JURISDICTION IN CYBERSPACE: A THEORY OF INTERNATIONAL SPACES

Darrel C. Menthe*


INTRODUCTION ........................................................................................ 69
I. PRINCIPLES OF JURISDICTION................................................................. 71
II. THE THEORY OF THE UPLOADER AND THE DOWNLOADER .......... 73
III. REJECTING TERRITORIALITY: THE TROUBLE WITH MINNESOTA ... 75
IV. REJECTING TERRITORIALITY: “THE LAW OF THE SERVER” ............ 79
V. THE THEORY OF INTERNATIONAL SPACES ........................................... 83
   A. Overview......................................................................................... 83
   B. Evolution of International Law ....................................................... 85
   C. The Case for International Spaces ................................................... 87
      1. History ...................................................................................... 87
      2. Jurisdiction in Antarctica............................................................ 88
      3. Jurisdiction in Outer Space.......................................................... 91
      4. Jurisdiction in Cyberspace:
         The Vessel of Nationality ............................................................ 93
VI. JURISDICTION IN CYBERSPACE: A PREVIEW .................................. 97
   A. Copyright Law ............................................................................. 97
   B. Libel.............................................................................................. 99
VII. CONCLUSION ...................................................................................... 101

INTRODUCTION

Where is cyberspace? The answers to this question seem to approach the metaphysical: it is everywhere and nowhere; it exists in the

* Darrel C. Menthe, J.D. Stanford ‘96, is a litigation associate in the Los Angeles office of Fried, Frank, Harris, Shriver & Jacobson. This article would not have been completed without the help of many people, a few of whom deserve special recognition and acknowledgment here. My heartfelt gratitude goes to Margaret J. Radin, without whose support and guidance this article would never have been completed, to David Lange, Patrick Eagleman and the MTTLR staff, for an incisive but merciful edit, and to Ward Breeze, whose loyal encouragement was in no small measure responsible for the submission of this piece.

1. The term “cyberspace” is sometimes treated as a synonym for the Internet, but is really a broader concept. For example, we know exactly how the Internet began, but not at
smallest bursts of matter and energy and is called forth only by the presence of man through the intercession of an Internet provider. If the answers are useless, it only shows that we are asking the wrong question. We should first ask: *what* is cyberspace? To this question at least a functional answer is possible. Functionally, cyberspace is a place. It is a place where messages and webpages are posted for everyone in the world to see, if they can find them. The United States Supreme Court’s first opinion about the Internet contains language that makes one hopeful that U.S. courts will accept the legal metaphor of cyberspace as a place outside national boundaries: “Taken together, these tools constitute a unique medium—known to its users as ‘cyberspace’—located in no particular geographical location but available to anyone, anywhere in the world, with access to the internet.”

Unfortunately, when the law confronts cyberspace the usual mode of analysis is analogy, asking not “What *is* cyberspace?” but “What *is* cyberspace *like*?” The answers are varied: a glorified telephone, a bookstore, a bulletin board. I propose that we look at cyberspace not in these prosaic terms, but rather through the lens of international law in order to give cyberspace meaning in our jurisprudence.

The thesis of this paper is that there exists in international law a type of territory which I call “international space.” Currently there are three such international spaces: Antarctica, outer space, and the high seas. For jurisdictional analysis, cyberspace should be treated as a fourth international space.

In cyberspace, jurisdiction is the overriding conceptual problem for domestic and foreign courts alike. Unless it is conceived of as an international space, cyberspace takes all of the traditional principles of

---

2. In his book *Wyrms*, science fiction author Orson Scott Card describes a most remarkable place called Heffiji’s house, which could have been a metaphor for cyberspace. Heffiji had a sign on her house reading “Answers” that lured many curious people. She asked questions of all her visitors and wrote the answers down on scraps of paper. These scraps of paper were scattered all around her enormous house. Unfortunately she had no brain, so she could not learn anything. She did, however, know where she had put the pieces of paper, and you could learn anything from her if you asked the right question. *Orson Scott Card, Wyrms* 165–188 (1987).


4. It is hornbook custom to cite *The Paquete Habana* for the proposition that, “international law is part of our law.” *The Paquete Habana*, 175 U.S. 677 (1900).
conflicts-of-law and reduces them to absurdity. Unlike traditional jurisdictional problems that might involve two, three, or more conflicting jurisdictions, the set of laws which could apply to a simple homespun webpage is *all of them*. Jurisdiction in cyberspace requires clear principles rooted in international law. Only through these principles can courts in all nations be persuaded to adopt uniform solutions to questions of Internet jurisdiction.

I. PRINCIPLES OF JURISDICTION

There are three types of jurisdiction generally recognized in international law. These are: (1) the jurisdiction to prescribe; (2) the jurisdiction to enforce; and (3) the jurisdiction to adjudicate.5 The jurisdiction to prescribe is the right of a state to make its law applicable to the activities, relations, the status of persons, or the interests of persons in things.6 This paper deals almost exclusively with the jurisdiction to prescribe. It is useful at this point, however, to note the distinction between the jurisdiction to prescribe a rule of law for a particular action and the jurisdiction to enforce that rule. This paper will not discuss extradition.

Under international law, there are six generally accepted bases of jurisdiction or theories under which a state may claim to have jurisdiction to prescribe a rule of law over an activity. In the usual order of preference, they are:

1. Subjective Territoriality
2. Objective Territoriality
3. Nationality
4. Protective Principle
5. Passive Nationality
6. Universality

As a general rule of international law, even where one of the bases of jurisdiction is present, the exercise of jurisdiction must be reasonable.7

Subjective territoriality is by far the most important of the six. If an activity takes place within the territory of the forum state, then the

---

6. *Id.* § 402.
7. *Id.* § 403.
forum state has the jurisdiction to prescribe a rule for that activity. The vast majority of criminal legislation in the world is of this type.

Objective territoriality is invoked where the action takes place outside the territory of the forum state, but the primary effect of that activity is within the forum state. The classic case is that of a rifleman in Canada shooting an American across Niagara Falls in New York. The shooting takes place in Canada; the murder—the effect—occurs in the United States. The United States would have the jurisdiction to prescribe under this principle. This is sometimes called “effects jurisdiction” and has obvious implications for cyberspace which will be discussed below.

Nationality is the basis for jurisdiction where the forum state asserts the right to prescribe a law for an action based on the nationality of the actor. Under the law of the Netherlands, for example, a Dutch national “is liable to prosecution in Holland for an offence committed abroad, which is punishable under Netherlands law and which is also punishable under the law of the country where the offence was committed.” Many other civil law countries have similar laws.

Passive nationality is a theory of jurisdiction based on the nationality of the victim. Passive and “active” nationality are often invoked together to establish jurisdiction because a state has more interest in prosecuting an offense when both the offender and the victim are nationals of that state. Passive nationality is rarely used for two reasons. First, it is offensive for a nation to insist that foreign laws are not sufficient to protect its citizens abroad. Second, the victim is not being prosecuted. A state needs to seize the actor in order to undertake a criminal prosecution.

The Protective principle expresses the desire of a sovereign to punish actions committed in other places solely because it feels threatened by those actions. This principle is invoked where the “victim” would be the government or sovereign itself. For example, in United States v. Rodriguez, the defendants were charged with making false statements in immigration applications while they were outside the United States. This principle is disfavored for the obvious reason that it can easily offend the sovereignty of another nation.

The final basis of jurisdiction is universal jurisdiction, sometimes referred to as “universal interest” jurisdiction. Historically, universal interest jurisdiction was the right of any sovereign to capture and punish pirates. This form of jurisdiction has been expanded during the past

century and a half to include more of *jus cogens*: slavery, genocide, and hijacking (air piracy). Although universal jurisdiction may seem naturally extendable in the future to Internet piracy, such as computer hacking and viruses, such an extension is unlikely given the traditional tortoise-like development of universal jurisdiction. Just as important, universal jurisdiction traditionally covers only very serious crimes. As a result, all nations have due process type problems with convictions under this principle.

The general mode of international conflict of law analysis is to weigh the interests of competing states in determining whether jurisdiction to prescribe exists. Although subjective territoriality usually trumps other interests, a strong state interest in protecting its nationals can outweigh a weak state interest in prosecuting the crime on its own soil.

It is not always clear what the result will be for an individual defendant if a state lacks the jurisdiction to prescribe law. Under some domestic legal systems, a defendant will be released if the court convicted the defendant where it had no jurisdiction to prescribe. In the United States, this question is intertwined with due process analysis and presumptions about the intent of Congress not to violate international law.

At a minimum, under international law a claim will accrue to the state whose sovereignty is offended by the conviction of its national.

II. The Theory of the Uploader and the Downloader

The public interacts with cyberspace in two primary ways: either putting information into cyberspace or taking information out of cyberspace. At law in cyberspace, then, there are two distinct actors: the uploader and the downloader. Under this theory, the uploader and the downloader act like spies in the classic information drop—the uploader puts information into a location in cyberspace, and the downloader accesses it at a later time. Neither need be aware of the other’s identity.

---


11. See, e.g., U.S. Const. art. I, § 8, cl. 10 (granting Congress the right “To define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations”).

12. The court will construe U.S. law to conform to international law where possible. See Restatement (Third) of Foreign Relations § 114 (1986).

13. I speak here of “one-to-many” Internet communications, rather than direct (“one-to-one”) communication over the Internet, such as email. I will address the latter topic later in the paper. Suffice it to say now that these direct communications do not present the same conflict of law problems as general postings to the world.
Unlike the classic information drop, however, there need not be any specific intent to communicate at all. Some areas of the Internet are accessed by hundreds of thousands of people from all over the world, while others languish as untrodden paving stones on the seemingly infinite paths of cyberspace.

In both civil and criminal law, most actions taken by uploaders and downloaders present no jurisdictional difficulties. A state can forbid, on its own territory, the uploading and downloading of material it considers harmful to its interests. A state can therefore forbid anyone from uploading a gambling site from its territory, and can forbid anyone within its territory from downloading, i.e. interacting, with a gambling site in cyberspace. For example, the Supreme Court recently declared the “Communications Decency Act” (CDA) unconstitutional for overbreadth and vagueness on a facial challenge, but therefore did not have a chance to address its international implications. Quite apart from the internal limitations of the U.S. Constitution, there is little doubt that, under international law, the United States has the jurisdiction to prescribe law regulating the content of what is uploaded from United States territory. Had the Supreme Court been presented with an actual case or controversy concerning the application of the CDA to a foreign national resident abroad, the Supreme Court would have had to consider the extraterritorial application of the law as written, and could have been expected to apply the presumption against extraterritoriality and to have circumscribed the CDA in that regard.

Two early American cases demonstrate how this theory would be manifest. The Schooner Exchange held that a French war vessel was not subject to American law, although it was in an American port. Similarly, a webpage would be ascribed the nationality of its creator, and thus not be subject to the law of wherever it happened to be downloaded.

The Cutting Case provides an example of how anuploader should be viewed in a foreign jurisdiction that is offended by material uploaded into cyberspace. Mr. Cutting published an article in Texas which offended a Mexican citizen. When Mr. Cutting visited Mexico he was

14. Interacting may involve considerably more than downloading, but it always involves the act of downloading.
16. The Schooner Exchange v. McFaddon, 11 U.S. (7 Cranch) 116 (1812). We can ignore for now the question of whether the ship’s status as a war vessel was dispositive. The “temporary presence” doctrine was elaborated in later cases.
17. See Letter, Secretary of State to United States Ambassador to Mexico. Department of State, Washington, November 1, 1887 (reprinted in part in, Joseph Sweeney, et al., The International Legal System 90–93) (emphasis added).
incarcerated on criminal libel charges. The United States Secretary of State instructed the U.S. ambassador in Mexico to inform the Mexican government that, “[T]he judicial tribunals of Mexico were not competent under the rules of international law to try a citizen of the United States for an offense committed and consummated in his own country, merely because the person offended happened to be a Mexican.”

As a general proposition, where uploading certain material is a crime, it is an offense “committed and consummated” in the state where the uploader is located.

III. Rejecting Territoriality: The Trouble with Minnesota

What many states want to do is altogether more troubling. Several states seek to exercise jurisdiction over uploaders (and to a lesser extent, downloaders) outside their own territorial boundaries. Minnesota is one of the first jurisdictions to attempt a general exercise of such jurisdiction. Minnesota’s Attorney General, Hubert Humphrey III, issued a memorandum stating that “Persons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws.”

Since Hubert Humphrey III’s memorandum was issued, a federal district court and the Minnesota Court of Appeals have applied his rationale and found personal jurisdiction based merely on the fact that information placed on the Internet was downloadable in the state in question. The opinion in Minnesota v. Granite Gate Resorts (a case argued for the state by the very same Hubert Humphrey III), accepted the Attorney General’s argument and asserted jurisdiction over the website owner based in part on the fact that “during a two-week period in February and March 1996, at least 248 Minnesota computers accessed and ‘received transmissions from’ appellant’s websites.” While this disturbing and poorly thought out result may eventually be overturned by federal legislation or case law defining due process, the federal case from Missouri, Maritz v. Cybergold, is more troubling. In

18. Id. (emphasis added).
21. Granite Gate, 658 N.W.2d at 718.
22. Minnesota’s long-arm statute permits courts to assert jurisdiction over defendants to the extent that federal constitutional requirements of due process allow. MINN. STAT. § 543.19 (1997).
Maritz, a federal district judge accepted the plaintiff’s “downloadable” argument most likely because of its conceptual simplicity, and additionally because of the traditional preference of courts and choice of law schemes to find jurisdiction in the domestic forum. Fortunately, no federal appellate court has made a binding determination, and no case involving in personam jurisdiction and the Internet has yet been decided by the Supreme Court. Therefore, these judicial missteps have not yet become formidable law.

Minnesota’s concerns are no doubt sincere, but the memorandum itself is not. Everybody “knows” that all information in cyberspace may be downloaded in Minnesota, and such an eventuality is always foreseeable. Minnesota’s rule thus makes all of cyberspace subject to Minnesota law. If every state took this approach (and following the initial success of Minnesota’s reasoning, there is no reason why every state could not), the result would be unbearable, especially for multinational corporations with attachable assets located all over the world. Nonetheless, Minnesota’s law lays out a simple syllogism that is easy for lawyers to grasp: anyone who “being without the state, intentionally causes a result within the state prohibited by the criminal laws of this state,” is subject to prosecution in Minnesota. Since anyone who puts up a webpage knows that it will be visible from Minnesota, “downloadable” in Minnesota’s Attorney General’s memorable words, then every Internet actor intentionally causes a result in the state of Minnesota and is subject to Minnesota’s criminal laws. This simple approach, conceivably appealing at first, dissolves upon a sufficiently detailed international legal analysis.

A much more sensible view is that of the Florida Attorney General: “the resolution of these matters must be addressed at the national, if not international, level.” An interesting question for strict constructionists is whether, under the federal system, Minnesota has any obligations under international law. As a practical matter, Minnesota, as well as all states and nations, will be constrained by international law. Where possible, the Supreme Court always interprets congressional mandates in accordance with international law, and that presumption is possibly stronger against state legislatures. Indeed, most provisions of U.S. foreign relations law are designed to keep international questions in federal hands. Of course, treaties are the “supreme law of the land,” superior to

any state law. At any rate, considerations of comity, which are underdeveloped and often thinly conceived in relations between the United States and foreign sovereigns, will be important if Minnesota attempts to assert this jurisdiction internationally.

Minnesota’s approach has several problems. First, Minnesota has ignored the presumption against extraterritorial in application of U.S. laws. It seems that the Minnesota Attorney General was under the impression that, because the mode of analysis for conflicts of law is the same for conflicts between U.S. states as for conflicts between a U.S. state and a foreign country, the results will also always be the same. The sovereignty of individual American states, however, is not as easily offended (or defended) as the sovereignty of nation-states. In other words, courts will accord France’s interest in its sovereignty greater weight than Delaware’s (this is especially true of French courts). Under the theory of international spaces outlined below, Minnesota has no jurisdiction to prescribe law over objects in cyberspace because under the federal system, Minnesota has no “nationality” to assert. Nationality is a function of national sovereignty, and the jurisdiction predicated thereon is federal.

Second, Minnesota has conflated in personam jurisdiction with the jurisdiction to prescribe law. The former is subject to the “minimum contacts” analysis, the latter is not. A nexus with Minnesota territory sufficient to establish in personam jurisdiction over a defendant may not be sufficient to give Minnesota the jurisdiction to prescribe a rule of law for the action. Indeed, Minnesota courts may have in personam jurisdiction over a defendant but may, according to their own choice of law statutes, choose to apply foreign law in the case at hand.

Although the analysis conducted in Granite Gate looks like a standard in personam jurisdiction decision, the court really decided the case while assuming it had the jurisdiction to prescribe law for actions in cyberspace. The court looked no further than its own state’s long-arm statute in finding in personam jurisdiction without considering issues of federalism, comity, or international law, i.e., without considering whether jurisdiction to prescribe existed or not. From an international law perspective, what Minnesota’s Court of Appeals and its Attorney General have actually done is chosen to rely on “effects” jurisdiction or

27. U.S. Const. art. VI, cl.2.
“objective territoriality” to find implicitly the jurisdiction to prescribe, where it is the territoriality of the object state, rather than (or in addition to) that of the subject actor, which prescribes the rule of law. The Restatement (Second) of Foreign Relations described objective territoriality as the following:

A state has jurisdiction to prescribe a rule of law attaching legal consequences to conduct that occurs outside its territory and causes and effect within its territory if either -

(a) the conduct and its effect are generally recognized as constituent elements of a crime or tort under the law of states that have reasonably developed legal systems, or

(b) (i) the conduct and its effect are constituent elements of activity to which the rule applies; (ii) the effect within the territory is substantial; (iii) it occurs as a direct and foreseeable result of the conduct outside the territory; and (iv) the rule is not inconsistent with the principles of justice generally recognized by states that have reasonably developed legal systems. 30

Minnesota’s rule misses the connotations of this description. None of these cyberspace “crimes” can meet part (a) of the test, because none of them is a traditional crime, generally recognized, and because the act of uploading is not currently a constituent element of any crime anywhere. Part (b) of the test is more important for analyzing jurisdiction to prescribe conduct in cyberspace. Part (b) speaks of substantial effect and principles of justice “generally recognized.” However, laws about pornography and gambling fail to meet either or both of these tests. Moreover, considerations of comity always play a major role in a basis of jurisdiction so offensive to foreign sovereignty. Objective territoriality is not a blanket to be thrown over cyberspace, but is appropriate only in unusual circumstances, where (as in the hypothetical example of the Canadian shooting an American) the state asserting jurisdiction on this principle is somehow the target state, uniquely or particularly affected by an action intended to cause such an effect. In short, under international law, Minnesota needs to find another basis for asserting prescriptive jurisdiction over actions in cyberspace.

30. Restatement (Second) of Foreign Relations § 18 (1965).

Another approach to jurisdiction in cyberspace is to treat the server where webpages are physically “located” (i.e. where they are recorded as electronic data) as the situs of a criminal action for the purposes of asserting territorial jurisdiction. Under this theory, a webpage “located” on a server at Stanford University is subject to California law. Where the uploader is also in the forum state, or is a national of the forum state residing abroad, this approach is consistent with the theory of jurisdiction in international spaces. But where the uploader is in a foreign jurisdiction, this analysis displays fatal shortcomings. To say that a webpage is “located” at the server means redefining downloading and uploading as a communication between two physical places, the location of the uploader and the “location” of the webpage. As a practical matter, we know that data sent from an uploader to even a nearby server can travel in data packets through nodes around the world, thus being sent and received through several jurisdictions on its journey to the downloader. This territorialization of cyberspace through its servers would create jurisdictional mayhem and may produce strange results if applied literally. For example, could an uploader be subject to the jurisdiction of a state where a randomly assigned routing node momentarily held a packet of contraband data?

One could envision a system in which we accept the theory of the uploader and the downloader and insist on exercising territorial jurisdiction over webpages “located” at a server. Under the theory of the uploader and the downloader, the act of uploading is performed entirely at the computer terminal of the uploader, within one and only one state. Naturally, if that state is the same state as the server, then asserting jurisdiction over a webpage based on a territorial theory of the server’s “location”, rather than on the location of the uploading, will produce no difference except in doctrine.

The ramifications of this doctrine will become apparent when the uploader and the server are in different states. When this is the case, in order to apply the law of the state where the server storing the webpage is located, one must assert that the act of uploading had an effect in the server’s state. This effect must be substantial enough to provide a basis for jurisdiction under the theory of objective territoriality or “effects”

31. With today’s technology, one can easily access an Internet account from any other server in the world, by use of “telnet” and “rlogin” commands over the UNIX platform. In the future, data exchange through the Internet will presumably be easier and more transparent. Indeed, it is not a far-fetched idea to have a universal server utilizing hard drive space around the world for storage, the way a single hard drive stores data all over its dozens of sectors.
jurisdiction. The theory of objective territoriality, however, can provide the basis for jurisdiction to prescribe acts in cyberspace only under unusual circumstances. As a general rule, it will not function for ascribing criminal liability to foreign uploading because all states have an equal interest in uploading since they are all equally affected by the universally accessible data. Objective territoriality requires a unique interest.

The natural response is to point to the computer files which create a webpage and say that it would be false to claim that the webpage was anywhere else but on the server. This narrow approach ignores the interactivity of cyberspace in four important ways. The first can be best stated in the following question: does a webpage really exist before it is accessed and constituted on the screen of the downloader? Surely a single gif file containing pornography cannot be “obscene” until compiled and displayed on the downloader’s machine in the community whose standards must be applied to define it as such. This has more than metaphysical implications. It is not difficult to figure out who put garbage into cyberspace, but it is very difficult to say what happens to it once it is there. If a webpage is located at Stanford, it is difficult to decide for jurisdictional purposes whether a Bolivian accessing it comes to Stanford or the webpage “travels” to Bolivia.

Second, constituent parts of a webpage are often called from other servers, with the source code for the page consisting mostly of images called up from other places. We do not know what the future will bring, but we can only suppose that “sites” consisting of data pulled from around the world at the downloader’s request will become more common. Thus, the “illegal” portion of a webpage may exist on a server in another country, where the materials are completely legitimate.

Third, a webpage consists in large part of links to other pages which may be “located” in other countries. Even if the data is not called up by the webpage itself, links to other data are presented to the downloader for him to “click” on. It becomes irrational to say that a webpage with links to gambling and pornography “located” in twenty different countries is subject to the law of any or all of those countries. A government could criminalize the creation of links to certain sites, but this would

32. The term “gif” file refers to pictures saved in the Compuserve format.
create jurisdictional bedlam. I would like to believe that this analysis of cyberspace would fail the Restatement test of reasonableness.

Fourth, as it is often overlooked, such interactivity is complicated by randomness and anonymity. William Byassee argues persuasively that territoriality should refer only to the “physical components of the cyberspace community”, who are the “sender and recipient.” The terms “sender” and “recipient” imply the intent of two (and only two) parties to communicate with each other. These are not the same people as the “uploader and downloader.” The uploader and the downloader do not necessarily know who or where the other is. The substantive results of this analysis would lead to a considerable amount of seemingly random criminal liability, without really adding anything to a state’s ability to control the content of cyberspace. Persons traveling around cyberspace need to know what set of laws applies to their actions. If we reject the territorialization of cyberspace and accept the theory of the uploader and the downloader, we must reject the broad form of the “law of the server.”

By contrast, the theory of international spaces developed below creates a clear rule. The state where a server is located retains jurisdiction over the acts performed in that state’s territory, i.e. the creation of the Internet account for the foreign persona non grata, and the tolerance of that account (and its potential offensive content) by whoever exercises control over the server (typically a sysop). The rule of nationality in cyberspace means that United States nationals and corporations cannot

---

33. Picture a computer screen full of links, each one subject to the laws of at least one other jurisdiction, and the webpage itself subject to the law of its server on top of all that. Among other things, one shudders to consider the First Amendment analysis of a law criminalizing the HTML command, `<a href = "www.university.edu/~homepage">`, or the random link.

34. Restatement (Second) of Foreign Relations § 403(1) (1965). “Even when one of the bases for jurisdiction . . . is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable.”

35. See William Byassee, Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community, 30 Wake Forest L. Rev. 197 (1995) (arguing that current legal structures are inapplicable to cases arising in Cyberspace, and calling for the creation of separate jurisdictions defined by “virtual communities” in order, for example, to define “community standards” for the purposes of pornography law).

36. Sysop means “system operator,” also often referred to as a system administrator, with no apparent thought to the inconsistency. System administrators often have very little control over the system, and indeed can often barely keep it running.

37. The ascribed nationality of corporations is a study in itself. The U.S. government is particularly willing to ascribe nationality liberally to its corporations acting abroad. For an example, see the case of Dresser France and the Soviet Pipeline. Clyde H. Farnsworth, Company Loses in Plea to Prevent Penalties on Soviet Pipeline Sale, N.Y. Times, Aug. 25, 1982, at A1.
circumvent domestic law by uploading from foreign jurisdictions, assuring the United States government a distinct slice of control over the cyberspace content contributed by its citizens.\(^{38}\)

The theory of international spaces thus converts the “law of the server” into the law of the sysop. It may be a law of vicarious liability, but it would be a law concerning only a sovereign and its territorial jurisdiction over a sysop, which presents no problems in international law. A sysop could be criminally liable for the content over which he has some measure of control, regardless of the nationality or location of the uploader, but an uploader would only be criminally liable if he was located within the territory of the forum state, or was a national of that forum state.

Fortunately for the future of sysops, this result has three main drawbacks. First, it may prove impossible to determine where the material was uploaded from, or the nationality of the uploader. Second, this would create a two-class system of servers in cyberspace, those “located” within the territory of the forum state, and those without, while all are equally accessible. Third, and perhaps worst for those in favor of free speech on the Internet (a principle soundly upheld in \textit{Reno}^{{39}}), making a sysop liable for any “crimes” committed on his or her system means putting the onus on the sysop to regulate content or suffer the consequences. This would spawn a regime of private, unregulated censorship, based on fear of litigation. It is difficult to imagine that such a system would be effective in promoting the state’s interests or the value of free speech that is fundamental to democracy. In addition, monitoring systems for content is virtually impossible given the sheer amount of data that can be put up overnight. A victim of a single incident of “spamming”\(^{40}\) will understand that a single person often cannot

\(^{38}\) A relic of cyberspace’s beginnings in the worldwide scientific community is that the primary language of cyberspace is English. The monolingual nature of cyberspace is changing as it becomes “inhabited” by ordinary people around the world. As this happens, the ability of a government to regulate its nationals, and thereby most of what appears in cyberspace in the national language, will surely seem much more valuable than territorial jurisdiction. The history of the printing press is illustrative. Ordinary publishing began as a trans-European Latin language venture in the 16th century. By the end of the 17th Century, international book commerce had given way to broad national vernacular markets. See \textit{Benedict Anderson}, \textit{Imagined Communities: Reflections on the Origin and Spread of Nationalism} 25 (1983).


\(^{40}\) “Spamming” is Internet jargon for sending multiple copies (hundreds or thousands) of a message to an email address in order to clog that person’s electronic mailbox and effectively paralyze that person. As this author is aware from personal experience, spamming is a very effective tactic. Note: spamming can also mean to send thousands of copies of a single piece of e-mail to thousands of recipients, either through e-mail or through newsgroups, as a form of bulk mailing (i.e. Internet junk mail).
read his or her own email in a single day, never mind the practicality of monitoring thousands of email accounts. Moreover, such a system seems ultimately so unjust for the poor overworked sysop; it is the equivalent of holding a homeowner liable for obscenity if, come morning, teenagers have spray-painted obscene language on the house during Devil’s Night. As a consequence, national governments are likely to make very little use of the “law of the sysop,” and instead concentrate on regulating downloaders and uploaders.

V. The Theory of International Spaces

A. Overview

The theory of international spaces begins with one proposition: nationality, not territoriality, is the basis for the jurisdiction to prescribe in outer space, Antarctica, and the high seas. This general proposition must be assembled through observations. In outer space, the nationality of the registry of the vessel, manned or unmanned, is the relevant category. In Antarctica, the nationality of the base governs. Other informal arrangements (for instance, the United States providing all air traffic control in Antarctica) weigh heavily in decisions about jurisdiction.

On the high seas, the nationality of the vessel—the “law of the flag”—is the primary rule. A competing view is emerging positing that jurisdiction at sea is really “floating island” jurisdiction, a subspecies of territorial jurisdiction. This theory posits that vessels at sea are really “floating islands,” and that the jurisdiction predicated upon them is territorial in nature. The Supreme Court has weighed in against this

41. There is a special provision in the Antarctic Treaty for exchanges of scientists and observers. These individuals are subject only to their own national law. Antarctic Treaty, Dec. 1, 1959, art. VIII § 1, 12 U.S.T. 794, 402 U.N.T.S. 71 [hereinafter Antarctic Treaty].


44. There actually was a floating island. Fletcher Ice Island (T-3) is 99% ice, 7 miles wide, 4 miles across, and 100 feet thick. No mere iceberg, it was sighted by an American in 1947, and has been occupied by the US since 1952. Fletcher Ice Island meanders around the Arctic Ocean. In 1961, for example, it was grounded on the Alaskan coastline near Point Barrow. In 1970, it was in the Baffin Sea, 305 miles from Greenland (Denmark) and 200 miles from Ellesmere Island (Canada). That year, Mario Jaime Escamilla was convicted of involuntary manslaughter in a U.S. Federal court for the shooting death of Bennie Lightsey while both were on Fletcher Ice Island. Bizarrely, the court of appeals reversed and remanded the case on procedural grounds, after first noting that it was “unable to decide” the jurisdictional issue. See United States v. Escamilla, 467 F.2d 341, 344 (4th Cir. 1972). That is to say that in the only recorded case of a floating island, the court was unable to endorse the “floating island” theory as a basis for jurisdiction.
interpretation, pointing out that stepping onto a U.S.-flagged vessel is not legally the same as entering the United States.\(^{45}\) The “floating island” theory appears to derive from the obsolete notion that vessels must somehow possess territoriosity because “the right of protection and jurisdiction . . . can be exercised only upon the territory.”\(^{46}\)

One approach is to treat these three areas as \textit{sui generis} treaty regimes. Some scholars see international law as no more than the sum of various international agreements—a purely positivist approach.\(^{47}\) This has the veneer of theoretical consistency, but only if we fail to recognize an evolving organic international legal system.

The \textit{sui generis} conception of international law is out of touch with the treatment of the respective international regimes in American courts. It is usual for American courts to treat these regimes as analogs to one another. \textit{Smith v. United States} is typical in this regard:

Antarctica is just one of three vast sovereignless places where the negligence of federal agents may cause death or physical injury. The negligence that is alleged in this case will surely have its parallels in outer space. . . . Moreover, our jurisprudence relating to negligence of federal agents on the sovereignless high seas points unerringly to the correct disposition in this case.”\(^{48}\)

In \textit{Hughes Aircraft},\(^{49}\) the U.S. Court of Federal Claims held that U.S. patent law did not apply to foreign spacecraft in outer space and relied on the decision in \textit{Smith v. United States} that barred the application of the Federal Tort Claims Act to claims arising in Antarctica.\(^{50}\) The governing treaties are also similar in their conception and design.\(^{51}\)

---


\(^{47}\) See, \textit{e.g.}, Benjamin R. Barber, \textit{Global Democracy or Global Law: Which comes first?}, 1 \textit{IND. J. GLOBAL LEGAL STUDIES} 119 (1993).

\(^{48}\) Smith v. United States 507 U.S. 197, 122 L.Ed. 2d 548, 556–57 (1993) (Stevens J., dissenting). Justice Stevens went on to claim that a theory of “personal sovereignty” held in Antarctica. “As was well settled at English common law before our Republic was founded, a nation’s personal sovereignty over its own citizens may support the exercise of civil jurisdiction in transitory actions arising in places not subject to any sovereign.” \textit{Id.} Stevens cited Mostyn v. Fabrigas, 98 Eng.Rep. 1021, 1032 (K. B. 1774). The reader will soon note that it is the physicality of these “sovereignless regions,” above any relevant legal characteristic, which makes the assertion of a similar regime for cyberspace somewhat intrepid. It is precisely this \textit{Pennoyer v. Neff} view of sovereignty, presence, and power which we must learn to move beyond.


\(^{50}\) Smith v. United States, 507 U.S. 197, 122 L.Ed. 2d. 548 (1993).

\(^{51}\) The Outer Space Treaty was based directly on the Antarctic Treaty. See section C, \textit{infra}. 
The next theoretical and conceptual hurdle is physicality. These three physical spaces are nothing at all like cyberspace which is a non-physical space. The physical/nonphysical distinction, however, is only one of so many distinctions which could be made between these spaces. After all, one could hardly posit three more dissimilar physicalities—the ocean, a continent, and the sky. What makes them analogous is not any physical similarity, but their international, sovereignless quality. These three, like cyberspace, are international spaces. As a fourth international space, cyberspace should be governed by default rules that resemble the rules governing the other three international spaces, even in the absence of a regime-specific organizing treaty, which the other three international spaces have.

B. Evolution of International Law

International law is neither a code nor an international common law. Its sources are many and varied, and they rely heavily on tradition and custom. The statute of the International Court of Justice is illustrative:

1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
   a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
   b. international custom, as evidence of a general practice accepted as law;
   c. the general principles of law recognized by civilized nations;
   d. [J]udicial decisions and the teachings of the most highly qualified publicists of the various nations, as a subsidiary means for the determination of rules of law.\(^{52}\)

Under this scheme, treaties are only one, albeit the primary, source of law. Customary international law is often the most important part of international law. International conventions generally codify customary law, rather than create brand new law. Central to the nature of securing the signatures of a hundred or more nations to broad multilateral treaties is the formulation of a broad consensus, and this consensus is

---

\(^{52}\) Statute of the International Court of Justice, June 26, 1945, art. 38, 59 Stat. 1055, 1060.
often expressed in customary international norms. This reliance on custom contrasts with both civil law systems, in which the code is paramount, and with common law systems, in which statutes and judicial decisions together form the core of the law. International law, then, is not a model of positive law. Elements of natural law, including notably *jus cogens*, are mixed into positive law and custom without a grand conceptual framework or meta-narrative.\(^{53}\)

Two concepts of particular importance in the disputes over international spaces demonstrate the point: *res nullius* and *res communis*. Under *res nullius* (literally, “a thing of no one”), a theory grounded in Roman law and Lockean concepts of natural law, any state can assert sovereignty if the traditional tests of the validity of a territorial claim are met.\(^{54}\) The debate over the sea bed in international waters, Antarctica, and the moon, revolved around just such a possibility of a nation asserting territorial jurisdiction. Other nations, especially former colonies who correctly identified *res nullius* with imperialism, asserted that these areas were *res communis* (a common thing). This argument won the day and is echoed in lofty provisions in treaties such as the Law of the Sea Convention,\(^ {55}\) and the Outer Space Treaty\(^ {56}\) calling these places “the common heritage of mankind.” *Res communis* owes its origin to Roman law, natural law theories, arguments of customary international law, and general principles of equal sovereignty embodied in the League of Nations and United Nations charters.\(^ {57}\)

Therefore, we see that international law is a system of mixed heritage, overlapping sources of authority, and disparate, varied, and even inconsistent modes of legal reasoning. This diversity of legal authority

---


54. Claiming “undiscovered” islands (with or without natives) requires a mix of history and presence. The Falkland Islands have been disputed by Britain and Spain (and Spain’s successor in interest, Argentina) on largely these grounds. One could summarize the theory as follows: anything not nailed down is mine, anything I can pry up is not nailed down.


57. The UN Charter Preamble states that among the purposes of the UN is “to reaffirm faith in fundamental human rights, in the dignity and worth of the human person in the equal rights of men and women and of nations large and small.” Charter of the United Nations, Preamble. Similarly, the League of Nations Covenant guaranteed equality of member states in Article 3: “At meetings of the Assembly each member of the league shall have one vote.” The Charter also states in Article 10: “The Members of the League undertake to respect and preserve as against eternal aggression the territorial integrity and existing political independence of all Members of the League.”
is what makes international law so wonderful: it flows from the full experience of human history and legal traditions, and despite theoretical inconsistencies that would give a libertarian a headache, it works. There is simply no single standard method for arguing within the framework of international law. All we have are the sources of international law outlined by the International Court of Justice, which amount to custom, tradition, and treaty.

Given the diffused, decentralized nature of international law, it is entirely appropriate to urge the recognition of a general principle of law derived from custom, treaty, and existing general principles of international law. No argument about what international law should be is inherently invalid. One simply tries to line up as much authority on one’s side, however disperse and contradictory. If the ultimate argument makes sense to supernational courts (including the International Court of Justice and the European Court of Justice) and to powerful or influential national governments, the proposed policy will become policy-in-fact, and perhaps thence custom and even treaty. It is on this basis that this article proceeds. How each state or court deals with arguments about international law is up to it, and the various treatments are, not surprisingly, always varied and inconsistent. Because of international law’s lack of consistent centralized sources, it is a sound methodology to recognize a general principle of law from various sources, including custom, treaty, and the current existing principles of international law.

C. The Case for International Spaces

1. History

The history of international spaces begins at sea. Modern admiralty law and the law of the High Seas began in large part with Grotius in the 17th Century. The Law of the Sea remains the dominating voice in the discussion of international spaces, and the oceans have long been the most important of the international spaces. Antarctica was not discovered until about 1820, and it did not become the subject of serious inquiry until then.

58. This famous work by Grotius is perhaps the seminal work in modern international law: HUGO GROTIIUS, DE IURE BELLII AC PACIS [On the Law of War and Peace] (1631).
59. The Roman mare nostrum “our sea” for the Mediterranean was the result of two centuries of no real conflicts of law, the Pax Romana. The idea of international law being a law between equal powers simply has no grounding in Roman history. Modern international law really begins with the Peace of Westphalia (1648) which endorsed a theory (a de facto result of the Thirty Years’ War) that the equal sovereign states are the building blocks of the political world. Today, the notion of sovereignty and ultimately nationality is so ingrained that we imagine that every individual has a nationality just as he or she has a gender. BENEDICT ANDERSON, IMAGINED COMMUNITIES: REFLECTIONS ON THE ORIGIN AND SPREAD OF NATIONALISM 14 (1983).
international attention until the 1950s, especially during the International Geophysical Year (1957-58). Although visible since time immemorial, outer space remained similarly unexplored until 1957, when Sputnik introduced man to a new international space. Cyberspace emerged during the 1970s and 1980s as the apparatus of the Internet took root, but it was not until the early 1990s that an explosion in users and uses, including commercial uses, introduced a worldwide virtual community to another international space.  

In each international space, the specter of international conflict has been a prime factor in forming treaty regimes. Concerns over the Antarctic “pie” during the Cold War led to a treaty regime that, in effect, froze the national claims to polar wedges. 61 These competing national claims will be discussed in greater detail below. Some scholars regard the 1982 Falklands War as a war over Antarctic resources. 62 Humanity’s entrance into outer space was also attended at its outset by international conflict, primarily surrounding the Cold War, though also encompassing the ambitions of tertiary powers such as France.

Similar pressures will soon come to bear in cyberspace. Computer viruses and the “munitions” status of cryptography 63 ensure that international confrontation will enter cyberspace even if human beings cannot. Cyberspace is as much a space for traditional public international law as for private international law.

2. Jurisdiction in Antarctica

The Antarctic Treaty does not itself prescribe a complete system of jurisdiction. Instead, questions relating to the exercise of jurisdiction in Antarctica were included in the illustrative list of matters which may be taken up by Antarctic Treaty Consultative Meetings. 64 So far, no measures dealing specifically with jurisdictional questions have been adopted. 65 However, the treaty does contain some minor jurisdictional provisions. It provides for open observation of all bases and the

---

60. Future generations may yet view the experience of “absolute” national sovereignty running from about 1650 through 2000 as a brief aberration in the political history of the earth. This kind of perspective is often lacking in discussions of the future of international law.


exchange of scientific personnel between these bases. The treaty also provides that such observers and scientific personnel be subject to jurisdiction based solely on their nationality, and not on either strict territorial jurisdiction or “floating island” jurisdiction (i.e. the notion that the nationality of the base would grant jurisdiction to that state over all persons thereon).

Subsequent treaties have addressed nationality more directly. The Convention for the Conservation of Antarctic Seals provides expressly that, “Each Contracting Party shall adopt for its nationals and for vessels under its flag such laws, regulations and other measures, including a permit system as appropriate, as may be necessary to implement this convention.” It does not endorse a territorial or universalist approach.

One reason for avoiding questions of territorial jurisdiction in Antarctica is that seven nations have made overlapping claims to various polar wedges of Antarctic territory (Argentina, Chile, the United Kingdom, France, Norway, Australia, and New Zealand). All of these claims are suspended while the treaty is operational. Several nations, including the United States and the Soviet Union, deny all claims, but during the Cold War, both superpowers made a point of maintaining bases in all seven claimed areas. The United States accomplished this the easy way, by maintaining a base directly on the South Pole.

It is essential that we recognize that Antarctica is not just governed by a set of treaties, but by a regime or system. This systemic nature is acknowledged in several of the treaties themselves. For example, the Convention on the Regulation of Antarctic Mineral Resource Activities describes the regime as follows: “This Convention is an integral part of the Antarctic Treaty system, comprising the Antarctic Treaty, the measures in effect under that Treaty, and its associated separate legal instruments. . . .” It is the established practice of the parties to the various treaties to consider them as part of a single whole.

---

66. See Antarctic Treaty, supra note 64, art. VIII.
67. Convention for the Conservation of Antarctic Seals, June 1, 1972, art. 8 § 1, 29 U.S.T. 441, 447, 11 I.L.M. 251, 256 (emphasis added).
68. The treaty was originally to run for thirty years, from 1961–1991. Antarctic Treaty, supra note 64, art. XII § 2(a). It chilled ambitions in the Antarctic with both superpowers agreeing to freezing the status of all claims. The success of the regime was demonstrated when it was renewed in 1991, after the end of the Cold War.
69. For an excellent visual representation of the Antarctic Treaty System, see <http://www.icair.iac.org.nz/treaty/map.html> maintained by the International Centre for Antarctic Information and Research, Christchurch, New Zealand.
71. Watts, supra note 65, at 292.
To date there are forty signatories to the Antarctic treaty, and all those nations involved in Antarctica are signatories. For this reason, it is somewhat academic whether the regime applies to non-treaty parties. Commentators argue, however, that the Antarctic Treaty system constitutes an “objective regime, such that it is valid for, and confers rights and imposes obligations upon third states.”\footnote{Id. at 295.} Although the treaty does not by its own terms apply \textit{erga omnes},\footnote{The Antarctic Treaty does not declare that it applies to non-signatory parties (\textit{erga omnes:} against everyone). A strict positivist view of international law might hold that the treaty therefore can never apply to non-signatories. The competing viewpoint, and the one that I favor as more consonant with general principles of international law, is that the Antarctic Treaty Regime is a complicated international system built on treaties between all of the world’s major powers that is developing, or ripening, into customary international law as time goes by. For this reason, if a non-signatory party violates the treaty principles, such as the ban on military use, or the Madrid protocol on environmental protection, it will meet the condemnation of a united international community. See Antarctic Treaty, supra note 64.} general acquiescence can establish a regime. In addition, the Vienna Convention on Treaties (which makes clear that a single treaty does not create obligations on third states without their consent)\footnote{Vienna Convention on the Law of Treaties, May 23, 1969, art. 34, 8 I.L.M. 699.} provides, “Nothing in Articles 34 to 37 precludes a rule set forth in a treaty from becoming binding upon a third state as a customary rule of international law, recognized as such.”\footnote{Id., art. 38.} It is reasonable to conclude that the Antarctic Treaty Regime has, like the law of the sea, ripened into full international customary law.

There are several American cases dealing with Antarctica that illustrate the texture of international law in action. \textit{Beattie v. United States},\footnote{Beattie v. United States, 765 F.2d 91 (D.C. Cir. 1984).} is a fascinating case about international law, comity, and international spaces. The facts are tragic: an Air New Zealand jet crashed into Mount Erebus, Antarctica, on December 28, 1979, killing all 257 passengers and the crew. Families of the passengers sued the United States government, claiming negligence by the U.S. air traffic controllers at McMurdo Station, Antarctica. The question before the court was whether, under the Federal Tort Claims Act (FTCA), Antarctica fell under the “foreign country” exception to the waiver of sovereign immunity under the FTCA. The court held that, for these narrow purposes, Antarctica was not a foreign country, and allowed the lawsuit to proceed.\footnote{Beattie was overruled in its direct holding that Antarctica was not a foreign country under the FTCA. Smith v. United States, 507 U.S. 197 (1993). Judge Scalia’s dissenting opinion in Beattie became Justice Rhenquist’s majority opinion in Smith. See Smith, 507 U.S. at 199–200. However, the reversal is only the tip of the iceberg. The Court’s “plain meaning” reading of the FTCA in both instances ignores the role of comity. The real difference between Beattie and Smith is that the Beattie case was very important to New Zealand, and adopting Scalia’s opinion would have left a grievous injury to that foreign power’s na-}
In allowing the suit, the American court must have noticed that this accident “in terms of loss of human life and family bereavement was the worst disaster to strike New Zealand since the end of the 1939-45 war.”

*Environmental Defense Fund v. Massey* contains an exposition on the domestic presumption against extraterritorial application of U.S. law. Again, the case deals with the McMurdo base, which is an American base near the Ross Ice Shelf. As is typical, the court notes that “Antarctica is generally considered to be a ‘global common’ and frequently analogized to outer space.” In declining to apply the presumption, the court holds that “[w]here there is no potential for conflict between our laws and those of other nations, the purpose behind the presumption [against extraterritoriality] is eviscerated, and the presumption against extraterritoriality applies with significantly less force.” The court seems to suggest that it would also likely endorse the corollary that where, as in cyberspace, the potential for conflicts of law is tremendous, the presumption against extraterritoriality is very forceful. Taken together, these cases show that domestic law has absorbed the notion of an international regime in Antarctica and analogized it to outer space.

3. Jurisdiction in Outer Space

The fundamental document in outer space law is the Treaty on Principles Governing the Activities of States in the Exploration and Use of
Outer Space. The treaty was adopted pursuant to a United Nations General Resolution which contains verbatim much of the text of the treaty. The resolution and the treaty explicitly state that States have jurisdiction over objects bearing their registry. Remarkably, this resolution of the General Assembly was unanimous.

There is also no doubt that the Outer Space Treaty was based on the Antarctic Treaty. Hearings held before the Senate Committee on Foreign Relations in 1967 actually include a copy of the Antarctic Treaty. In the hearings, the committee noted that the Outer Space Treaty was specifically based on the Antarctic Treaty.

The treaty states that outer space, including the moon, is not subject to claims of sovereignty. Therefore, no territorial jurisdiction is possible. Article III provides that all activities shall be in accordance with international law. This article assures us that international law is not merely a terrestrial phenomenon, but includes all non-sovereign spaces, whether on this earth or beyond it. The treaty skirts many jurisdictional problems through Article VI, which declares that all activities are to be authorized by a State. States are to assure “national activities” are carried out in conformity with the treaty. Article VII makes a state responsible for damage caused by objects that it launches or causes to be launched, thus embracing the state of registry and the state of the launcher. Jurisdiction as set forth in Article VIII is then an easy matter: the national registry of an object gives the state of registry jurisdiction over that object and over any personnel thereof. This national status functions like the “temporary presence” doctrine announced in The Schooner Exchange and Brown v. Duchesne. When the objects return to earth, their special national status for jurisdictional purposes is not affected. Thus, jurisdiction in outer space, as in Antarctica, is predicated on the nationality principle.

---

83. Id. at 2411.
84. Aside from being extremely rare, this unanimous resolution represents a new multinational approach to new worlds. It is a significant improvement over the Treaty of Tordesillas 1494, in which the Pope divided the whole unclaimed world between the Spanish and the Portuguese.
85. Hearings before Senate Committee on Foreign Relations 90th Cong. 80 (1967).
86. Id.
87. Outer Space Treaty, art. II.
88. Id., art. III.
91. Hughes Aircraft v. United States, 29 Fed. Cl. 197 (1993). In this case, an invention under U.S. patent was on board a foreign spacecraft in the United States preparing for
4. Jurisdiction in Cyberspace: The Vessel of Nationality

Making nationality work as a principle in cyberspace requires an analysis appropriate to cyberspace. It is too easy to fall into the trap of analogy by asking how nationality would play out on the open sea, in outer space, or in Antarctica, and then trying to make direct applications to cyberspace. As we have seen, the nationality principle is firmly entrenched in these areas, but its implications are different for each.

For example, if we are applying the “law of the flag” from maritime law, we can get bogged down in the analysis of how the nationality of a ship is determined. There is, of course, an international regime in place which determines the registry of a ship, and there are such things as “flags of convenience,” under which U.S. nationals may fly a Panamanian flag and then be subject to Panamanian law at sea. The obvious question might be, “What is the nationality of a vessel in cyberspace?” But we are at a loss to find a ship or plane in cyberspace. Thus, we must ask first, what is the vessel of nationality in cyberspace, i.e. what carries nationality into cyberspace?

Registry will not suffice as it does not currently exist. International treaties may at a later date specify that all files and messages be “registered” with a nationality. Until such time, however, we must discover the default rules. Before there was registry at sea, there was still nationality. Justice Stevens recently referred to the principle as the personal sovereignty of the nation over its citizens. In cyberspace, persons bring nationality into the international space of cyberspace through their actions. An uploader marks a file or a webpage with his nationality. We may not know “where” a webpage is, but we know who is responsible for it. The nationality of items in cyberspace could be determined by the nationality of the person or entity who put them there, or perhaps by the one who controls them.

This analysis is relatively easy to undertake with regard to webpages. Generally, determining the nationality of a webpage is not a problem. The creator of a webpage is usually listed on the webpage, and is typically an individual or an organization. However, webpages are now also created by individuals and companies for others. This makes us ask who “owns” the page for jurisdictional purposes—the creator or the person on whose behalf it is maintained? International law is not launch. It was held not to be subject to U.S. law because of the “temporary presence” doctrine. The court made analogies to Antarctica as well.


93. The webpage is my paradigm because the world wide web surely prefigures the future of cyberspace: a place where complex, sophisticated “sites” are maintained by individuals and organizations, rather than only commercial and governmental interests.
displeased with either answer. If a nation wishes, it can ascribe nationality to all webpages maintained “on behalf of” its citizens, as well as any webpages actually created (i.e. uploaded) by its citizens. Either solution essentially solves the conflict of laws problem by reducing the conflict to two states at the most. Courts will have to make their own judgments about what level of connection between a cyberspace item and an individual is reasonable for the nationality of that person to dictate the jurisdiction to prescribe law. The theory of international spaces turns cyberspace from a place of infinitely competing jurisdictions into a place where normal jurisdictional analysis can continue.

Similarly, links to pages in cyberspace will follow the same jurisdictional analysis. The person who creates the link is subject to his or her own national laws governing what links he or she may create. Also, a person is subject to the territorial jurisdiction from which he or she uploads data (data that may include a link), and that jurisdiction’s law may be used to dictate which links are permissible and which are not. A person who follows a link is simply a downloader, and is subject to the territorial jurisdiction of the keyboard at which he or she sits, as well as the laws governing persons of his or her nationality in cyberspace.

What the theory of international spaces avoids is the downloader having to be aware of following links that were illegal for the uploader to make based on the uploader’s territorial presence or nationality. There is no basis under this theory for the uploader’s state to prescribe laws governing the foreign downloader’s actions.

The following scenario is an example of how the proposed system might work: a webpage, commissioned by a U.S. citizen, is uploaded from Moldova by a Moldovan citizen. If the webpage contains advertising considered fraudulent under U.S. law, that U.S. citizen could be subject to prosecution by U.S. authorities. Additionally, the Moldovan could be subject to the laws of Moldova that regulate uploading. Moreover, a U.S. citizen in Moldova is not immune from U.S. law simply because he uploads from Moldova (into cyberspace) rather than from the United States. What the United States cannot do is prescribe a
law for a webpage created and uploaded by a Moldovan who lacks any reasonable connection to an American national (i.e. a connection cognizable at international law as a basis for the jurisdiction to prescribe), merely because the webpage is “downloadable” in the United States.

Some of the other complexities of cyberspace deserve a little attention here. One of these complexities is a “mirror” site—a website set up to contain identical information to another site in order to alleviate overburdening of the servers or allow faster downloading to websurfers in different geographic locations. Mirror sites are intentionally placed at internet addresses that are in different parts of the network, often on servers in different countries. While the location of the server should be of no importance, it often means that a mirror site involves an international alliance. For example, suppose a software company in Japan maintains a mirror site for a German software company, and allows the German company access to its ftp (file transfer protocol) site. In this situation, the content is controlled by the German company, but the Japanese company is involved in the production of the page. The question then becomes a highly factual inquiry, requiring the court to determine the extent to which the person maintaining the foreign mirror site is involved in the uploading and downloading of material. Two general results are possible. First, if the Japanese national takes an active role in creating and maintaining the site, then the Japanese government will have jurisdiction to prescribe law governing material on that site. If, however, the Japanese national takes an entirely passive role, simply providing available space for the German national to store data, then the extent to which Japan has the jurisdiction to prescribe law regulating the content of that site is directly related to the “law of the sysop” analysis discussed above.

However, a site maintainer is also different from the sysop. Unlike the hapless sysop, a site maintainer may often (a) play a role in determining the content of the site, (b) easily be able to control that content, and (c) have a specific intent to control the content of the site. When this is true, a nexus exists between the actions of the foreign national (the Japanese national in the above example) and the contents of the “mirror” site, a nexus that does not exist between an ordinary downloader and a website maintained by an unrelated individual in another jurisdiction. Under these circumstances, it may then be altogether “reasonable” for the foreign state to assert jurisdiction over the site. This, too, will be a highly subjective and factual inquiry for a court in
addressing each mirror site, and local law alone will determine the amount of control over a mirror site that is sufficient to make the person wielding that control liable for the site’s content. Nonetheless, it is my sincere hope that the principle of nationality will be established firmly enough that states will not attempt to regulate this corner of cyberspace based on subjective territoriality.

Of course, cyberspace is more than the world wide web. There are bulletin boards, USENET groups, and electronic mail (email), portions of cyberspace that contain messages sent by individuals. These individual message senders may be anonymous, but since anonymity is as much a practical problem for any municipal law as for international law, the problems presented by the anonymity issue are not addressed in this article. Once a person is identified, his nationality will provide the basis for the jurisdiction to prescribe rules for his actions in cyberspace. For example, the United States government may make it illegal to post to alt.sex.bestiality (a USENET group), but this cannot provide the basis for holding a Korean citizen in Korea (without connection to a United States national) criminally liable for posting to alt.sex.bestiality.

A problem also arises when the line between cyberspace and normal telecommunications is blurred. Despite its transnational routes, email is probably not properly considered to be in the international space of cyberspace. Cyberspace is a virtual community, and international law applies because it is readable by the world. When private email is sent from one individual to another across jurisdictional lines, the jurisdictional analysis is different. An email from an Arizonan to an Italian is always subject to Arizona law, but could also be subject to Italian law—just as a telephone call would be. In the case of private email communication, the Arizonan “purposely availed himself” (to use the resounding formulation of World-Wide Volkswagen v. Woodson98) to the benefits of the Italian jurisdiction. This private, one-time email does not share the essential characteristics of an item in international cyberspace; rather, it is a mere international communication.

Naturally, we need a clearer definition of when we enter cyberspace. Is a message sent “cc:otherfolks” to several jurisdictions subject to the laws of all of those jurisdictions? Can a message intended to defame a Mexican citizen, as in the 1887 Cutting Case,99 and actually emailed to that citizen, be saved from liability by also being sent to a hundred other individuals? When is an electronic communication international enough to be cyberspace? Ultimately, this conundrum will resolve itself through a focus on the intent of the sender to cause an

99. See Letter, supra note 17.
effect in a given country. The relevant question under international law is whether it is reasonable for the state in question to exercise jurisdiction based on **objective** territoriality. Given the properties of cyberspace discussed in this article, the burden will clearly be on the prosecuting state to prove that an item in cyberspace was targeted to that state, giving that state a special interest above others. We cannot forget the importance of the test of reasonableness of the jurisdiction to prescribe, a question that will be litigated in the courts of the prosecuting state. Because of the nature of cyberspace, and the great potential for conflicts of law, a fairly strong connection between the emailer and the target state will be necessary for the target state to assert the jurisdiction to prescribe based on the principle of objective territoriality.

VI. Jurisdiction in Cyberspace: A Preview

In this final section, this article shall discuss how the theory of international spaces would apply to two burgeoning topics in cyberspace law: copyright and libel.

A. Copyright Law

As the world wide web fills with easily replicable written, visual, and aural information, it will be the source of considerable copyright litigation. Two American cases which have dealt with Internet copyright issues, *Religious Technology Center v. Netcom*,\(^\text{100}\) and *Playboy Enterprises v. Frena*,\(^\text{101}\) avoided international jurisdictional problems. Both were cases brought by American nationals against American nationals, all of whom were also clearly subject to American territorial jurisdiction. As the adage goes, there can be no conflict of laws unless there is an actual conflict.

Of course, we can propose a hypothetical situation in which one of the parties is not subject to U.S. territorial and national jurisdiction. Suppose that in the *Netcom* case, Scientology’s religious books were copyrighted in the United States, but were not copyrighted in Latvia. In this instance, a Latvian uploads a web site containing a link to a file that contains the religious work. All the downloader needs to do is click on the appropriate icon, and the copyrighted work will appear on his computer.


At its greatest extent under international law, American copyright law could reach a webpage created by an American and uploaded in Latvia. It could also reach a webpage created for an American, by a Latvian national, and uploaded in Latvia. However, as a matter of international law, the United States would not have jurisdiction to prescribe copyright law for a webpage uploaded by a Latvian national in Latvia whose only connection with the United States was a wish that Americans should download this material. In this situation, there would be no American nationality on which to predicate such jurisdiction, nor would there be territorial jurisdiction. Objective territoriality, or “effects” jurisdiction, is per se unreasonable without more. An American court should throw out this suit for want of jurisdiction or apply Latvian law based on the Latvian nationality of the uploader and controller, and likewise dismiss the suit.

A more complicated problem arises in the context of contributory infringement, where the crime is predicated upon the defendant’s inducing infringement. As with many jurisdictional questions in cyberspace that are apt to arise, it is important to remember that exercise of jurisdiction on the basis of objective territoriality is merely disfavored, not forbidden, and the time to exercise that jurisdiction might arise when a particular state has a special interest in asserting jurisdiction. The theory of international spaces posits that uploading copyrighted information in cyberspace, without more, would not be sufficient for a state to prosecute the uploader for contributory infringement on the basis of objective territoriality. To exercise jurisdiction to prescribe on the basis of objective territoriality, a state would have to demonstrate a special interest, requiring a fact-specific inquiry. It is my hope that U.S. courts will refrain from exercising jurisdiction except where a peculiar and special interest is involved.

102. Exactly when and how a “wish” materializes into something strong enough for the exercise of jurisdiction, on either the protective principle or the principle of objective territoriality, is discussed below.

103. How much more? Probably quite a bit, given how hostile Latvian courts would be to such a proposition. Comity would play a huge role here. American law may appear to authorize jurisdiction on the basis of a long-arm statute such as Minnesota’s, and it is up to the courts to recognize that the exercise of jurisdiction would violate principles of international law, and refrain from doing so.

104. The reader should note that in personam jurisdiction may exist by service of process under the Hague Convention, and that is not the jurisdictional question at issue here.

105. U.S. courts are probably key to accepting this theory of cyberspace because the U.S. has a history of showing little respect, or understanding, of principles of international law. For an example, see Nicaragua v. United States of America, I.C.J. Rep. 392 (1984), where the United States claimed the right to voluntarily remove itself from the jurisdiction of the World Court, to avoid an unfavorable outcome, and then ignored the court’s exercise of jurisdiction and adverse judgment. Or see the U.S. invasion of Panama, and the resulting
the hypothetical example above, this would mean that unless the Latvian directed the webpage explicitly at United States citizens, the United States would not bring in absentia charges against the Latvian national, or alternatively that those charges would be rejected by a court as violative of international law through the application of the presumption against extraterritoriality. However, to date, such issues have not arisen, and the only cases in the United States involving in personam jurisdiction over the Internet have not involved international issues where international law might be tested, although those cases do show a disturbing lack of interest in any international ramifications of their decisions.

B. Libel

Unlike the criminal copyright violations cited above, libel in the United States is purely a civil matter. In this instance, we see a somewhat different result. In any civil case, especially as regards libel, we can assume that plaintiff and defendant have a closer relationship than merely uploader and downloader. Libel requires some measure of intent, usually malice.

A recent case in the Supreme Court of Western Australia allowed a U.S. national to sue an Australian defendant over a bulletin board (BBS) posting which the U.S. national claimed was defamatory. The result did not offend the sovereignty of any state except Australia, and thus while the result was perhaps unjust, it was unlikely to encounter international sanction. The Australian court probably had little theoretical difficulty reaching its result. Under traditional conflict of law rules, if the publication were in a newspaper in Australia, the analysis would be fairly straightforward: if the place of the tort (lex loci delicti) was Australia, then Australia would have the jurisdiction to prescribe a rule for that action under the principle of subjective territoriality.


107 Strict liability offenses are precisely the reason why cyberspace must be considered a fourth international space.


109 The “governmental interest” test used by many states, including California, uses a different methodology more in tune with balancing the interests of sovereign states, i.e.,
By contrast, under the theory of international spaces, cyber-libel would be defined as the uploading of tortious material and its subsequent publication in cyberspace. For Australian law to apply under the principle of subjective territoriality, the place of the uploading would have to be Australia.

Had the Australian court applied this analysis, it would have discovered that in this case the *lex loci delicti* of the tort of libel is difficult to find. The act (uploading) occurred in the uploader’s physical location (the United States), subject to the territorial jurisdiction of that United States, but the libel was published in cyberspace. Since publication is a necessary element of defamation, libel must in this instance be viewed as having been consummated in cyberspace. Under the nationality principle, Australia has the jurisdiction to prescribe law for libels committed by Australian nationals in cyberspace. An Australian cannot escape the long arm of Australian libel law simply by uploading from a different jurisdiction. Since the uploading did not occur in Australia and the libeler was not an Australian national, the Australian court could have declined jurisdiction on the grounds that none was for this act committed by a foreign national in cyberspace.

Once again, objective territoriality rears its ugly head. We simply must assume, as with the Cutting Case,\(^\text{110}\) that libel does not allow invocation of this “effects” jurisdiction where the publication is not in the forum state trying to exercise jurisdiction. The closer Australia can get to defining the publication as occurring in Australia, rather than in cyberspace, the more likely it can be to exercise jurisdiction to prescribe law on the basis of objective territoriality. Again, in this situation, no one will pressure Australia (save the defendant) to do otherwise because no foreign state is offended when Australia allows its own national to be liable to suit by a foreign national.

If it were the American who had libeled the Australian, the situation would be quite different. The Australian could sue the American in U.S. courts for uploading the libel, if uploading libel were actionable under U.S. law. In this instance, jurisdiction to prescribe is based simply on subjective territoriality. Naturally, the Australian would most likely prefer to sue in an Australian court. Here, we discover that Australia has no jurisdiction to prescribe law based on either subjective territoriality or nationality, and the presence of the libel in cyberspace makes objective territoriality an impossibility. The suit could still proceed if Australian courts apply conflict of law principles and apply

more in tune with international law and comity. For that reason, the traditional and more troublesome *lex loci* test is discussed here.

U.S. law to the American’s action in cyberspace. If U.S. law does not so provide, an Australian may have no remedy at all for libel committed by an American national in cyberspace.

The lack of reciprocity would be troublesome. Comity might urge towards the exercise of jurisdiction on grounds similar to that in Beattie if the case were sufficiently important and the case from the Supreme Court of Western Australia were clearly stated state policy. More likely, however, this is a perfect situation for the United States to endorse the theory of international spaces and thus guarantee that its citizens will not be hauled into court for libel suits brought in nations with freedom of speech laws that are more restrictive than those guaranteed by the First Amendment. As always with international law, the law gains strength from court decisions in which international law favors the sovereign who might be offended by its breach, and is tested when sovereigns must exercise restraint and accept an adverse outcome. In order for this system to be worked out rationally by international law rather than by some jurisdictional equivalent of the law of the jungle (the stronger state wins), we can only hope that states offended by excessive exercise of jurisdiction by (in all likelihood) the United States resist on the grounds of international law, prompting the United States to adopt a similar, reciprocal stance towards suits brought against American nationals on those grounds. The case in Western Australia provides little in the way of hope, but the European Union might well engage the United States over international law, as it is doing with the Helms-Burton law.

VII. Conclusion

The survey of international law and the treatment of the jurisdiction to prescribe in vast sovereignless regions provided in this article supports the theory of international spaces. Antarctica, outer space, the high seas, and cyberspace are four international spaces that share the unusual characteristic, for jurisdictional purposes, of the lack of any territorial jurisdiction. In these four places, nationality is, and should

111. Libel law is generally state law. The difficulty in figuring out the provisions of such a suit under each of the fifty-one jurisdictions in the United States is an example of the jurisdictional circus involved if no principle of international law can limit the exercise of jurisdiction to prescribe law based on objective territoriality by more than a hundred and fifty sovereign nations.


be, the primary principle for the establishment of jurisdiction. Such a rule will provide predictability and international uniformity. It strikes a balance between anarchy and universal liability, and it works. Recognition of cyberspace as an international space is more than overdue. It is becoming imperative.

I will conclude with a final hypothetical situation, which may serve as a warning to national courts not yet aware of the international character of cyberspace. A Danish citizen posts lurid photographs on his personal web page that is “located” on a server in Denmark. However, the government in Copenhagen has not taken any action to forbid the uploading of such material. Indeed, Danish courts or the European Court of Justice may already have deemed such a law unconstitutional or violative of basic human rights. The unsuspecting Dane meanwhile goes to visit a cousin in the United States over Thanksgiving weekend. Learning of his arrival, the FBI telephones local law enforcement. Local law enforcement, intent on enforcing state obscenity laws, perhaps based on some local cause celebre regarding this website and some teenagers, immediately contacts a magistrate, giving her the URL, and requests a warrant for his arrest. The magistrate soon downloads the offensive material, finds that it is clearly obscene under Miller v. California in the community where the magistrate sits, and after reading Maritz v. Cybergold, and the local long-arm statute, issues the warrant without a further thought to jurisdiction to prescribe. Local law enforcement makes the arrest Wednesday night.

On Monday morning, the court-appointed lawyer for the somewhat melancholy Dane files a petition seeking a writ of habeas corpus. “My client is Danish national,” argues the lawyer, “and furthermore he uploaded the obscene material while in Denmark.” Neither the United States nor any of them has jurisdiction to prescribe a law for this action under either the nationality principle or the territoriality principle. Exercise of jurisdiction would violate international law. The state’s obscenity law and jurisdictional statutes should be construed to conform

---

114. URL stands for Uniform Resource Locator. This is a set of words (usually preceded by http://) that serve as a designation for the numerical Internet address (such as 123.123.123.22).
to international law, in the absence of Congressional permission for states to violate international law. 117

The case requires immediate attention; the judge must decide whether to continue to hold the man who has been in jail for three days already. No doubt an international incident is already brewing. 118 This article provides the Dane’s lawyer with an argument, and the judge with an answer.

117. The Supreme Court appears willing to allow violations of international law where Congress appears to have authorized violations of international law. See, e.g., United States v. Alvarez-Machain, 504 U.S. 655 (1992) (exercising jurisdiction over a Mexican national forcibly abducted and brought to the United States for trial—in violation of customary international law—because the extradition treaty with Mexico did not explicitly forbid kidnapping of Mexican nationals).

118. The Massachusetts murder trial of Louise Woodward in October, 1997, is an example of international furor; imagine the outrage if the crime with which she was charged was not even a crime in the United Kingdom. See Commonwealth v. Woodward, 1997 WL 694119 (Mass. Super. Nov 10, 1997).