the Arizona federal court in *EDIAS Software International, L.L.C. v. BASIS International Ltd.*[203] established jurisdiction in a defamation action. In its analysis of defamation allegations under the first part of an "effects" test similar to that in *California Software*,[204] the court stated:

> The Central District of California concluded that a similar allegedly libelous statement circulated in a computer forum established jurisdiction based on the foreseeable injury felt in the forum state. This court . . . agrees . . . that [defendant] should not be permitted to take advantage of modern technology through an Internet Web page and forum and simultaneously escape traditional notions of jurisdiction.[205]

Regarding the second part of the test, the court found that allegedly defamatory statements posted on the Web page, a contractual relationship between the parties, and the defendant's contract-related activities in Arizona constituted purposeful availment.[206] Of the seven reasonableness factors which the court used, as in *California Software*,[207] the second and third factors are the most important in the context of international jurisdiction. Although the court basically treated the case as a domestic one, it recognized the jurisdictional conflicts resulting from a foreign defendant in a U.S. court. The court looked at the burden of defendant to litigate in Arizona, noting that the distance a foreign defendant must travel and its unfamiliarity with laws should be considered.[208] It determined that the defendant would not have to travel far, apparently because the defendant had signed the contract in New Mexico and agreed to be subject to New Mexico law. The court also decided that
the defendant would be sufficiently familiar with federal law. Although the court ultimately found that the third factor,

involving sovereignty conflicts, was not a bar to the exercise of jurisdiction, it acknowledged that such conflicts can arise when a defendant resides in a foreign country.[209] The court stated, "[s]overeignty issues arise when a defendant resides in a foreign country such that concerns about conflicts with the home State's sovereignty relate to the possible results of litigation."[210] Therefore, in an international case, the result could have been different under the same facts and in the same forum.

The first factor of the court's "reasonableness" test—the purposeful availment factor—was of the most substantive importance to the court: "[t]he visits and the many phone, fax, and e-mail communications that [defendant] made to Arizona, in addition to . . . invoices . . . sent to Arizona, and the allegedly defamatory statements indicate that [defendant] purposefully availed itself of the benefits and protections of Arizona."[211]

The court resolved the fourth factor, Arizona's interest in adjudicating the dispute, in favor of the plaintiff. It pointed to the plaintiff's local address; defendant's knowledge of the address; and other activity within the state, including billing, receiving payment, visiting plaintiff, and contacting plaintiff by telephone, fax, and e-mail.[212] Regarding the last three factors relating to the efficiency, convenience, and importance of the forum and the existence of an alternate forum, the court determined that Arizona would be most convenient for the plaintiff, although New Mexico was an alternate forum.[213]

Not all of the policy considerations are convincing on the international level. However, the intentional contacts of the defendant with the forum state went beyond fortuitous communication on the Internet and reached a level that justifies the exercise of jurisdiction.

g. Resuscitation Technologies, Inc. v. Continental Health Care Corp.

As opposed to *EDIAS*, where the defendant visited the forum state, the Indiana federal court in *Resuscitation Technologies, Inc. v. Continental Health Care Corp.*[214] had to resolve jurisdiction based more strongly on on-line communications. Multiple communications across state lines—e-mail, phone, and fax—were enough to satisfy an Indiana federal court that direct communications, rather than those involving third parties, were at issue in jurisdiction over the defendant. The defendants learned about the plaintiff, a start-up Indiana company in need of capital, through its Web site. The defendants requested information via e-mail, and a flurry of correspondence ensued, including eighty e-mail messages.[215] Additionally, two meetings were held in other states. The parties were negotiating a joint venture calculated to satisfy a creditor of the plaintiff and make an initial public offering in return for acquisition of patent rights.[216] The parties signed confidentiality agreements during the negotiations. When the negotiations soured and the defendants refused to be bound by the confidentiality agreements, the plaintiff brought a declaratory action for lack of a contractual relationship, breach of the confidentiality agreements, tortious interference, and conversion.[217]

The court examined whether the defendants had transacted business in Indiana. It stated:

> [T]his notion of transacting business over the Internet involves examining the level of interactivity, and the commercial nature of the exchange of information that occurs. The quality of those electronic contacts is measured with reference to the intended object of that activity. . . .[Especially when] the dispute is about whether or not a contract was formed between two parties by reason of their use of the Internet or other electronic transmissions. . . . [A] . . . factual inquiry . . . requires a direct examination of the nature and content of . . . Internet communications. . . .[218]

The court focused not on "who started it,"[219] but on the level of Internet activity involved. It opined that "one or two inquiries about some Indiana goods or services would not support local jurisdiction."[220] In this case, however, a continuing and long-term relationship was contemplated. As a consequence, the e-mail messages were numerous and continuous over a period of months.[221]

Citing *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*[222] for its "intended object" analysis,[223] the court found that the initial Internet solicitation and e-mail response, and the ensuing communications were focused on Indiana and

showed that the defendant's "intended objects" of the contacts were "to transact business and develop the business" in Indiana.[224] Furthermore, the plaintiff's cash-poor status made it more difficult to travel for litigation. The court made a policy decision to adjudicate disputes involving small, in-state companies seeking capital so that such companies would not have to fear litigation in other states.

Similar to *CompuServe*, this court did not overvalue the electronic contacts, but rather seemed to base its decision on a bundle of other factors. The factors included signed agreements, meetings, faxes, and, particularly, the contemplation of a long-term relationship to transact business in the forum state. However, the court's weighing of the ability of poor plaintiffs to litigate outside the state is pure protectionism and highly problematic as a legal rule on the international level. It would mean that every destitute Third World plaintiff who sued an American company would always have the home court advantage.

h. Hall v. LaRonde

Unlike *EDIAS* and *Resuscitation Technologies*, the California court in *Hall v. LaRonde*[225] was faced with business transactions conducted exclusively over the Internet and telephone lines. The plaintiff provided sales and technology services for the defendant, a New York company selling computer software. The parties contracted for continuing obligations, such as continuing royalty payments to the plaintiff. They had an ongoing relationship regarding the development of a software module. The plaintiff performed all services in California and communicated with the defendant only by e-mail and telephone; he had no other connections with New York. Under these circumstances, the court was satisfied with electronic contacts as the basis for a finding of minimum contacts. The court stated, "[t]he speed and ease of [electronic] communications has increased the number of transactions that are consummated without either party leaving the office. There is no reason why the requisite minimum contacts cannot be electronic."[226]

Under the facts of this case, the court's decision is sound. In other cases, though, careful attention must be given to the facts, to prevent findings of worldwide jurisdiction based on the existence of even automatic electronic communications with a forum state.[227]

i. Pres-Kap, Inc. v. System One, Direct Access, Inc.

Even the existence of a contract for computer services from a Miami database was not enough to call a New York company into a Florida court. In *Pres-Kap, Inc. v. System One, Direct Access, Inc.*,[228] the New York defendant, a travel agency, negotiated a contract for computer database services with a Delaware corporation through its New York branch office. The contract provided for on-line access to plaintiff's Miami database.[229]

The court analyzed the travel agency's contacts under the minimum contacts, "arising out of," and fairness considerations of personal jurisdiction. It determined that the transaction was based in New York, not Florida. Regarding the issue of fairness, the court stated:

> Based on the trial court's decision, below, users of such "on-line" services could be haled into court in the state in which supplier's billing office and database happen to be located, even if such users, as here, are solicited, engaged, and serviced entirely instate by the supplier's local representatives. Such a result, in our view, is wildly beyond the reasonable expectations of such computer-information users.[230]

In fact, the contacts to Miami were fortuitous because the database might even have been located abroad—for tax reasons or cheaper labor—without necessarily influencing the parties' contractual relationship. Thus, the court's decision was sound in looking at the basis of the transaction rather than the source of electronic contacts.

2. Expansive Approach

A hint of international jurisdictional issues central to this analysis was present in *State v. Granite Gate Resorts, Inc.*[231] However, *Granite Gate Resorts* was litigated too soon for international issues to arise; the defendants were preparing to operate their computer service from Belize, but they had not yet done so at the time of suit.

Although such issues were not directly resolved, this court and others have expanded their jurisdictional reach into cyberspace. The cases demonstrate approaches that move toward a rule calling for jurisdiction over a defendant in all states based on the accessibility of the defendant's Web site by users in all states. If this rule was adopted internationally, a defendant would be subject to the jurisdiction and differing laws of every State worldwide.

a. California Software, Inc. v. Reliability Research, Inc.

The California federal court in *California Software, Inc. v. Reliability Research, Inc.*[232] exemplifies both a moderate approach and an expansive approach to jurisdiction. The case involved the effects on a state of a national bulletin board posting. The defendants wrote messages to three companies via a bulletin board and communicated with three California residents via telephone and letter, saying that the plaintiffs' right to market software was in question.[233]

The court took a moderate approach in determining that general jurisdiction did not exist due to lack of sufficient contacts with California. The defendants were not located in California. The corporate defendant did not have offices or otherwise conduct business within the state except to communicate with California users through the national bulletin board.[234] The court stated, "[t]he mere act of transmitting information through the use of interstate communication facilities is not . . . sufficient to establish jurisdiction over the sender."[235]

The court's decision to find limited jurisdiction over the defendants was more expansive. It followed a three-part test from *Data Disc, Inc. v. Systems Technology Associates, Inc.*,[236] a case that dealt with the effect of a long-distance telephone call. Under the first part of the test, which looks at a defendant's "purposeful availment" of the forum state, the court chose to look at whether the defendants intended to cause injury in California. It stated, "[d]efendants made tortious statements which, though directed at third persons outside California, were expressly calculated to cause injury in California."[237] Regarding whether the defendant engaged in a "forum-related activity"—the second part of the test—the court found that "intentional `manipulation' of third persons who thereby refrain from consummating a contemplated transaction in California" was sufficient.[238] The court stated:

> Unlike communication by mail or telephone, messages sent through computers are available to the recipient and anyone else who may be watching. Thus, while modern technology has made nationwide commercial transactions simpler and more feasible, even for small businesses, it must broaden correspondingly the permissible scope of jurisdiction exercisable by the courts.[239]

The court looked at the third part of the test, a seven-factored "reasonableness"[240] test.[241]

Most significantly under this "reasonableness" analysis, the court found that the defendants had "purposefully injected themselves into California through third parties [even though they] did not induce reliance in California itself through the [computer] message."[242]

The first part of the *Data Disc* test is workable because of the court's focus on whether there was express intent to cause injury within the jurisdiction. The second part of the test, however, is too expansive because of the lack of foreseeability. Any defendant who posts information on the Internet could be seen as engaging a potentially vast audience in a "forum-related activity" within the states. The third part of the test—the "reasonableness" factors—is problematic because it allows a court to invoke jurisdiction under a host of different factual situations, using broad discretion. In the international context, any State wishing to protect its nationals could decide that jurisdiction existed under these factors. For instance, the burden on the defendant could routinely be given less weight than the State's interest in deciding the case. Only if the question of a defendant's "purposeful interjection" into the State were limited to communications directed toward a particular jurisdiction would a State have less than complete worldwide jurisdiction. In the international context, States treat each other as equal sovereigns, and they collectively determine international law. Thus, it is unlikely that States will agree upon such a vague formula when the interests of their nationals are at stake.

b. Digital Equipment Corp. v. AltaVista Technology, Inc.

In *Digital Equipment Corp. v. AltaVista Technology, Inc.*,[243] the Massachusetts federal court used a moderate approach to find jurisdiction based on more than a contract; in dicta, it took a more expansive approach on the issue of jurisdiction based on Web site advertising alone. After the plaintiff bought a California defendant's rights to the trademark "AltaVista" and then licensed back certain rights, the plaintiff sued the defendant for infringement. The licensing contract included a Massachusetts choice-of-law clause.[244] Additionally, the defendant's Web site was accessible to Massachusetts residents, the defendant advertised and solicited sales through the Web site, and the defendant made at least three sales to Massachusetts residents, and the alleged infringement occurred on the Web site.[245] The court rejected the argument that the defendant's advertising was only general, and not directed toward Massachusetts residents; it concluded that the Web site was integral to the contract with the Massachusetts company and to the cause of action.[246]

The court stated:

> I cannot ignore the fact that the medium through which many of the significant Massachusetts contacts occurred is anything but traditional; it is a site in cyberspace, a Web-site. . . .
>
> The Internet has no territorial boundaries. To paraphrase Gertrude Stein, as far as the Internet is concerned, not only is there perhaps "no there there," the "there" is *everywhere* where there is Internet access. When business is transacted over a computer network via a Web-site accessed by a computer in Massachusetts, it
> takes place as much in Massachusetts, literally or figuratively, as it does anywhere. . . .
>
> . . . To impose traditional territorial concepts on the commercial uses of the Internet has dramatic implications, opening the Web user up to inconsistent regulations throughout fifty states, indeed, throughout the globe.[247]

Under a "due process" analysis, the court found that the claim arose out of Massachusetts through the contract and subsequent maintenance of the Web site.[248] It also determined that the defendant purposefully availed itself of Massachusetts by violating the plaintiff's rights with a Web site that it knew would "plainly . . . attract Massachusetts residents."[249] Finally, the exercise of jurisdiction was reasonable because the defendant's travel would not be overly burdensome, Massachusetts had an interest because the trademark infringement occurred there, the venue was convenient to the plaintiff, and the parties had agreed to a choice-of-law provision.[250] The court additionally stated:

> [I]t . . . troubles me to force corporations that do business over the Internet, precisely because it *is* cost-effective, to now factor in the potential costs of defending against litigation in each and every state. . . . On the other hand, it is also troublesome to allow those who conduct business on the Web to insulate themselves against jurisdiction in every state, except in the state (if any) where they are physically located.[251]

In dicta, the court indicated how it would rule on a jurisdictional question involving only advertising on a Web site. Importantly, it stated that the defendant's knowledge of the Web site's accessibility to Massachusetts residents was sufficient to show that the site was directed toward them. It stated that the defendant had continuous contacts with the state through the Web site's twenty-four hour availability to Massachusetts residents. Furthermore, the court noted that software sold to Massachusetts residents could be transmitted directly through the Internet.[252]

Despite the court's concern over possible worldwide jurisdiction, it set a dangerous precedent. Obviously, the court overlooked the fact that resolutions to such complex problems are not simply black or white. Compromise solutions, as evidenced by other court decisions, are possible between the extremes of permitting worldwide jurisdiction based solely on Internet advertising, and denying jurisdiction in forum states other than where the defendant is physically located.

c. State v. Granite Gate Resorts, Inc.

An even more expansive approach was taken in a case involving a public Web site which advertised, but did not sell, gambling services. In *State v. Granite Gate Resorts, Inc.*,[253] the Minnesota District Court found gambling advertising on a Web site was aimed at residents in Minnesota, where gambling is illegal. The defendant corporation was formed in Nevada and the gambling service had not yet been activated at the time of the suit, but the defendants' intent was to offer the service from a server located in Belize.[254]

If the Attorney General had waited until the server was operational, the case would have involved international law issues central to this analysis.[255] Although the business had been set up in Nevada, a state that allows gambling, the defendants were planning to run the operation from Belize. The defendants, therefore, wanted to run a foreign business for purposes of U.S. law. This indicates that they believed international laws to be more favorable to its business interests, and to the outcome of U.S. litigation.

The court conducted a traditional domestic personal jurisdiction analysis. Regarding the quality of the defendants' contacts with Minnesota, the court discussed *Inset Systems, Inc. v. Instruction Set, Inc.*,[256] in which the court found jurisdiction in Connecticut because advertising and dissemination of a toll-free number via the Internet was available in all states, including Connecticut.[257] The court in Minnesota stated:

> [T]he computer hits on Defendants' Web sites and the fact that the advertisements give consumers phone numbers to call, along with the fact that the Court has determined WagerNet's mailing list includes Minnesota residents, are more than sufficient evidence that Defendants have made a direct marketing campaign to the State of Minnesota. Therefore, it is not unforeseen nor unreasonable to Defendants to be required to come to Minnesota to defend themselves particularly when the Defendants have said that they have the option for any of the customers of WagerNet with whom they have a dispute to sue them in Minnesota.[258]

In response to the defendants' argument that Minnesota residents, not they, made the illegal computerized gambling transmissions, the court analogized *Playboy Enterprises*,[259] in which responsibility was placed on a computer service for inviting users to download images onto their computers.[260]

The court found that the nature and quality of defendants' contacts were sufficient because the defendants maintained a Web site for the purpose of soliciting business from Internet users, including Minnesota residents.[261] Furthermore, the Minnesota Attorney General had the right to pursue violations involving gambling solicitations of in-state residents.[262] The court found that a consumer fraud action involving Minnesota residents could only lie in Minnesota and was appropriate because the defendants "crossed the Minnesota borders through Internet advertisements."[263] Also, Minnesota was more convenient than Belize; the defendants told their customers that they were subject to suit in either their home states or Belize.[264]

Finally, defendants had minimum contacts with the state due to their continuous advertisement on the Internet and their notice to prospective customers of suits in their home forum or in Belize.[265]

The court took an expansive approach in determining that the defendants had sufficient contacts with Minnesota because Minnesota residents accessed their Web site. By contrast, in *California Software, Inc., v. Reliability Research, Inc*.[266] the defendants conveyed information to third parties for the specific purpose of harming the plaintiffs. Here, residents could download information directly from the defendants' Web site without the defendants' specific intent to target them.

It is questionable whether the mere accessibility of a Web site has the substantial, direct, and foreseeable effect within this jurisdiction which is required by section 421(2)(j) of the *Restatement*. At least on the international level, it is not sufficient for a State to simply refer to the nature of the Internet as a way of decreasing the requirements for a

reasonable exercise of jurisdiction:

> The Defendants attempt to hide behind the Internet and claim that they mailed nothing in Minnesota, sent nothing to Minnesota, and never advertised in Minnesota. This argument is not sound in the age of cyberspace. Once the Defendants place an advertisement on the Internet, that advertisement is available 24 hours a day, seven days a week, 365 days a year to any Internet user until the Defendants take it off the Internet.[267]

This accessibility argument might even justify jurisdiction over the editor of the *Sports Illustrated Online Swimsuit Edition* in courts of any Islamic country with strict decency rules, if two of the top 500 users are from the forum state.[268]

d. Heroes, Inc. v. Heroes Foundation

In *Heroes, Inc. v. Heroes Foundation*,[269] the District of Columbia federal court seemed to be more inclined to follow *Inset Systems*[270] over *Bensusan*[271] in finding personal jurisdiction over the defendant in a trademark infringement and unfair competition case between two charities. It pointed to a newspaper advertisement published in the Washington Post and "the defendant's home page on the Internet, which is always available to District residents."[272] The defendant relied on *Bensusan*, the decision of a New York federal district court.[273] The court noted that the Connecticut federal court in *Inset Systems* took the opposite view.[274] It concluded:

> Because the defendant's home page is not the only contact before the Court . . . the Court need not decide whether the defendant's home page by itself subjects the defendant to personal jurisdiction in the District. In weighing the importance of this particular contact, however, the Court notes that the defendant's home page explicitly solicits contributions, and provides a toll-free number for that purpose. The home page also contains the defendant's allegedly infringing trademark and logo, the subject of the plaintiff's underlying claims. And the home page is certainly a sustained contact with the District; it has been possible for a District resident to gain access to it at any time since it was first posted.[275]

Although the court did not directly follow *Inset Systems*,[276] it was influenced by the reasoning; thus, it is subject to the same criticisms.

e. Zippo Manufacturing Co. v. Zippo Dot Com, Inc.

Unlike in *Heroes*, the Pennsylvania federal court in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*[277] focused on computer advertising and sales. Contracts with service providers and sales to consumers relating to Internet usage in Pennsylvania tipped the balance for the court. The manufacturer of Zippo lighters sued a California Internet news service for using domain names such as "zippo.com."[278] The defendant had no physical presence in Pennsylvania, but it operated a Web site advertising its services which was accessible to Pennsylvania residents. Additionally, the defendant sold 3,000 passwords over the Internet to state subscribers and entered into seven contracts with Pennsylvania access providers.[279]

The court framed the relevant inquiry: "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdictional principles."[280]

The court classified the case as a "doing business over the Internet"[281] case similar to *CompuServe*.[282] Regarding purposeful availment, the defendant argued unsuccessfully that it was advertising and merely operating a Web site and that its contacts were "fortuitous."[283] The court found that the defendant repeatedly processed residents' applications and assigned passwords knowing that this would result in the influx of electronic messages into Pennsylvania. It concluded that, rather than merely advertising on the Internet, the defendant was engaging in

"electronic commerce." Furthermore, even though the defendant's sales to Pennsylvania subscribers constituted only two percent of its total sales, the court concluded that even one sale would have been sufficient as a forum-related activity.[285] The court decided that the cause of action arose in Pennsylvania because much of the alleged infringement, dilution, and injury arose in Pennsylvania, where the plaintiff was located. Additionally, the exercise of jurisdiction was reasonable, in the court's view, because Pennsylvania had a strong interest in resolving suits over trademark infringement of resident corporations and because the plaintiff's choice of forum was entitled to respect, especially because the defendant chose to conduct business in Pennsylvania.[286]

The court's guiding principle that jurisdiction depends on the nature and quality of commercial activity is surely fair and reasonable. However, applying the principle so that a Web site advertisement and a single sale in the forum state are sufficient is incompatible with the international "reasonableness" standard.

f. Inset Systems, Inc. v. Instruction Set, Inc.

The Connecticut federal court in *Inset Systems, Inc. v. Instruction Set, Inc.*[287] expanded its jurisdictional reach to out-of-state defendants who advertised via the Internet. The plaintiff sued the defendant for trademark infringement based on the defendant's use of "Inset" in its Internet domain address. The defendant, a Massachusetts corporation, had no employees or offices in Connecticut, nor did it regularly conduct business there.[288] In finding jurisdiction over the Massachusetts defendant, the court stated:

> [Defendant] has been continuously advertising over the Internet, which includes at least 10,000 access sites in Connecticut. Further, unlike hard-copy advertisements . . . , which are often quickly disposed of and reach a limited number of potential consumers, Internet advertisements are in electronic printed form so that they can be accessed again and again by many more potential consumers.
>
> The court concludes that advertising via the Internet is solicitation of a sufficient repetitive nature to satisfy [Connecticut's long-arm statute] . . . .[289]

It found that the defendant could reasonably anticipate being haled into Connecticut court because it directed its advertising activities and its toll-free number toward all states, including Connecticut.[290] Furthermore, the court found that it was fair to decide the dispute in Connecticut because the distance between Connecticut and Massachusetts was "minimal."[291]

Under the court's approach, a defendant who advertises via the Internet is subject to jurisdiction in every forum from which users have Internet access. The concern with distance between the forum state and the defendant's location is of little help in the international context for bordering states. A citizen of a small country surrounded by many other countries would be subject to a multitude of jurisdictions. Even on the U.S. level, this argument would enable a Mexican court in Juarez to hale an El Paso resident who allegedly violated a Mexican law by posting a message criticizing corruption in the Mexican government. Ironically, under the court's analysis, the writer of a newspaper article voicing the same criticism might not be subject to a foreign jurisdiction because of the more limited dissemination of hard-copy media.

g. Maritz, Inc. v. Cybergold, Inc.

Unlike *Inset Systems*, not even proximity was required in *Maritz, Inc. v. Cybergold, Inc.*[292] In this trademark action, the Missouri federal court found personal jurisdiction over a defendant that advertised an upcoming Internet mailing list service from its California Web site.[293] The Web site was accessed by Missourians 311 times, although 180 of those times were by the plaintiff.[294] The court determined that the defendant's advertisements amounted to purposeful availment of the privilege of doing business within Missouri, which satisfied the state's long-arm statute.[295] In analyzing whether due process was satisfied by an exercise of jurisdiction over defendant, the court addressed five factors[296] almost identical in wording to the five-part test in *Granite Gate Resorts.* In examining the nature and quality of the defendant's contacts with Missouri, the court stated:

> Although [defendant] characterizes its activity as merely maintaining a "passive website," its intent is to reach all internet users, regardless of geographic location. . . . By analogy, if a Missouri resident would mail a letter to [defendant] in California requesting information . . . regarding its service, [defendant] would have the option as
> to whether to mail information to the Missouri resident and would have to take some active measures to respond to the mail. With [the] website, [defendant] automatically and indiscriminately responds to each and every Internet user who accesses its website. Through its website, [defendant] has consciously decided to transmit advertising information to all Internet users, knowing that such information will be transmitted globally.[297]

Regarding the quantity of contacts, the court disregarded the plaintiff's 180 contacts with the Web site and found that the defendant had 131 contacts with Missouri users for the purpose of promotion and solicitation.[298] Finally, under the test, the court found that the defendant's posting of information and act of developing a mailing list was sufficiently related to plaintiff's trademark claims.[299] The court relied upon *California Software*[300] and *Inset Systems*[301] in determining that the defendant had purposefully availed itself of the privilege of doing business in Missouri by posting information on the Internet.[302] It found that jurisdiction over the defendant did not violate traditional notions of "fair play and substantial justice" because of the state's interest in protecting the trademark of a Missouri corporation and because the defendant had purposefully availed itself of the forum.[303]

The *Maritz* court's theory is overbroad. A country that opposes certain fiction writers need only point to American jurisprudence such as *Maritz* and the memorandum of the Minnesota Attorney General[304] to indict an American publisher for offering Salman Rushdie's *Satanic Verses* to its citizens through the Internet. Through a State's efforts to protect its citizens through a broad exercise of jurisdiction over the Web, it risks exposing its citizens to a whole world of liability.

Even though these cyberspace cases show new fact patterns, solutions for the problems follow established patterns of legal analysis. Genuine new questions concerning international jurisdiction to adjudicate would arise if States instituted virtual courts[305] or contented themselves with the virtual presence of a defendant or accused.

The danger with extensions of jurisdiction that go beyond reasonable legal limits is that defendants who operate Web sites will take measures to limit their legal exposure in ways that reduce the flow of information. One measure would be to install a filter to restrict access to users in certain jurisdictions with unfavorable laws.[306] Another would be to decline business from users within certain jurisdictions.[307] Yet another would be to post a notice on the Web site that its use is restricted to users in certain States.[308] A fourth possible measure would be to avoid transmitting data or information, such as software, that a court might quantify as "goods" being delivered into a State.[309] Finally, to avoid jurisdiction in courts that would look at additional contacts with the State beyond Internet activity, defendants who use the Internet might take care to avoid all other contacts with a State to avoid jurisdiction.[310]

Large-scale implementation of these methods and others would conflict with the Internet's promise of worldwide information. It would divide the Worldwide Web into Statewide Webs. And in those States where jurisdictional rules differ from area to area within borders, such measures would further divide the Worldwide Web into Local Webs.

3. Universality Principle

The universality principle is not only a legitimate basis for jurisdiction to prescribe. It also allows a State to exercise jurisdiction through its courts to enforce its criminal laws that punish universal crimes.[311] Thus, netizens who engaged in direct and public incitement to commit genocide or warcrimes[312] by means of computer communications could be haled worldwide into any court. In the case of violations of the Statute of the International Tribunal for the Former Yugoslavia,[313] the perpetrator could even be requested by the International Tribunal. Article 7 of the Statute states the individual responsibility for aiding and abetting in the planning, preparation, or execution of crimes outlawed by this [314]

statute. According to Article 9, the International Tribunal and national courts have concurrent jurisdiction, but the International Tribunal has primacy over the latter ones.[315]

C. Jurisdiction to Enforce

Jurisdiction to enforce deals with a State's authority to induce or compel compliance or to punish noncompliance with its laws or regulations, whether through the courts or by use of executive, administrative, police, or other nonjudicial action.[316] The U.S. enforcement agencies, in particular, are starting to enforce national laws on the Internet.[317] It is widely assumed that a state may not enforce its rules unless it has jurisdiction to prescribe those rules.[318] The mere existence of jurisdiction to prescribe, however, is insufficient to justify the state to exercise enforcement jurisdiction in another state's territory. Especially concerning measures in aid of enforcement of criminal law, a state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the state, given by duly authorized officials of that state.[319]

Enforcement measures requiring consent include not only the physical arrest of a person, but also, for example, service of subpoena, orders for production of documents, and police inquiries.[320] Police investigations may therefore not be mounted on the territory of another State without its consent. The consequences may seem odd for anyone not familiar with the eagerness of States to protect their national sovereignty. Millions of foreign tourists take pictures of the San Marco Place in Venice and talk to guides. If the San Marco Place, however, is the scene of a crime, and the FBI wants to take pictures or talk to witnesses, permission is required. Enforcement jurisdiction is linked quite closely to the territory. Its limits are much more strictly observed than is the case with jurisdiction to prescribe. When agents of the German military secret service, MAD, observed two persons and followed them to Austria, both Austria and Germany agreed that the incident violated international law.[321] In 1973, an Italian inspector of finances was arrested in Switzerland for making inquiries about the movement of contraband toward Italy.[322] Two French customs officials traveled to Switzerland on several occasions in 1980 to interrogate a former employee of a Swiss bank, requesting from him computer lists containing the names, addresses, account numbers, and credit balances of French customers. The person interrogated informed Swiss authorities, and subsequently the French customs officials were arrested and sentenced to imprisonment.[323]

An interesting question arises when the investigation is accomplished without entering another State's territory, by running, for instance, a computer program which searches databases installed in another country. At least two different scenarios are imaginable. Police could send "dog sniffs" via network to hard drives to check their contents.[324] Or, law enforcement agencies could try to filter the streams of e-mail communication by searching for certain keywords,[325] evaluating the communication in certain news groups, or checking suspicious Web sites. The first scenario is distinguished from the second insofar as the objects of supervision—hard drives—have a certain territorial location. Even though they can be easily moved, they are like all tangibles always physically located, either within or outside the borders of a certain jurisdiction. It is much more difficult to locate Web sites or public bulletin boards.

Even when the location of a hard drive, a Web site, or a bulletin board is known, the question is whether the activity of a foreign law enforcement agency might be allowed because the territory was not physically entered by any agent. The Swiss Federal Tribunal, Lausanne, decided in 1982 that a violation of sovereignty did not necessarily require that the violating person acted on the territory of the violated State.[326] A German undercover agent had contacted a Belgian suspect by telephone, inducing him to come for a business deal to Switzerland. When the suspect arrived in Switzerland, Germany requested his extradition.[327] The Swiss Federal Tribunal refused the extradition, arguing that to give effect to the German request would have made Switzerland a party to the violation of which Germany was considered guilty. This strict attitude was not shared by the Court of Appeals for the Second Circuit in *United States v. Romano*.[328] The appellants, domiciled in Italy, were induced by U.S. agents to come to the United States to complete a transaction which had been negotiated and arranged by telephone conversations. Confronted with the complaint of violation of foreign sovereignty, the court followed a narrow approach. "It must be stated at the outset that in this case no peace officer or officer of the United States ever entered Italian territory. Therefore, there was no violation of territorial sovereignty or offense to any State."[329]

This approach, however, is too narrow. In the cases of service of subpoena or orders for production of documents, no government agent enters foreign territory. Nevertheless, these cases are recognized as examples of infringement of sovereignty. They are unilateral acts by public authorities compelling a certain result which is not in accordance with the legal order of the State where the effects occur. The above-mentioned telephone conversations are arguably distinguishable. The Court of Appeals for the District of Columbia made a clear and well-justified distinction between the service of notice, which merely involves the supply of information, and compulsory process.[330] Telephone conversations concerning fake business deals are not compulsory by their nature. It might also be reasonable to allow everyone, even secret services, to surf the Net.[331] A search of one's hard drive by a foreign law enforcement agency from abroad, however, has another quality. It has the same effect as a traditional search of premises, a law enforcement measure reserved to the territorial sovereign. Such a "cybersearch" constitutes a unilateral act aimed at legal consequences. As territorial sovereignty serves, inter alia, to protect the residents from physical persecution of other states,[332] this protection must be extended when persecution no longer needs to physically enter foreign territory. As a consequence, it might be concluded that whenever a "cybersearch" targets a hard drive, a bulletin board, or a Web site in the course of a law enforcement measure, the consent of the territorial sovereign in which the target is located is required. First, however, the
target must be tied to a specific foreign jurisdiction, which may not be easy in all cases involving the Internet.

III. Conclusion and Outlook

International law allows many more States to exercise jurisdiction than a Netizen might be aware. And there is little hope that States will respect the "independence of cyberspace."[333]

States have already regulated the moon and other celestial bodies,[334] the deep seabed,[335] and Antarctica.[336] Although States will face seemingly insurmountable problems in their efforts to domesticate a network of computers, they will gradually find solutions.

Certain limits to the international exercise of jurisdiction, however, are clear. Jurisdiction to prescribe, absent links of territoriality or nationality, is only legal under international principles if a defendant targets a State or commits a crime to which the universality principle applies.

International jurisdiction to adjudicate is not triggered by the mere accessibility of a Web site by a State's citizens unless the alleged Internet crime falls under the universality exception. For instance, States are, in general, not allowed to exercise jurisdiction over defendants located abroad who merely advertise services over Web sites which are accessible to their citizens without particularly targeting them.[337] The consequences of such expansive jurisdiction would be severe. In areas where laws differ significantly from State to State, forum shopping could occur with a sweep as broad as the Internet is accessible.[338] Furthermore, exorbitant assertions of jurisdiction could provoke diplomatic protests, trigger commercial or judicial retaliation, and threaten friendly relations in unrelated fields.[339]

Jurisdiction to enforce by computerized means over databases or hard drives located in foreign countries is tempered by the interests of those territorial States. International law strongly suggests that such jurisdiction requires their consent.

Traditional concepts of international law, however, will need further development to solve future conflicts of competing jurisdictions. Consent on abstract concepts might be reached relatively easily, but the resolution of concrete cases will provoke troubles. International solutions, which might help to solve cyberspace-specific problems of lack of territoriality or abundance of territorial links, are still at a very early stage of development.[340]

The Association of South-East Asian Nations started in March 1996 to consider plans to regulate the Net. A recent initiative of the Organization for Economic Co-operation and Development (OECD) is aiming at a comparative study of national legislations and an exchange of experiences on the issue of illegal content on the Internet.[341] French ministry officials are also drafting an international agreement for the OECD to regulate the Internet.[342]

In October of 1996, the European Commission approved a "Communication" on "illegal and harmful content" on the Internet as well as a "Green Paper," which focused on "the protection of minors and human[s]" in the context of electronic services. The Communication presents policy options for immediate action with respect to the Internet, while the Green Paper takes a "horizontal approach" and is intended to initiate a longer-term discussion across all electronic media.[343] The European Commission identified a wide range of distinct areas concerning potentially illegal and harmful content on the Internet:

- *national security* (instructions on bomb-making, illegal drug production, terrorist activities);
- *protection of minors* (abusive forms of marketing, violence, pornography);
- *protection of human dignity* (incitement to racial hatred or racial discrimination);
- *economic security* (fraud, instructions on pirating credit cards);
- *information security* (malicious hacking);
- *protection of privacy* (unauthorised communication of personal data, electronic harassment);
- *protection of reputation* (libel, unlawful comparative advertising);
- *intellectual property* (unauthorised distribution of copyrighted works, *e.g.* software or music).[344]

The European Commission emphasizes the importance of cooperation among member States to combat the creation and distribution of illegal materials on the Internet.[345] At the same time, however, it proposes to extend the dialogue to international bodies composed of the largest number of countries possible, such as the OECD, the World Trade Organization, the United Nations, or one of the more specialized United Nations bodies.[346]

Similarly, at a conference which took place in Bonn last July, ministers of twenty-nine European countries considered international cooperation to be essential in this area.[347] They supported a multilateral as well as a European approach.[348] The U.S. government seems to prefer a more informal dialogue with selected partners. Its new policy approach is based on the development of an informal dialogue with key trading partners on public policy issues such as hate speech, violation, sedition, and pornography.[349] The U.S. government is particularly concerned that different national regulations might serve as disguised trade barriers.

National solutions are necessarily more limited in their effects. Due to the lack of authority on the international level, national approaches to jurisdiction must use sound reasoning to convince the international community.[350]

Usenet posters, Web page editors, archive maintainers, and especially service providers may find themselves in an unexpected legal pickle while traveling abroad in countries with strict laws that choose to exercise jurisdiction over cyberspace broadly. They should keep in mind that the First Amendment on the global level is nothing more than a local statute. Activities which are protected by constitutional rights in the United States might simply be prohibited in other countries. The Net offers exposure to many different cultures, experiences, and personalities. It offers, as well, exposure to many different penal codes. Robust anonymity might be a means to solve the problem of surprise legal jurisdiction—on both the national and international levels.[351] But in the meantime, the consequence for a few keystrokes could be severe. Indeed, in a world where some countries use harsh corporal punishments for acts they consider to be indecent, purveyors of potentially obscene materials like the Thomases should be wary—it could be worse than Tennessee and Utah.

* Associate, Rogers & Wells; Admitted to New York Bar (1997); LL.M., University of Chicago (1996); Research & Teaching Fellow, University of Tübingen (1990-1995); Second State Exam, Baden-Württemberg (1993); M.A., Political Science, University of Tübingen (1991); First State Exam (J.D. Equivalent), University of Tübingen (1990); Maîtrise en droit, Aix-Marseille III (1987).

** Associate, Rogers & Wells; Admitted to New York Bar (1997); Law Clerk, Honorable Harry D. Leinenweber, U. S. District Court for the Northern District of Illinois (1995-1996); J.D., University of Chicago (1995); B.A., Rice University (1991).

The Authors wish to thank Cynthia L. Kahn, a partner at Rogers & Wells, for her valuable comments and words of encouragement. We are indebted to Klaus H. Jander, a partner at Rogers & Wells, for his encouragement and support. Kurt Wm. Hemr, an associate at Rogers & Wells, also provided valuable advice. Any errors in this article, however, are exclusively attributable to the Authors. Special thanks go to Panayiota Souras, Jacqueline Acciarello, Sandra Lee, and Tuesday Umphries for their help in editing this Article.

1. Pink Floyd, *Eclipse*, *on* Dark Side of the Moon (Capital Records 1973).

2. Mark Lottor's Domain Survey, which counts the overall number of registered host computers connected to the Net, found 1.8 million hosts in July 1993. From July 1994 to July 1995, the number of hosts counted rose from 3.2 million to 6.6 million. In 1996 the number jumped to 12.8 million, and in 1997 the number of host computers connected to the Net reached 19.5 million. Mark Lottor, *Internet Domain Survey* (July, 1997)

<http://www.nw.com/zone/WWW/top.html>; *see also* Andrew Kantor & Michael Neubarth, *Off the Charts: The Internet 1996*, Internet World, Dec. 1996, at 44, 46. By the end of the decade, 120 million machines will be connected to the Net, according to the Internet Society of Reston, Virginia. No one knows exactly how many people use the Internet. Claims that 20 million to 40 million people are connected to the Internet stem, in most cases, from Lottor's survey. They are based on a rough rule of thumb guessing the number of users of a connected host. International Data Corp. in Framingham, Massachusetts, for example, estimates that by the end of the decade, 200 million users will join the Net. Cynthia Bournellis, *Internet '95*, Internet World, Nov. 1995, at 47, 47.

3. Michael Neubarth, *The Internet: A Global Look*, Internet World, Nov. 1995, at 95, 95.

4. Bournellis, *supra* note 2, at 47.

5. Neubarth, *supra* note 3, at 95.

6. *Illegal and Harmful Content on the Internet: Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions* (visited Oct. 23, 1997)

<http://www2.echo.lu/legal/en/internet/content/communic.html> [hereinafter *Illegal and Harmful Content on the Internet*].

7. Kantor & Neubarth, *supra* note 2, at 46.

8. Brent Gregston, *The European Picture: The Net is Conquering the Old World*, Internet World, Dec. 1996, at 52, 52.

9. Gene Mesher, *The Internet in Asia: Modern Countries Move Ahead*, Internet World, Dec. 1996, at 56, 56; *see also* Steven Schwankert, *Dragons at the Gates*, Internet World, Nov. 1995, at 109. Despite China's population of 1.2 billion, it has only 30,000
Internet users. *China: The Giant Infant: China and the Internet*, Internet World Online (Dec. 1996) <http://www.internetworld.com/1996/12/china.shtml>.

10. Message from Dave Hughes to Cyber-Rights (Sept. 7, 1997) (available at Cyber-Rights Library)

<http://snyside.sunnyside.com/cpsr/lists/listserv_archives/cyber-rights/970109.cr_The_Net_comes_to_Ulaan_Bator>.

11. *Pyongyang Home Page: Mad Dogs @ www*, N.Y. Times, Jan. 17, 1997, at A10; *see also Saddam Hussein Opens Home Page on the Internet*, N.Y. Times, May 5, 1997, at D6.

12. *See* Howard W. French, *On the Internet, Most of Africa Is Getting off to a Slow Start*, N.Y. Times, Nov. 17, 1995,

at A5; William Wresch, *New Lifelines: The Net is Sprouting in Africa—and Aiding Countries with Phone Systems*, Internet World, Nov. 1995, at 102. A weekly compilation of international Internet events, Netacross the World, is posted by Madanmohan Rao, Communications Director for the United Nations Inter Press Service Bureau. *See, e.g.*, Madanmohan Rao, *The Internet Will Become Increasingly Multilingual*, Netacross the World (Jan. 8, 1996)

<http://www.iworld.com/netday/NATWIN960205.html>, *abstracted from* Hong Kong Standard, Jan. 4, 1996.

13. *Cf.* Alan J. Hartnick, *Copyright & Trademark On the Internet—And Where to Sue*, N.Y. L.J., Feb. 21, 1997, at 5 ("The cases are developing: Should a New Orleans web site host be sued in Uganda?"); Wendy R. Leibowitz, *The Internet Blunts TM Protection*, Nat'l L.J., Feb. 10, 1997, at B1.

14. "Cyberspace refers to the interaction of people and businesses over computer networks, electronic bulletin boards, and commercial online services. The largest and most visible manifestation of cyberspace is the Internet . . . ." R. Timothy Muth, *Old Doctrines on A New Frontier: Defamation and Jurisdiction in Cyberspace*, Wis. Law. Sept. 1995, at 11, 11. See also the definition in Edward A. Cavazos & Gavino Morin, Cyberspace and the Law: Your Rights and Duties in the On-Line World 1-11 (1994).

15. "Since the Internet has moved from techie preserve to office park, shopping mall and entertainment arcade, it is sheer fantasy to expect that it will be left a libertarian island in a world full of jealous competitors and conflicting public objectives." Eli M. Noam, *An Unfettered Internet? Keep Dreaming*, N.Y. Times, July 11, 1997, at A1.

16. A slightly different vision is offered by Joe Shea, Editor-in-Chief of The American Reporter:

I think we need to defend the Net from all the people who want to regulate it by creating the Internet Liberation Army (ILA), made up of a corps of top-flight engineers working together to defeat various regulatory schemes by technical and political means.

. . . Let's make the Net a virtual country and create a group of well-disciplined people including leaders, an army and a population of supporters who pledge to keep it free.

Message from Joe Shea to Cyber-Rights (Mar. 22, 1996) (available at Cyber-Rights Library) <http://snyside.sunnyside.com/cpsr/lists/listserv_archives/cyber-rights/960322.cr_Internet_Liberation_Army_—_>.

17. *Cf. Global Information Networks*, Ministerial Conference Bonn 6-8 July 1997, & 22 (visited Oct. 23, 1997) <http://www2.echo.lu/bonn/final.html> [hereinafter Ministerial Conference] ("Ministers stress that the general legal frameworks should be applied on-line as they are off-line.").

18. Julian Dibbell, *A Rape in Cyberspace*, The Village Voice, Dec. 21, 1993, at 36; *see also* James Adams, *US Paedophiles Lure Children on the Internet*, Sunday Times-London, June 25, 1995, *available in* 1995 WL 7678431.

19. Rosalind Resnick, *Cybertort: The New Era*, Nat'l L.J., July 18, 1994, at A1.

20. Benjamin Wittes, *Information-Highway Robbery: Is Law Enforcement Ready for Cybercrime?*, Legal Times, Oct. 10, 1994, at 16; *see also* Marc S. Friedman & Kenneth R. Buys, *`Infojacking': Crimes on the Information Superhighway*, Computer Law., Oct. 1996, at 1.

21. Euskadi Koordination, *Political Censorship on the Internet*, (Apr. 2, 1996) (available at Cyber-Rights Library) <http://snyside.sunnyside.com/cpsr/lists/listserv_archives/cyber-rights/960403.cr_Political_Censorship_on_Inte> (protesting against an "Attentate against the Freedom of Speech and Privacy Rights through a cyberterroristic attack against the publication of information about the Basque Country on Internet"); *see also* John H. Cushman, Jr., *Basque Web Site Suspended After Protests*, N.Y. Times, July 28, 1997, at D3.

22. *See Scams and Frauds Spread Through Cyberspace*, Netacross the World, *abstracted from* Associated Press, Jan. 4, 1996 (on file with author); David Post, *New Rules for the Net?*, Am. Law., July/Aug. 1995, at 112, 112 ("The backlash is coming from all points on the political spectrum . . . . "); Peter H. Lewis, *Group Urges Internet Ban on All*

Hate Groups' Messages, N.Y. Times, Jan. 10, 1996, at A1; *cf.* Tony Tuths, *State of the Art. . .Traffic Court*, The New Legist, July/Aug./Sept. 1995, at 31, 31:

By this time next year, the great techno-unwashed will be hooked up. Over fifty million Mom and Pops, Suzy and Biffs will be wired up to the Net, poking around, and getting into trouble. And when that many people start reaching out and touching each other, legal problems have been known to arise. In fact, we could be witnessing the biggest legal goldrush since Palsgraf got plowed by that scale.

23. The Communications Decency Act is just one example of the regulation of the Net on the national level. *See* A Swedish Proposal for a Law About Computer-Mediated Communication (visited Oct. 23, 1997)

<http://www.dsv.su.se/~jpalme/SOU-1996-40-eng.html>.

24. The incident is best described by the German journalist Michael Kunze who writes for the major German news magazines, *Der Spiegel* and *Der Spiegel Online*. Message from Michael Kunze to Cyber-Rights (Jan. 6, 1996) (available at Cyber-Rights Library)

<http://snyside.sunntside.com/cpsr/lists/listserv_archives/cyber-rights/960111.cr_CIS_censorship%3a_The_whole_St>. A list of more than 200 news groups was presented to CompuServe as containing "suspicious news groups." In the attached letter from the Munich prosecutor, it is recommended
to CompuServe "to take the necessary steps in order to avoid an eventual prosecution." *Id.*; *see also* Nathaniel Nash, *Holding Compuserve Responsible*, N.Y. Times, Jan. 15, 1996, at D4. Since CompuServe did not have the technical ability to block only German users, it eliminated access for all its users, about 4 million worldwide. It seems as though the prosecutor had tried to bring CompuServe to court to get his legal position checked. CompuServe's servile tactics, however, frustrated this goal. The first comments in U.S. newspapers were influenced by inaccurate facts. S*ee, e.g.*, *CompuServe Blocks `NetSex Groups*, USA Today, Dec. 29, 1995, at 1A ("It is the most sweeping instance of Internet censorship so far, and the most drastic action taken by a government."); *cf.* Howard Goldberg, *CompuServe Blocks Access to Sex Forums on Net*, Chi. Sun-Times, Dec. 30, 1995, at 12 (quoting Arno Edelmann, CompuServe product manager for Germany: "It is perhaps an overreaction, but we want to cooperate with the Bavarian prosecutor's office."). Subsequently, however, when CompuServe decided to challenge prosecutors by restoring access and handing out free software for blocking pornography, it was indicted for aiding in the distribution of pornography and computer games. Prosecutors charged that CompuServe did not do enough to block Germans from accessing the material. Edmund L. Andrews, *Germany's Efforts to Police Web Are Upsetting Business*, N.Y. Times, June 6, 1997, at A1. In another investigation in Hamburg, a prosecutor is considering whether America Online should be liable for its members' dissemination of child pornography through e-mail accounts. America Online contends that it cannot control what its members send out. *Ermittlungen gegen AOL wegen der Verbreitung von Kinderpornographie*, Neue Juristische Wochenschrift Computerreport, Nov./Dec. 1996, at 392. In a third instance of Internet investigation, German prosecutors forced German Internet access providers to block access to a magazine published in the Netherlands which provided instructions on how to sabotage railway lines. Blocking access, however, required that all content on the Dutch server—including harmless content—be blocked. Dutch officials have complained, but not intervened. *Illegal and Harmful Content on the Internet*, *supra* note 6, pt. 4.b.iv. A left-wing politician had to fend off German prosecutors for leading others to a link on her Web page to the "terrorist" magazine. The charges were eventually dismissed, but attorneys for both sides agreed that the court's narrow decision did not resolve the issue of restricting Internet access. Edmund L. Andrews, *German Judge Dismisses Criminal Charge Over Internet Link*, N.Y. Times, July 1, 1997, at D7. According to prosecutorial spokesman Ruediger Reiff prior to the court's decision, "Those who committed the initial crime of writing the articles . . . are as yet unidentified, but Ms. Marquardt appears to have committed the crime of aiding this felony. Press freedom does not go that far." *German Left-Winger's Links Break Law?*, Netday News (Jan. 17, 1997)

<http://netday.iworld.com/97Jan/1703-german.html>. In court Marquardt said that the German prosecutors' efforts to stop her reminded her "[o]f the kind of censorship we protested against in East Germany." Edmund L. Andrews, *German Judge Dismisses Criminal Charge Over Internet Link*, N.Y. Times, July 1, 1997, at D7.

25. John Markoff, *On-Line Service Blocks Access to Topics Called Pornographic*, N.Y. Times, Dec. 29, 1995, at A1

(quoting Esther Dyson, Chairperson, Electronic Frontier Foundation); *see also* Edmund L. Andrews, *Germany's Efforts to Police Web are Upsetting Business*, N.Y. Times, June 6, 1997, at A1 (Chris Kuner, an American cyberspace lawyer in Germany stated: "[t]he Internet created a universal jurisdiction, so that once you are on the Internet you are subject to the laws of every country in the world."); *see also* Message from Robert Cannon, Esq., to Cyber-Rights (Mar. 15, 1996) (available at Cyber-Rights Library) <http://www.cpsr.org/cpsr/nii/cyber-rights/Library/> ("We must remember that simply because what we do is legal in our country, it does not mean that it is legal in another country.").

26. Peter H. Lewis, *Limiting A Medium Without Boundaries*, N.Y. Times, Jan. 15, 1996, at D1; *see also* Seth Faison, *Chinese Tiptoe Into Internet, Wary of Watchdogs*, N.Y. Times, Feb. 5, 1996, at A3; Mesher, *supra* note 9, at 57.

27. Message from Patrick Brennan to Cyber-Rights (Jan. 7, 1996) (available at Cyber-Rights Library) <http://www.cpsr.org/cpsr/lists/lis. . .cr_1289_%3a_Compuserve_caves_I>; *see also* Noam, *supra* note 15. *But see The Internet Will Become Increasingly Multilingual*, Netacross the World (Jan. 8, 1996), *abstracted from* Hong Kong Standard, Jan. 4, 1996. (on file with author).

28. George Cole, *Censorship in Cyberspace*, The Fin. Times, March 21, 1996, at 20, *available in* 1996 WL 6151123; Gregston, *supra* note 8, at 53.

29. Dato V. L. Kandan & Chuah Jern Ern, *Malaysia Prepares "Cyberlaws"*, Intell. Prop. Worldwide (July/Aug. 1997) <http://www.ipww.com/jul97/pllmalaysia.html>.

30. *Singapore Laws Will Apply in Cyberspace*, Netacross the World (Feb. 26, 1996), *abstracted from* The Straits (Singapore), Feb. 24, 1996 (on file with author). The government is requiring the registration of operators and owners of Web sites containing political or religious information. Mesher, *supra* note 9, at 57; *see also* Noam, *supra* note 15.

31. *Cf. Illegal and Harmful Content on the Internet*, *supra* note 6, at 2 ("What is illegal offline remains illegal online . . . ."); *id.* at 3 ("[T]he Internet does not exist in a legal vacuum . . . .").

32. *See, e.g.*, Carol M. Beach, *Taxing the Internet* (posted Mar. 29, 1997)

<http://www.slate.com/Gist/97-03-29/gist.asp>; John Berry, *Who will Tax the Web?*, Internet World, April 1997, at 37.

33. *See* Bruce A. Lehman & Ronald H. Brown, The Report of The Working Group on Intellectual Property Rights, Intellectual Property and the National Information Infrastructure (1995) (discussing the problems of intellectual property and copyright as they apply to the Internet). The report eloquently poses the choice of law problem: "Which country's law controls the resolution of a copyright infringement dispute—the country from which a copyrighted work is uploaded or to which it is downloaded, or the country where the host server is located?" *Id.* at 147; *see also* Martin H. Samson, *Trademark Lawsuits in Cyberspace*, N.Y. L.J., Dec. 2, 1996, at S10; Alan J. Hartnick, *Copyright & Trademark on the Internet* (visited Oct. 23, 1997)

<http://www.ljx.com/internet/02cptmint.html>.

34. *Cf.* William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* (visited Oct. 23, 1997) <http://www.ljx.com/internet/ecommframe.html> (explaining the new approach of the U.S. government).

35. *See Internet Casino Opens in South Africa*, Netacross the World (Apr. 1, 1996), *abstracted from* Wkly. Mail & Guardian (South
Africa), March 29, 1996; *see also The Gaming Club* (visited Oct. 23, 1997) <http://www.casino.co.za>.

36. *See* Cole, *supra* note 28; *Internet Could Become Dirty Money Haven*, Reuters News Service, March 13, 1996, *available in* LEXIS, News Library, Reuwld File.

37. Some Internet enthusiasts, focusing on the electronic bits, hope that the Internet is beyond regulation. However, a government can go after physical elements, if not intangible ones. "Communications are a matter not just of signals but of people, institutions and physical hardware . . . ." Noam, *supra* note 15; *cf.*, *e.g.*, Lawrence Lessig, *The Path of*

Cyberlaw, 104 Yale L.J. 1743 (1995).

38. Geanne Rosenberg framed the question as follows: "Whether a person or business on the Internet falls under the laws of some, all or any of the jurisdictions from which that Internet site can be reached." Geanne Rosenberg, *Trying to Resolve Jurisdictional Rules on the Internet*, N.Y. Times, Apr. 14, 1997, at D1; *see also* David R. Johnson, *Traveling in Cyberspace*, Legal Times, Apr. 3, 1995, at 26; John Perry Barlow, *Thinking Locally, Acting Globally*, Time, Jan. 15, 1996, at 76; David G. Post, *Anarchy, State and the Internet*: *An Essay in Law-Making in Cyberspace*, 1995 J. Online L. art. 3, para. 4

<http:// www.law.cornell.edu/jol/post.html>; T.J. Thurston, *Tackling Conflicts of Law on the Internet*, The Internet Newsletter, March 1997, at 8, *available in* LEXIS, News Library, Curnws file; John P. Ratnaswamy & Ross E. Kimbarovsky, *Where Can a Person or Business Be Sued for Alleged Claims Arising From Their Use of the Internet?* 25 Computer L. Rep. (May 1997) <http:/www.hopsut.com/internet.html>.

39. *Sex on the Internet*, The Economist, Jan. 6, 1996, at 18.

40. Post, *supra* note 38, para. 38; *see also* David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1378 (1996). For a profound criticism of this idealistic approach, see Lawrence Lessig, *The Zones of Cyberspace*, 48 Stan. L. Rev. 1403 (1996).

41. Johnson, *supra* note 38, at 26.

42. *See, e.g.*, Matthew R. Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 Vand. J. Transnat'l L. 75 (1996); Eric J. McCarthy, Comment, *Networking in Cyberspace: Electronic Defamation and the Potential for International Forum Shopping*, 16 U. Pa. J. Int'l Bus. L. 527 (1995); Kyu Ho Youm, *Suing American Media in Foreign Courts: Doing an End-Run Around U.S. Libel Law*, 16 Hastings Comm/Ent L.J. 235 (1994); Michael Smyth & Nick Braithwaite, *First U.K. Bulletin Board Defamation Suit Brought*, Nat'l L.J., Sept. 19, 1994, at C10; Richard H. Acker, Comment, *Choice-of-Law Questions in Cyberfraud*, 1996 U. Chi. Legal F. 437.

43. Restatement (Third) of the Foreign Relations Law of the U.S. § 401 cmt. a (1987) [hereinafter Restatement].

44. *See* Barcelona Traction, Light and Power Co. (Belg. v. Spain), 1970 I.C.J. 3, 17-53 (Feb. 5).

45. Arthur T. von Mehren & Donald T. Trautman, *Jurisdiction to Adjudicate: A Suggested Analysis*, 79 Harv. L. Rev. 1121, 1127 (1966); Gary B. Born, *Reflections on Judicial Jurisdiction in International Cases*, 17 Ga. J. Int'l & Comp. L. 1, 33 (1987).

46. Louis Henkin et al., International Law 1046 (3d ed. 1993); Barry E. Carter & Phillip R. Trimble, International Law 726 (2d ed. 1995); Bernard H. Oxman, *Jurisdiction of States*, *in* Encyclopedia of Public International Law 277 (Rudolf Bernhardt ed., Instalment 10 1987); Thomas Buergenthal & Harold G. Maier, Public International Law 159 (2d ed. 1990); Restatement, *supra* note 43, § 401.

47. Oxman, *supra* note 46, at 277.

48. Restatement, *supra* note 43, at 230-31.

49. *Cf*. Andreas F. Lowenfeld, International Litigation and the Quest for Reasonableness 19 (1996). Gary B. Born took a cautious approach when the Restatement was adopted. Born, *supra* note 45, at 19 (the "`reasonableness test'probably reflects an emerging consensus on international law in this field").

50. Restatement, *supra* note 43, at 236-37.

51. *Id.* § 403 cmt. a.

52. *Id.*

53. Vienna Convention on Diplomatic Relations, Apr. 18, 1961, art. 34, 500 U.N.T.S. 95.

54. Restatement, *supra* note 43, § 402.

55. Another principle, the passive personality principle, will not be discussed in this analysis. The passive personality principle asserts that a State may apply law—particularly criminal law—to an act committed outside its territory by a person not its national where the victim of the act was its national. The principle has not been generally applied with approval for ordinary torts or crimes, but it is increasingly accepted as applied to terrorist attacks and other organized attacks on a State's nationals by reason of their nationality. So far, no realistic scenarios have arisen in the cyberspace context that would provoke use of the passive personality principle.

56. Restatement, *supra* note 43, § 403(1).

57. *Id*. § 403(2).

58. *Id.* § 403(3); *see also* International Chamber of Commerce, The Extraterritorial Application of National Laws, 38-40 & 46-48 (Dieter Lange & Gary Born eds., 1987) [hereinafter International Chamber of Commerce].

59. Restatement, *supra* note 43, § 404.

60. *Id.* § 402 cmt. c.

61. *See, e.g.*, Nathaniel C. Nash, *Germans Again Bar Internet Access, This Time to Neo-Nazism*, N.Y. Times, Jan. 29, 1996, at D6. The Germany-based T-Online service of Deutsche Telekom, a privatized former State enterprise, said it voluntarily blocked access to the World Wide Web site of Ernst Zündel, a Toronto-based Neo-Nazi, after German prosecutors warned the company that they were investigating whether it was helping to incite racial hatred. According to the European Commission, "some third countries have introduced wide-ranging legislation to block all direct access to Internet via access providers by introducing a requirement for `proxy servers' similar to those used by large organisations for security reasons, combined with centralised blacklisting of documents . . . ." *Illegal and Harmful Content on the Internet*, *supra* note 6, pt. 4.b.iv.

62. *See, e.g.*, Hiawatha Bray, *UMass Shuts Down Web Site Containing Neo-Nazi Material*, Boston Globe, Feb. 2, 1996, at 28. Free speech advocates at Stanford University and Carnegie-Mellon University have obtained the offending material (Holocaust-revisionist Web pages), posted it on other Web sites, and urged others to post it in locations not blocked by Deutsche Telekom. The idea is to put the material on so many Web sites that Germany would have to completely disconnect from the Internet to censor it. *Id.*

63. *Cf.* Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

64. John Markoff, *German Pornography Laws Determine What America Sees,* N.Y. Times, Dec. 31, 1995, § 4, at 2.

65. *Cf.* Lea Brilmayer, Justifying International Acts 107 (1989). ("It cannot be the case that a state is prohibited from engaging in any actions that produce changes in another state, because in an interdependent world, virtually everything that one state does has impacts on the others.").

66. *See* Howard Goldberg, *CompuServe Blocks Access to Sex Forums on Net*, Chi. Sun-Times, Dec. 30, 1995, at 12 (quoting the statement of CompuServe spokesman William Giles: "We're in over 140 countries around the world. If you want to play in their yard, you have to play by their rules."); *see also* Terence Gallagher, *German Cabinet Approves Internet Regulation*, (Dec. 19, 1996) (available at Cyber-Rights Library)

<http://snyside.sunnyside.com/cpsr/lists/listserv_archives/cyber-rights/961219.cr_German_Regulation_of_Interne>:

German Chancellor Helmut Kohl's cabinet approved an Internet regulatory bill Wednesday that seeks to protect users' privacy and keep out smut and Nazi propaganda . . . . The . . . law puts responsibility . . . on `suppliers' [who are warned that illegal] material can be accessed through their systems [if] they have the technical means to block it.

In response to this new proposed "multimedia law," CompuServe is considering "moving its German operations to a neighboring country if the law becomes too restrictive." *Id.*; *see also* John Browning, *Europeans On-Line: National Boundaries Still Matter, Even in Cyberspace*, Sci. Am., May 1995, at 35 (stating that as U.S.-dominated on-line services emerge in Europe, one of the "optimistic assumptions" of cyberspace is about to be challenged: that there are no geographical limits or boundaries in cyberspace).

67. John Markoff, *On-Line Service Blocks Access to Topics Called Pornographic*, N.Y. Times, Dec. 29, 1995, at A1; Peter H. Lewis, *Limiting a Medium Without Boundaries*, N.Y. Times, Jan. 15, 1996, at D1.

68. *Cf.* Eric Schneiderman & Ronald Kornreich, *Personal Jurisdiction and Internet Commerce*, N.Y. L.J., June 4, 1997, at 1 (arguing "that lawyers and courts should focus their analysis of in personam jurisdiction based on Web contacts by evaluating the quantity and quality of contacts with a Web site by a forum's citizens.").

69. Wendy R. Leibowitz, *How Risky Is Business on the Internet?*, Nat'l L.J., May 26, 1997, at B1. The Paris court decided on June 9, 1997 to dismiss the lawsuit, but only on procedural grounds. *Legal Headlines* (visited June 10, 1997)

<http://www.ljx.com/news/french.htm>; Wendy R. Leibowitz, *National Laws Entangle the `Net: It's A Small, Small, Litigious Web*, Nat'l L.J., June 30, 1997, at B7.

70. Mike King, *Language Police Patrolling Internet Sites*, The Gazette (Montreal), June 14, 1997, at A1; Leibowitz, *supra* note 69.

71. Declan McCullagh, *Banning Iran*, HotWired (Aug. 28, 1996)

<http://www.eff.org/~declan/global/iran/hw.iran.082896.txt>.

72. *American Library*, 969 F. Supp. 160 (S.D.N.Y. 1997).

73. *Id.* at 167.

74. *Id.* at 161; U.S. Const. art. I, ` 8, cl. 3.

75. Carter & Trimble, *supra* note 46, ch. 7; Blackmer v. United States, 284 U.S. 421 (1932); J. L. Brierly, The Law of Nations 231-32 (Oxford 5th ed. 1955). *But see* Geoffrey R. Watson, *Offenders Abroad: The Case for Nationality-Based Criminal Jurisdiction*, 17 Yale J. Int'l L. 41, 83 (1992) ("The United States, the crusading champion of extraterritorial jurisdiction, continues to reject one of the least controversial forms of extraterritorial criminal jurisdiction, nationality-based jurisdiction. As a result, U.S. nationals commit serious crimes overseas and escape prosecution.").

76. *See* Margaret A. Healy, *Prosecuting Child Sex Tourists at Home: Do Laws in Sweden, Australia, and the United States Safeguard the Rights of Children as Mandated by International Law?*, 18 Fordham Int'l L.J. 1852 (1995).

77. §§ 6, 184(3) StGB (German Penal Code). For a translation, see, for example, *The Penal Code of the Federal Republic of Germany*, 28 The American Series of Foreign Penal Codes (Edward M. Wise ed. & Joseph J. Darby trans., 1987). According to the wording of StGB § 6, German law is even applicable to certain international crimes of non-nationals committed abroad. However, the German Federal Supreme Court for Criminal Matter considered the principle of nonintervention and required a legitimizing link of the case with Germany. BGH Urteil, StR, 3 (1976), 298; *see also* Schönke & Schröder, Strafgesetzbuch - Kommentar, introductory note to §§ 3-7 n.8 (Albin Eser) (25th ed. 1997); Wilhelm Wengler, *Völkerrechtliche Schranken des Anwendungsbereichs von Strafgesetzen*, 32 Juristenzeitung 257 (1977); Philip Kunig, *Die Bedeutung des Nichteinmischungsprinzips für das Internationale Strafrecht der Bundesrepublik Deutschland*, 18 Juristische Schulung 595 (1978).

78. Restatement, *supra* note 43, § 402 cmt. e.

79. *See* David Plotnikoff, *Bite Lacking in Protests of On-Line Censorship*, San Jose Mercury News, Jan. 4, 1996. ("Last week, a foreign power successfully bullied an American company into pulling the plug on part of the news feed that reaches millions of Americans.").

80. Oxman, *supra* note 46, at 280; United States v. Aluminum Co. of America, 148 F.2d 416, 444 (2d Cir. 1945).

81. International Chamber of Commerce, *supra* note 58, at 4-32; Richard Whish, Competition Law 370-385 (3d ed. 1993).

82. Restatement, *supra* note 43, § 402 reporters' n.; Jason Coppel, *A Hard Look at the Effects Doctrine of Jurisdiction in Public International Law*, 6 Leiden J. Int'l L. 73 (1993); Margaret Loo, *IBM v. Commissioner*: *The Effects Test in the EEC*, 10 B.C. Int'l & Comp. L. Rev. 125 (1987).

83. Werner Meng, *Regeln über die Jurisdiktion der Staaten im amerikanischen* [*Restatement (Third) of Foreign Relations Law*], 27 Archiv des Völkerrechts 156, 183 (1989) (preferring to justify the results of the effects principle by reference to general principles of international law); *see also* F.A. Mann, *The Doctrine of International Jurisdiction Revisited After Twenty Years*, 186 R.C.A.D.I. 9, 26 (1984 III) ("[T]he purely commercial effect . . . should be insufficient to confer . . . any international right to prescribe conduct abroad."); c*f.* Vaughan Lowe, *International Law and the Effects Doctrine in the European Court of Justice*, 48 Cambridge L.J. 9 (1989).

84. *Thomas*, 74 F.3d 701 (6th Cir.), *cert. denied*, 117 S. Ct. 74 (1996).

85. *Id.* at 710.

86. United States v. Thomas, 113 F.3d 1247 (10th Cir. 1997).

87. On the national level the federal prosecution of the Thomases looks more like "a good example of bad law." Mark Eckenwiler, *Criminal Law and the Internet*, Legal Times, Jan. 23, 1995, at S32. Because the federal obscenity laws regulate all kinds of transfer, no special issues are raised in the cyberspace context. The question whether the "contemporary community standards" requirement should be modified is therefore not really caused by technological innovations. The problem arises even when a person is travelling from the East Coast to the West Coast with pornographic material in the trunk. For a summary of the problems, see Cavazos & Morin, *supra* note 14, at 89-104; John S. Zanghi, *"Community Standards" in Cyberspace*, 21 U. Dayton L. Rev. 96 (1995); William S. Byassee, *Jurisdiction in Cyberspace: Applying Real World Precedent to the Virtual Community*, 30 Wake Forest L. Rev. 197 (1995); Timothy S.T. Bass, Comment, *Obscenity in Cyberspace: Some Reasons for Retaining the Local Community Standard*, 1996 U. Chi. Legal F. 471.

88. *Playboy Enter.*, 939 F. Supp. 1032 (S.D.N.Y. 1996).

89. *Id.* at 1039.

90. *Id.* (citation omitted).

91. *Id.* at 1040.

92. Gambling—Wire Communications—Lotteries—Use of Internet or Wire Communications to Conduct Gambling; Cruises to Nowhere, Op. Fla. Att'y Gen., No. AGO 95-70, 1995 WL 698073 (Oct. 18, 1995).

93. *Id.* at *4, *6.

94. *Id.* at *7.

95. Warning to All Internet Users and Providers, Mem. Minn. Att'y Gen. (visited Oct. 24, 1997) <http://www.state.mn.us/ebranch/ag/memo.txt> [hereinafter Minnesota Memorandum]; *see also* Mark Eckenwiler, *States Get Entangled in the Web*, Legal Times, Jan. 22, 1996, at S35.

96. Minnesota Memorandum, *supra* note 95.

97. *Id*.

98. League of Nations, Committee of Experts for the Progressive Codification of International Law, Report to the Council of the League of Nations (1926).

99. The power to enforce presupposes jurisdiction to enforce. *See* Restatement, *supra* note 43, § 432 introductory note.

100. Minnesota Memorandum, *supra* note 95. The Attorney General applied his argument in opposing a motion to dismiss by a gambling company:

[E]very day for at least nine months defendants have solicited business from hundreds of thousands of Minnesota consumers by advertising two sports gambling services on the computer network known as the Internet. Although this . . . involves a relatively new technology, . . . the legal principle is not new: the State has jurisdiction to protect the public from unlawful solicitations by enjoining companies which have solicited business from Minnesota citizens.

State's Brief in Opposition to Motion to Dismiss, State v. Granite Gate Resorts, Inc., 1996 WL 767431 (Minn. Dist. Ct. Dec. 11, 1996) (No. C6-95-007227)

<http://www.state.mn.us/ebranch/ag/brief.txt>.

101. Playboy Enter. Inc. v. Chuckleberry Publ'g, Inc., 939 F. Supp. 1032 (S.D.N.Y. 1996).

102. *See, e.g.*, United States v. Morris, 928 F.2d 504 (2d Cir. 1991); David K. McGraw, *Sexual Harassment in Cyberspace: The Problem of Unwelcome E-Mail*, 21 Rutgers Computer & Tech. L.J. 491 (1995); *Former Italian Judge Receives Death Threats—Via Internet*, Netacross the World (Mar. 25, 1996), *abstracted from* Agence France Press; Straits Times (Singapore) March 24, 1996 (on file with author); Editorial, *Policing Cyberspace*, N.J. L.J., Feb. 27, 1995, at 22; *E-Mail Is Becoming A Conduit of Prejudice on Many Campuses*, N.Y. Times, Feb. 16, 1997, at 40.

103. Cavazos & Morin, *supra* note 14, at 5.

104. *Cf.* Trotter Hardy, *The Proper Legal Regime For "Cyberspace"*, 55 U. Pitt. L. Rev. 993, 1053 (1994).

105. Eckenwiler, *supra* note 87.

106. Restatement, *supra* note 43, § 402 cmt. d; *see also* Lamar v. United States, 240 U.S. 60 (1916) (holding that a telephone fraud could be prosecuted where the call terminated instead of where it originated from).

107. § 86, 86a StGB (German Penal Code).

108. *Id.* §§ 130(3), 220a(1). For the application of this provision, the conviction of Guenter Deckert in Germany's Federal Supreme Court of Justice is instructive:

In this decision, the Federal Supreme Court of Justice clearly enunciated its position that denial of the fact of the Holocaust is a serious crime and should be handled as such in view of its serious implications. The defendant Deckert is a right wing extremist who was charged with incitement to riot and promoting racial hatred. The Landgericht in Mannheim had sentenced [him] to one year of probation for expressing his belief that the Nazis did not commit mass murder of the Jews in the gas chambers, but this was a mitigated sentence as the court saw his as an honest expression of a political opinion in the effort to protect Germany from what he saw as unjust recriminations.

The Federal Supreme Court of Justice . . . . [held that] [t]here is no constitutional right or principle which allows for the justification or even mitigation of a criminal act through the devaluating characterization of a particular group. Finally, the Landgericht was in error by even considering a sentence mitigation in a case dealing with criminal penalties geared

at maintaining the public order.

The Deckert Case: No Tolerance for Holocaust Denial (last modified Jan. 26, 1995)

<http://www.jura.uni-sb.de/Entscheidungen/abstracts/deckert.html> France has a similar law prohibiting denial of the existence of crimes against humanity. Alan Riding, *French Icon Stumbles In Debate on Holocaust*, N.Y. Times, May 1, 1996, at A10.

109. Frank Bajak, *As Police Turn up the Heat, Neo-Nazis Build an Electronic Shield*, Associated Press, June 26, 1995, *available in* 1995 WL 4394533.

110. Eckenwiler, *supra* note 87.

111. *Cf.* International Chamber of Commerce, *supra* note 58, at 45:

extraterritorial regulatory measures generally should be permissible only where both foreign conduct and its effects are constituent elements of the activity to which the national law applies; where the effects within the territory are substantial; and where the effects are a direct and primarily intended result of the foreign conduct.

112. *Panavision Int'l*, 938 F. Supp. 616 (C.D. Cal. 1996).

113. *Id.* at 619.

114. *Id.* at 620.

115. *Id.*

116. *Id.* at 620 (quoting Omeluk v. Langsten Slip & Batbyggeri, 52 F.3d 267, 270 (9th Cir. 1995)).

117. *Id.* at 621.

118. *Data Disk*, 557 F.2d 1280 (9th Cir. 1977). For further discussion, see *infra* Part II.B.2.a.

119. *Panavision Int'l.*, 938 F. Supp. at 621.

120. *Id.*; *cf.* CD Solutions, Inc. v. Tooker, 965 F. Supp. 17, 20 (N.D. Tex. 1997) (holding that when a declaratory judgment plaintiff registered domain name that happened to incorporate defendant's trade name, action was dismissed because claims did not arise out of defendant's contacts with forum state).

121. *Panavision Int'l.*, 938 F. Supp. at 622 (citing Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd*, No. 96-9344,1383, 1997 WL S60048 (2d. Cir. Sept. 10, 1997) (*see* discussion *infra* Part II.B.1.d.); CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996) (*see* discussion *infra* Part II.B.1.e.); Pres-Kap, Inc. v. System One, 636 So. 2d 1351 (Fla. Dist. Ct. App. 1994) (*see* discussion *infra* Part II.B.1.i.)).

122. *Id.*

123. *Id.*

124. The seven factors are as follows:

(1) the extent of defendant's "purposeful" interjection; (2) the burden on defendant in defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum.

Id. at 622 (citing Burger King Corp. v. Rudzewicz 471 U.S. 462, 476-478 (1985)). The Court did not address the

factors individually. See *infra* Part II.B.1.f, Part II.B.2.a. for a discussion of almost identical factors in two other cases.

125. *Id.*

126. *Id.*

127. *Id.*

128. Restatement, *supra* note 43, § 402(3).

129. Ian Brownlie, Principles of Public International Law 304 (4th ed. 1990).

130. Restatement, *supra* note 43, § 402 cmt. f; Henkin et al., *supra* note 46, at 1082-84; Buergenthal & Maier, *supra* note 46, at 169.

131. A worm is "a usually small self-contained computer program that invades computers on a network and usually performs a malicious action." Merriam-Webster's Collegiate Dictionary 1364 (10th ed. 1996).

132. *Cf.* Kandan & Ern, *supra* note 29 (explaining that Malaysia's proposed Computer Crimes Bill intends to prevent mischievous activities such as hacking into computers, implanting viruses, and cracking passwords).

133. Douglas Barnes, *The Coming Jurisdictional Swamp of Global Internetworking (Or, How I Learned to Stop Worrying and Love Anonymity)* (visited Oct. 24, 1997)

<http://www.communities.com/paper/swamp.html>.

134. Restatement, *supra* note 43, § 402 cmt. f.

135. Joyce v. Dir. of Pub. Prosecutions, 1946 App. Cas. 347 (appeal taken from Crim. App.); *see* Encyclopedia of Public International Law 353 (Rudolf Bernhardt ed., Instalment 8 1985) (citing *Joyce*, 1946 App.Cas. 347) (discussing the value of this decision as an international precedent).

136. Brownlie, *supra* note 129.

137. International Covenant on Civil and Political Rights, Dec. 19, 1966, art. 20, 999 U.N.T.S. 171, 178.

138. Louis Henkin, Editorial Comment, *U.S. Ratification of Human Rights Conventions: The Ghost of Senator Bricker*, 89 Am. J. Int'l L. 341 (1995).

139. Robert Alfert, Jr., *Hostes Humani Generis: An Expanded Notion of U.S. Counterterrorist Legislation*, 6 Emory Int'l L. Rev. 171 (1992).

140. Restatement, *supra* note 43, § 404; *see supra* text accompanying note 59; *see also* Robert Alfert, Jr., *supra* note 139; Kenneth C. Randall, *Universal Jurisdiction Under International Law*, 66 Tex. L. Rev. 785 (1988); *cf.* Oxman, *supra* note 46, at 281; Brownlie, *supra* note 129, at 305.

141. Convention on the Prevention and Punishment of the Crime of Genocide, Dec. 9, 1948, art. III, 78 U.N.T.S. 277, 280.

142. "After the Oklahoma City bombing, the Senate terrorism subcommittee immediately convened hearings on `The Availability of Bomb-Making Information on the Internet,' at which Senator Dianne Feinstein expressed shock that racist militia organizations apparently use the Net to distribute `mayhem manuals' and other bomb-making instructional material and to spread their doctrines on the `Cyberhate' World Wide Web site and other similar outposts." David Post, *New Rules for the Net?*, Am. Law. July/Aug. 1995, at 112.

143. United Nations: General's Report on Aspects of Establishing An International Tribunal for the Prosecution of

Persons Responsible for Serious Violations of International Humanitarian Law in the Territory of the Former Yugoslavia, May 3, 1993, Annex I, art. 4(3), 32 I.L.M. 1159, 1192. [hereinafter Report on Establishing an International Tribunal].

144. *Id.* at 1194.

145. Restatement, *supra* note 43, § 401(b).

146. *Cf.*, *e.g.*, BGHZ 115, 90; Mann, *supra* note 83, at 32; Born, *supra* note 45.

147. Restatement, *supra* note 43, § 421(1).

148. *Id.* § 421 cmt. a.

149. Oxman, *supra* note 46, at 278; *see, e.g.,* Restatement, *supra* note 43, § 422(1) ("A court in the United States may try a person only for violation of United States law, not for violation of the penal law of a foreign state.").

150. Restatement, *supra* note 43, § 421(2).

151. Andreas Lowenfeld, International Litigation and the Quest for Reasonableness 46 (1996).

152. *International Shoe*, 326 U.S. 310, 316 (1945)

[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.* (emphasis added).

153. Restatement, *supra* note 43, § 421 cmt. e; *see also* Convention on Accession to the Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, Oct. 9, 1978, 18 I.L.M. 8, 21 (excluding "tag" service as an acceptable basis on jurisdiction); *cf.* Born, *supra* note 45, at 35.

154. *Cf.* Burnham v. Superior Ct. of Cal., 495 U.S. 604, 615 (1990) (Scalia, J.) ("We do not know of a single state or federal statute, or a single judicial decision resting upon state law, that has abandoned in-state service as a basis of jurisdiction. Many recent cases reaffirm it.").

155. Grace v. MacArthur, 170 F. Supp. 442, 447 (E.D. Ark. 1959) ("It cannot seriously be contended that a person moving in interstate
commerce is on that account exempt from service of process while in transit, and we think, it makes no practical difference whether he is traveling at the time on a plane, or on a bus or train, or in his own car.").

156. Born, *supra* note 45, at 36.

157. Asahi Metal Indus. Co. v. Superior Ct., 480 U.S. 102, 115 (1987) ("Great care and reserve should be exercised when extending our notions of personal jurisdiction into the international field . . . .") (quoting United States v. First Nat'l City Bank, 379 U.S. 378, 404 (1965) (Harlan, J., dissenting)); *see, e.g*., Gates Learjet Corp. v. Jensen, 743 F.2d 1325, 1333 (9th Cir. 1984); FDIC v. British-American Ins. Co., 828 F.2d 1439, 1444 (9th Cir. 1987); Sinatra v. Nat'l Enquirer, Inc., 854 F.2d 1191, 1199 (9th Cir. 1988).

158. Smith v. Hobby Lobby Stores, Inc., 968 F.Supp. 1358 (W.D. Ark. 1997). For further discussion of this case, see *infra* Part II.B.1.a.

159. McDonough v. Fallon McElligot, Inc., 40 U.S.P.Q.2d (BNA) 1826 (S.D. Cla. 1996). For further discussion of this case, see *infra* Part II.B.1.b.

160. Hearst Corp. v. Goldberger, No. 96 Civ. 3620 (PKL)(AJP), 1997 WL 97097 (S.D.N.Y. Feb. 26, 1997); Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd*, No. 96-9344, 1383, 1997 WL 560048 (2d Cir. Sept.

10, 1997); CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996); EDIAS Software Int'l, L.L.C. v. BASIS Int'l Ltd., 947 F. Supp. 413 (D. Ariz. 1996); Resuscitation Tech., Inc., v. Continental Health Care Corp., No. IP 96-1457-C-M/S, 1997 WL 148567 (S.D. Ind. Mar. 24, 1997); Hall v. LaRonde, 66 Cal. Rptr. 2d 399 (Cal. Ct. App. 1997); Pres-Kap, Inc. v. System One, Direct Access, Inc., 636 So. 2d 1351 (Fla. Dist. Ct. App. 1994). For further discussion of these cases, see *infra* Parts II.B.c-i, respectively.

161. *Hearst,* 1997 WL 97097; *Bensusan Restaurant,* 937 F. Supp. 295.

162. *CompuServe,* 89 F.3d 1257; *EDIAS Software Int'l,* 947 F. Supp. 413; *Resuscitation Tech.,* 1997 WL 148567; *Hall,* 66 Cal. Rptr. 2d 399.

163. *Pres-Kap,* 636 So. 2d 1351.

164. *Smith,* 968 F. Supp. 1358 (W.D. Ark. 1997).

165. *Id.* at 1363.

166. *Id.* at 1364.

167. *CompuServe,* 89 F.3d 1257. For further discussion of this case, see *infra* Part II.B.1.e.

168. *Zippo Mfg.,* 952 F. Supp. 1119. For further discussion of this case, see *infra* Part II.B.2.e.

169. *Smith,* 968 F. Supp. at 1365.

170. *McDonough,* 40 U.S.P.Q.2d (BNA) 1826 (S.D. Cal. 1996).

171. *Id.* at 1828.

172. *Id.* at 1827.

173. *Id.* at 1829.

174. *Id.*

175. *Id.* at 1828-29; *cf*. IDS Life Ins. Co. v. SunAmerica, Inc., 958 F. Supp. 1258, 1288 (N.D. Ill. 1997) ("It cannot plausibly be argued that any defendant who advertises nationally could expect to be haled into court in any state, for a cause of action that does not relate to the advertisements.").

176. *Hearst,* No. 96 Civ. 3620 (PKL)(AJP), 1997 WL 97097 (S.D.N.Y. Feb. 26, 1997).

177. *Id.* at *4.

178. *Id.* at *20. The court cited three cases discussed *infra* Part II.B.2.: *Maritz, Inc. v. Cybergold, Inc.*, 947 F. Supp. 1328 (E.D. Mo. 1996); *Inset Systems, Inc. v. Instruction Set, Inc.*, 937 F. Supp. 161 (D. Conn. 1996); and *Heroes, Inc. v. Heroes Foundation*, 958 F. Supp. 1 (D.D.C. 1996).

179. *Hearst,*1997 WL 97097, at *1; *see also* Naxos Resources (U.S.A.) Ltd. v. Southam Inc., 24 Media L. Rep. 2265 (C.D. Cal. 1996) (stating that publication via the Internet, LEXIS, and WESTLAW should not make a party vulnerable to jurisdiction in every state).

180. *Hearst*, 1997 WL 97097, at *10.

181. *Id.* at *12.

182. *Id.* at *13.

183. *Id.* at *15.

184. *Bensusan Restaurant*, 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd* No. 96-9344, 1383, 1997 WL 560048 (2d Cir. Sept. 10, 1997).

185. *Id.* at 301.

186. *Id.* at 297.

187. *Id.*

188. Lori I. Bauman, *Personal Jurisdiction and Internet Advertising*, The Computer Law., Jan. 1997, at 4 (citing Asahi Metal Indus. Co. v. Superior Ct. of Cal., 480 U.S. 102 (1992)).

189. *Bensusan Restaurant*, 937 F. Supp. at 301; *see also* Graphic Controls Corp. v. Utah Medical Products, Inc., No. 96-CV-0459E(F),
1997 WL 276232 (W.D.N.Y. May 21, 1997) (finding that Internet advertisement for medical goods did not constitute purposeful availment of New York where customers were given a nationwide telephone number to contact the company).

190. *Bensusan Restaurant*, 937 F. Supp. at 299.

191. *CompuServe*, 89 F.3d 1257 (6th Cir. 1996). For further discussion of this case, see *infra* Part II.B.1.e.

192. *CompuServe*, 89 F.3d 1257.

193. *Id.*

194. *Id.* at 1260.

195. *Id*.

196. *Id.* at 1261.

197. *Id.*

198. *Id.* at 1265.

199. *Id.* (citations omitted).

200. *Id.* at 1263.

201. *Id.* at 1268.

202. *Id.*; *cf.* State v. Interactive Gaming & Comm. Corp., No. CV97-7808, (Mo. Cir. Ct. May 23, 1997) (on-line offer to provide gambling services in exchange for payment of a registration fee was accepted in Missouri, causing a contract within the state).

203. *EDIAS Software Int'l*, 947 F. Supp. 413 (D. Ariz. 1996).

204. California Software, Inc. v. Reliability Research, Inc., 631 F. Supp. 1356 (C.D. Cal. 1986). For further discussion of this case, see *infra* Part II.B.2.a.

205. *EDIAS Software Int'l*, 947 F. Supp. at 420 (citation omitted).

206. *Id.* at 417-21.

207. *California Software*, 631 F. Supp. 1356. For further discussion of this case, see *infra* Part II.B.2.a.

208. *EDIAS Software Int'l*, 947 F. Supp. at 421.

209. *Id.* at 421-22.

210. *Id.* (quoting Asahi Metal Indus., Co., v. Superior Ct. of Cal., 480 U.S. 102, 102-3 (1987)).

211. *Id.* at 421; *see also* Cody v. Ward, 954 F. Supp. 43, 47 n.8 (D. Conn. 1997) (finding that out-of-state defendant's e-mail messages and telephone calls to plaintiff in Connecticut were sufficient purposeful minimum contacts).

212. *EDIAS Software Int'l*, 947 F. Supp. at 422.

213. *Id.*

214. *Resuscitation Tech*., No. IP 96-1457-C-M/S, 1997 WL 148567 (S.D. Ind. Mar. 24, 1997).

215. *Id.* at *2.

216. *Id.*

217. *Id.* at *2-3.

218. *Id.* at *4 (citation omitted). The court crafted its "nature and content" language based on other Internet case opinions. *Id.* (citing CompuServe Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996) (*see* discussion *supra* Part II.B.1.e); Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Penn. 1997) (*see* discussion *infra* Part II.B.2.e); and *EDIAS Software Int'l*, 947 F. Supp. 413 (*see* discussion *supra* Part II.B.1.f)).

219. *Id.* at *5.

220. *Id.* at *6.

221. *Id.*

222. *Zippo Mfg.*, 952 F. Supp. 1119. For further discussion of this case, see *infra* Part II.B.2.e.

223. *Resuscitation Tech*., No. IP 96-1457-C-M/S, 1997 WL 148567, at *4 ("Because the object of the defendant was to assign passwords and sell its Internet news service to residents of the forum state, the court found that its intended object was to transact business in that state.").

224. *Id.* at *5.

225. *Hall*, 66 Cal. Rptr. 2d 399 (Cal. Ct. App. 1997).

226. *Id.* at 402.

227. A more troublesome case, for example, is *Cody v. Ward*, 954 F. Supp. 43 (D. Conn. 1997), where the court held that four telephone calls and fifteen e-mails to Connecticut established sufficient minimum contacts. This made it unnecessary to decide whether defendant's 225 fraudulent messages on Prodigy should be counted as purposeful contacts with Connecticut. The court avoided the question of whether posting information on a bulletin board system warranted a finding of jurisdiction.

228. *Pres-Kap*, 636 So. 2d 1351 (Fla. Dist. Ct. App. 1994). For a criticism of this case, see Michael J. Santisi, Note, *Pres-Kap, Inc. v. System One, Direct Access, Inc.: Extending the Reach of the Long-Arm Statute through the Internet?*, 13 J. Marshall J. Computer & Info. L. 433 (1995).

229. *Pres-Kap*, 636 So. 2d at 1353.

230. *Id.*

231. *Granite Gate Resorts*, No. C6-95-7227, 1996 WL 767431 (Minn. Dist. Ct. Dec. 11, 1996) (denying defendant's motion to dismiss for lack of jurisdiction), *aff'd sub. nom.*, Humphrey v. Granite Gate Resorts, Inc., 568 N.W.2d 715 (Minn. Ct. App. 1997).

232. *California Software*, 631 F. Supp. 1356 (C.D. Cal. 1986).

233. *Id.* at 1358.

234. *Id.* at 1360.

235. *Id.* at 1360; *see also* Naxos Resources (U.S.A.) Ltd. v. Southam Inc., 24 Media L. Rep. 2265, 2267 (C.D. Cal. Aug. 16, 1996) (quoting *California Software*, 631 F. Supp. at 1360) (disseminating articles via the Internet, LEXIS, and WESTLAW is not sufficient to establish general jurisdiction).

236. *Data Disc*, 557 F.2d 1280 (9th Cir. 1977).

237. *California Software*, 631 F. Supp. at 1361; *see also Naxos Resources*, 24 Media L. Rep. at 2267 (holding that Canadian defendants purposefully availed themselves of doing business in California where newspapers were published on LEXIS, which is available to Californians, and distributed in California).

238. *California Software*, 631 F. Supp. at 1362; *cf. Naxos Resources*, 24 Media L. Rep. at 2268 (holding that limited jurisdiction was unavailable because the forum state was not the focus of the newspaper story and the harm suffered).

239. *California Software*, 631 F. Supp. at 1363.

240. This test is a domestic standard, distinct from the international law "reasonableness" standard.

241. The factors of the test are as follows:

(A) the extent of the purposeful interjection into the forum state;

(B) the burden on the defendant of defending in the forum;

(C) the extent of conflict with the sovereignty of defendant's state;

(D) the forum state's interest in adjudicating the dispute;

(E) the most efficient judicial resolution of the controversy;

(F) the importance of the forum to plaintiff's interest in convenient and effective relief; and

(G) the existence of an alternative forum.

California Software, 631 F. Supp. at 1363 (citations omitted).

An allegedly libelous article published in a print magazine and disseminated worldwide was not enough for the 9th Circuit to hale Swedish scholars into California under the same seven-factor test. Core-Vent Corp. v. Nobel Indus. AB, 11 F.3d 1482 (9th Cir. 1993).

242. *California Software*, 631 F. Supp. at 1364.

243. *Digital Equip.*, 960 F. Supp. 456 (D. Mass. 1997).

244. *Id.* at 463.

245. *Id.* at 464.

246. *Id.* at 466-67.

247. *Id.* at 462-63.

248. *Id.* at 467.

249. *Id.* at 470; *cf.* Cody v. Ward, 954 F. Supp. 43, 47 (D. Conn. 1997) (holding that where defendant posted messages via Prodigy specifically to plaintiff, the court could find jurisdiction based on telephone calls and e-mails, choosing not to address whether the Prodigy messages were "purposeful contacts" with Connecticut).

250. *Id.* at 470-71.

251. *Id.* at 471.

252. *Id.* at 469.

253. *Granite Gate Resorts*, No. C6-95-7227, 1996 WL 767431 (Minn. Dist. Ct. Dec. 11, 1996), *aff'd sub. nom.*, Humphrey v. Granite Gate Resorts, Inc., 568 N.W.2d 715 (Minn. Ct. App. 1997).

254. *Id.* at *2.

255. Interestingly, the court in *State v. Interactive Gaming & Communications Corp.*, No. CV97-7808 (Mo. Cir. Ct. May 23, 1997) spared the Grenada corporation by treating the parent company as its alter ego, thereby avoiding international complications.

256. *Inset Sys.*, 937 F. Supp. 161 (D. Conn. 1996). For further discussion of this case, see *infra* Part II.B.2.f.

257. *Granite Gate Resorts*, 1996 WL 767431, at *7.

258. *Id.*

259. *Playboy Enter., Inc., v. Chuckleberry Publ'g., Inc*., 939 F. Supp. 1032 (S.D.N.Y. 1996). For further discussion of this case, see *supra* Part II.A.2.c.(1)(b).

260. *Granite Gate Resorts*, 1996 WL 767431, at *9.

261. *Id.* at *10.

262. *Id.* at *11.

263. *Id.*

264. *Id.*

265. *Id.* Probably, the court was enraged by the overreaching forum clause, calling it the "coup de grace."

266. *California Software*, 631 F. Supp. 1356 (C.D. Cal. 1986). For further discussion of this case, see *supra* Part II.B.2.a.

267. *Granite Gate Resorts*, 1996 WL 767431, at *6.

268. *See id.* at *9.

269. *Heroes*, 958 F. Supp. 1 (D.D.C. 1996).

270. Inset Sys., Inc., v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996). For further discussion of this case, see *infra* Part II.B.2.f.

271. Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd* No. 96-9344, 1383, 1997 WL 560048 (2d Cir. Sept. 10, 1997). For further discussion of this case, see *supra* II.B.1.d.

272. *Heroes*, 958 F. Supp. at 5.

273. *Id.* at 4.

274. *Id.* at 4-5.

275. *Id.* at 5.

276. *See infra* Part II.B.2.f.

277. *Zippo Mfg.*, 952 F. Supp. 1119 (W.D. Pa. 1997).

278. *Id.* at 1121.

279. *Id.*

280. *Id.* at 1124.

281. *Id.* at 1125.

282. CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996). For further discussion of this case, see *supra* Part II.B.1.e.

283. *Zippo Mfg.*, 925 F. Supp. at 1126.

284. *Id.* at 1125-26.

285. *Id.* at 1127.

286. *Id.*

287. *Inset Sys.*, 937 F. Supp. 161 (D.Conn. 1996).

288. *Id.* at 162-63.

289. *Id.* at 164.

290. *Id.* at 165; *but see* IDS Life Ins. Co. v. SunAmerica, Inc., 958 F. Supp. 1258, 1268 (N.D. Ill. 1997) (stating general advertising on the Internet was insufficient for jurisdiction in Illinois where company had no property, was not registered to do business, paid no taxes, had no offices or employees, and did not make sales or offer services in Illinois).

291. *Inset Sys.*, 937 F. Supp. at 165. *But see* Expert Pagers v. Buckalew, No. C-97-2109-VRW, 1997 WL 488011 (N.D. Cal. Aug 6, 1997). In *Expert Pages*, the copying of a California plaintiff's copyrighted material was considered direct activity in California which caused injury within the state. This established minimum contacts in the view of the court. *Id.* at *3. Defendant, a "young adult" living in Virginia, allegedly violated plaintiff's copyright by making a copy of its Web site to send disparaging messages to the site's advertisers and offer a similar service through his own Web

site. The court noted that the pro se defendant's business "does not appear to have been terribly successful . . . ." *Id.* at *4. The court stated, "In view of his limited contact with California and the overwhelming burden that defending this case in this district would impose on defendant, the exercise of personal jurisdiction in this case would be constitutionally unreasonable." *Id.* at *5. However, the court stated: "The smaller the element of purposeful interjection, the less is jurisdiction to be anticipated and the less reasonable is its exercise." *Id.* at *3 (quoting Insurance Co. of N. Am. v. Marina Salina Cruz, 649 F.2d 1266, 1271 (9th Cir. 1981)).

292. *Maritz*, 947 F. Supp. 1328 (E.D. Mo. 1996).

293. *Id.* at 1330.

294. *Id.*

295. *Id.* at 1333.

296. *Id.* at 1332.

297. *Id.* at 1333.

298. *Id.* The court stated that if plaintiff's contacts were to be considered, a plaintiff could always try to create personal jurisdiction. Thus, the court implicitly followed the line of reasoning in *Hanson v. Denckla*, 357 U.S. 235, 253 (1958) ("The unilateral activity of those who claim some relationship with a non-resident defendant cannot satisfy the requirement of contact with the forum State.").

299. *Maritz*, 947 F. Supp. at 1333.

300. California Software, Inc., v. Reliability Research, Inc., 631 F. Supp. 1356 (C.D. Cal. 1986). For further discussion of this case, see *supra* Part II.B.2.a.

301. Inset Sys., Inc., v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996). For further discussion of this case, see *supra* Part II.B.2.f.

302. *Maritz*, 947 F. Supp. at 1334.

303. *Id.*

304. Minnesota Memorandum, *supra* note 94. For further discussion of this case, see *supra* Part II.A.2.c.(1)(d).

305. *But see*, *e.g.*, Message posted by cyber-rights@cpsr.org (Mar. 19, 1996) (available at Cyber-Rights Library) <http://www.cpsr.org/cpsr/nii/cyber-rights/Library/> (announcing the Virtual Magistrate Project, which shall assist in the resolution of private computer network disputes). The magistrates will be selected jointly by the American Arbitration Association and the Cyberspace Law Institute, both private institutions. The acceptance of these magistrates in the international network community is, however, uncertain. It is obvious that States would not recognize the competence of a judicial body consisting exclusively of nationals from one state or one legal system. *Id.*; *see also Gov't Proposes International Court to Deal with Internet*, The China Post, May 19, 1997, at 12; *cf.* Statute of the International Court of Justice, June 26, 1945, art. 3 § 1 ("The Court shall consist of fifteen members, no two of whom may be nationals of the same state.") and art. 9 ("At every election, the electors shall bear in mind not only that the persons to be elected should individually possess the qualifications required, but also that in the body as a whole the representation of the main forms of civilization and of the principal legal systems of the world should be assured.").

306. Robert A. Bourque & Kerry L. Conrad, *Avoiding Remote Jurisdiction Based on Internet Web Site*, N.Y. L.J. Dec. 10, 1996, at 1.

307. *Id.*

308. *Id.*

309. *Id.*

310. *Id.*

311. Restatement, *supra* note 43, § 421.

312. In 1983, the CIA, for example, produced a manual entitled *Operaciones sicológicas en guerra de guerrillas* which taught how to commit warcrimes. The CIA disseminated it to the so-called contras who fought against the government of Nicaragua. The International Court of Justice found that the USA thereby encouraged the commission of acts contrary to general principles of humanitarian law. Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.) 1986 I.C.J. 14, 148 (June 27); Tim Weiner, *C.I.A. Taught, Then Dropped, Mental Torture in Latin America*, N.Y. Times, Jan. 29, 1997, at A11. Posting this manual on the Net with the intention to make it available to people who use this knowledge would arguably pass the muster of aiding and abetting in war crimes.

313. Report on Establishing an International Tribunal, *supra* note 143, at 1192, Annex.

314. *Id.* Annex, art. 7.

315. *Id.* Annex, art. 9.

316. Restatement, *supra* note 43, § 401(c).

317. *Cf. FTC Halts Internet Pyramid Scheme*, FTC Press Release, May 29, 1997

<http://www.ftc.gov/opa/9605/fortuna.htm>; *DOT Assesses Penalty for Advertising*

Violations on the Internet, DOT Press Release, Nov. 21, 1995

<http://www.dot.gov/cgi-bin/AT-serversearch.cgi>.

318. Oxman, *supra* note 46, at 277-278; Mann, *supra* note 83, at 34. *But see* Restatement, *supra* note 43, § 431(1) ("A state may employ judicial or nonjudicial measures to induce or compel compliance or punish non-compliance with its laws or regulations, provided it has jurisdiction to prescribe in accordance with §§ 402 and 403.").

319. Restatement, *supra* note 43, § 432(2).

320. Mann, *supra* note 83, at 39; Brownlie, *supra* note 129, at 307; Whish, *supra* note 81, at 374; Federal Trade Comm. v. Compagnie de Saint-Gobain-Pont-à-Mousson, 636 F.2d 1300, 1304 (D.C. Cir. 1980) ("[T]he *act of service itself* constitutes an exercise of American sovereign power within the area of the foreign country's territorial sovereignty.").

321. Wolf Okresek, *Hoheitsakte auf fremdem Hoheitsgebiet—Eine Betrachtung anhand praktischer Fälle* [*Sovereign Acts in Foreign Territories—An Observation in Light of Practical Cases*], 35 Österreichische Zeitschrift für öffentliches Recht und Völkerrecht [Aus. J. Pub. Int'l L.] 331 (1985); *cf.* Michael J. Glennon, *Liaison and the Law: Foreign Intelligence Agencies' Activities in the United States*, 25
Harv. Int'l L.J. 1, 11 (1984) ("[S]uch surveillance would seem to interfere with the sovereignty of the United States.").

322. Restatement, *supra* note 43, § 432 reporters' n. 1.

323. Claus Schellenberg, *The Proceedings Against Two French Customs Officials in Switzerland for Prohibited Acts in Favor of a Foreign State, Economic Intelligence Service and Violation of the Banking Law*, 9 Int'l Bus. Law. 139 (1981) (translating art. 271 para. 1 of the Swiss Penal Code as follows: "[w]hoever performs on Swiss territory without being authorized any acts in favor of a foreign state which are reserved to a public authority or to a public official . . . whoever furthers any such acts, shall be punished with imprisonment, in severe cases with penal servitude.").

324. *Cf.* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 Emory L.J. 869, 882 (1996). The example comes from Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 Yale L.J. 1093 (1996).

325. *See, e.g.*, Sabine Nuss, *Die Welt Online, Staubsauger im Internet: Wie der Bundesnachrichtendienst das Datennetz überwacht* [*Vacuum Cleaner in the Internet: How the German Secret Service Keeps the Data Net Under Surveillance*] (March 22, 1996) <http://www.welt.de/archiv/1996/03/22/0322de03.htm>; *see also* Thomas J. Lueck, *3 Are Arrested on Evidence From an Internet Wiretap*, N.Y. Times, Dec. 30, 1995, at 42; John Markoff, *U.S. Rebuffed in Global Proposal For Eavesdropping on the Internet*, N.Y. Times, Mar. 27, 1997, at A1; Christopher Wolf & Scott Shorr, *Cybercops Are Cracking Down on Internet Fraud*, Nat'l L.J., Jan. 13, 1997, at B12.

326. X (Belgian Citizen) v. Swiss Fed. Prosecutor's Office, 10 EuGRZ 435 (Judgment of 15 July 1982) (Swiss Federal Tribunal, Lausanne, P1201/81/fs 1983). Additionally, see the legal opinion of Hans Schultz written on behalf of X, *Male Captus, Bene Deditus?*, 40 Schweizerisches Jahrbuch für Internationales Recht 93 (1984).

327. As Belgium does not extradite its own nationals, a request to Belgium would have been senseless.

328. *Romano*, 706 F.2d 370 (2d Cir. 1983).

329. *Id.* at 375. Compare the position of the U.S. Government in *United States v. Yunis*, 681 F. Supp. 909, 916 n.11 (D.C. Cir. 1988), *rev'd on other grounds*, 859 F.2d 953 (D.C. Cir. 1988).

330. Federal Trade Comm'n v. Compagnie de Saint-Gobain-Pont-à-Mousson, 636 F.2d 1300 (D.C. Cir. 1980); Mann, *supra* note 83, at 39.

331. *Cf*. Interview with Edzard Schmidt-Jortzig, German Minister of Justice, *in* "Der Nationalstaat ist Überholt" [*The National State is Antiquated*], Der Spiegel (Nov. 1996) <http://www.spiegel.de/special/heft2/schmidt-jortzig.html> [hereinafter Schmidt-Jortzig Interview] (indicting the belief that everybody may surf the Net, but that the Secret Service may not assume the role of a data police without statutory authorization).

332. *Cf.* Santiago Torres Bernardez, *Territorial Sovereignty*, Encyclopedia of Public International Law 487, 491 (Rudolf Bernhardt ed., Instalment 10 1988).

333. John Perry Barlow, *A Declaration of the Independence of Cyberspace* (posted Feb. 9, 1996) <http://memex.org/barlow.html>. The declaration was promulgated on February 8, 1996, surprisingly not in cyberspace, but in Davos, Switzerland. Had the Swiss authorities taken this act seriously, Barlow might have gotten in diplomatic trouble because Switzerland is very strict concerning acts of foreign sovereign entities on its territory. For a comprehensive study of relevant Swiss practice, see Dave Siegrist, Hoheitsakte auf fremdem Staatsgebiet [Sovereign Acts in Foreign National Territories] (1987).

334. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, *opened for signature* Jan. 27, 1967, 610 U.N.T.S. 205; Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, *opened for signature* Dec. 5, 1979, 1363 U.N.T.S. 3.

335. United Nations Convention on the Law of the Sea, *opened for signature* Dec. 10, 1982, pt. XI, arts. 133-85; Annexes III and IV, U.N. Doc. A/CONF. 62/122, Dec. 10, 1982.

336. Antarctic Treaty, Dec. 1, 1959, 402 U.N.T.S. 71; Convention for the Conservation of Antarctic Seals, June 1, 1972, 29 U.S.T. 441; Conservation of Antarctic Marine Living Resources, May 20, 1980, 33 U.S.T. 3476.

337. *See* Dale M. Cendali & James D. Arbogast, *Net Use Raises Issues of Jurisdiction*, Nat'l L.J., Oct. 28, 1996, at C7. The new approach of the U.S. government is to focus on the site of origin. Clinton & Gore, *supra* note 34, pt. III.8 ("The rules of the `country-of-origin' should serve as the basis for controlling Internet advertising to alleviate national legislative roadblocks and trade barriers."); *cf.* Bauman, *supra* note 188, at 6.

338. Richard Raysman & Peter Brown, *Computer Law: On-Line Legal Issues*, N.Y. L.J., Feb. 15, 1995, at 3.

339. Born, *supra* note 45, at 29.

340. *See* Schmidt-Jortzig Interview, *supra* note 331. The German Minister of Justice sees the first step in an European Agreement on the Liability of Internet Service Provider. The step in his view could be a worldwide convention, even though he acknowledges that the U.S. government would never sign an agreement that outlaws Holocaust-revisionist material. *Id.*

341. OECD, *Inform@tion, Computer and Communications Policy* (last modified Sept. 19, 1997) <http://www.oecd.org/dsti/sti_ict.html>. The initiative was particularly welcomed by the Ministerial Conference. *See* Ministerial Conference, *supra* note 17, ¶ 66.

342. Ministry of Postal Services, Telecomm. and Space, *Agreement on International Co-operation with Regard to the Internet: Draft French Contribution to the Preparatory Work for the OECD Ministerial Conference*, (Oct. 23, 1996)

<http://www.telecom.gouv.fr/english/activ/techno/charteint.htm>. The purposes of the proposed agreement are to "better apprehend the characteristics of [the Internet], to enhance their substantial potential, both at an economic and cultural level, and to combat illegal activities." *Id*. pmbl.

343. *Illegal and Harmful Content on the Internet*, *supra* note 6.

344. *Id*.

345. *Id.* pt. 6.1.a.

346. *Id.* pt. 6.3.b.

347. Ministerial Conference, *supra* note 17, ¶ 65.

348. *Id.* ¶ 66.

349. Clinton & Gore, *supra* note 34, pt. III.8.

350. Civil libertarian groups, such as the American Civil Liberties Union and the Electronic Frontier Foundation, say it is time for a "sweeping landmark case that clarifies the gray legal issues of cyberspace." Howard Bryant, *CompuServe Stirs Debate of Censorship*, San Jose Mercury News, Jan 21, 1996. It is, however, not clear which court should decide a landmark case on international jurisdiction in cyberspace. Cases like *Société Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522 (1987), *United States v. Alvarez-Machain*, 504 U.S. 655 (1992), and *Hartford Fire Ins. Co. v. California*, 509 U.S. 764 (1993) did not strengthen the reputation of the U.S. Supreme Court as a reliable adjudicator of international law. *But see Gov't Proposes International Court to Deal with Internet*, The China Post, May 19, 1997, at 12.

351. Barnes, *supra* note 133. For the mechanics of how "anonymity" is effected over the Internet, see, for example, A. Michael Froomkin, *Anonymity and Its Enemies*, 1995 J. Online L. art. 4 <http://www.law.cornell.edu/jol/froomkin.htm>; *see also* A. Michael Froomkin, *It Came From the Planet Clipper: The Battle Over Cryptographic Key "Escrow"*, 1996 U. Chi. Legal F. 15.