Introduction

"Liberty finds no refuge in a jurisprudence of doubt"
(Southeastern Pennsylvania v. Casey 112 S.Ct. 2791, 2803 (1992))

This article analyzes whether the technical characteristics of the Internet should create a separate legal jurisdiction, and if a separate jurisdiction would be beneficial to the Internet. Jurisdiction is a legal term for the limitation on the ability of a court to determine disputes. Generally, a nation state's jurisdiction only extends to individuals who reside within the country or to the transactions and events which occur within the natural borders of the nation.

The question is whether the global nature of the Internet naturally forms a separate legal arena. If a "natural" jurisdiction exists, then should special laws be enacted to govern the Internet? Should a Convention of Cyberspace be drafted similar to the separate international conventions governing the Law of the Sea and Admiralty Law? In essence, the question to be resolved is whether the Internet needs a separate set of laws or if current laws are adequate. We seek to answer these questions by exploring the nature of the Internet as a community and self-regulating body. A critical focus of the inquiry reflects on the technological nature of the Internet and the scientific traditions and philosophies that govern such technology.
The article begins with a discussion of the problems of applying law to the Internet. This analysis will focus on two issues: The problems of applying jurisdiction to online disputes, and the controversy inherent in applying law as a means of controlling technology. After reviewing the problem, we will focus on whether the Internet is a community that can control the behavior of its members. This requires a discussion of the nature of community and how communities traditionally creates law. Finally, the paper will conclude with an evaluation of the existence of a separate jurisdiction and the need for the creation of new laws.

**Jurisdiction in the United States**

In order to maintain a lawsuit in a given state or country, the court must have jurisdiction over the person or the subject matter of the suit. The United States Constitution permits the courts to exercise personal jurisdiction over persons who have sufficient minimum contacts with the state or judicial district attempting to assert jurisdiction (see [1]). These "minimum contacts" consist of physical presence, financial gain, stream of commerce, and election of the appropriate court via contract (International Shoe Co. v. Washington, 1945). The courts have also held that speech purposely directed at the forum may create sufficient contacts for jurisdiction (Calder v. Jones, 1984).

This means that even non-residents who are not physically present in the U.S. can be sued in a U.S. court as long as the person or entity has minimum contacts with the nation. In an era of computer-mediated communication, simple actions online may satisfy the minimum contacts analysis. Such global jurisdiction can apply to U.S. citizens as well: U.S. citizens may be brought in to court in other countries with a similar minimum contact requirement for online activities (Perritt, 1996).

Growth in transborder technology and commerce has forced U.S. courts to create complex ad-hoc legal theories to maintain jurisdiction over non-residents (Burk, May 18, 1995). The court in Hansen v. Denckla asserted that such technological progress made the defense of a suit in a foreign tribunal less burdensome (Hansen v. Denckla, 1958).

This may be contrasted with the decision in the recent U.S. case of Creative Technology, Ltd. v. Aztech System PTE, Ltd. (1995). Both Creative and Aztech are Singapore corporations with U.S. subsidiaries. All design and manufacturing is performed in Singapore. Creative sued Aztech for copyright infringement in a U.S. court. Aztech countered with a lawsuit in Singapore and filed a motion to dismiss the U.S. lawsuit. The trial court granted Aztech's motion to dismiss based on the legal doctrine of forum non conveniens: that hearing the law suit in the court where the action was filed is inconvenient to the non-resident parties and there is an alternative court available.

To prevail on the motion, Aztech was required to prove that there was an adequate alternative location to hear the suit and that a balance of private and public factors required the court to dismiss the case (Creative Technology, Ltd. v. Aztech System PTE, Ltd., 1995). The Appellate court affirmed the trial court's ruling due to the lack of convenience to the parties (as all witnesses were in Singapore) and despite the fact that Singapore law was less favorable to Creative.

Despite modern technology, the court considered the maintenance of a suit in the U.S. to be burdensome to the parties. U.S. law allows law suits to be maintained over foreign persons based on their contact with the forum. Applying the court's analysis to computer-mediated communication leads to confusion as to what nation would be the
appropriate site for a lawsuit. For example, if a company in Norway put up a Web page on a server in Singapore with Disney’s copyrighted images and the images were downloaded, cached and browsed in the U.S. and other countries, what law would apply? Would the downloading, caching and browsing be sufficient contact to bring a lawsuit against the Norwegian company in the United States? Such contacts may not be sufficient if, as in Creative, the maintenance of the suit is considered burdensome and an adequate alternative court exists outside the U.S. On a global network, a principal such as minimum contacts does not answer the question of which jurisdiction will apply in a dispute.

The Challenge of Applying Law to technology

The Internet is an inherently technological environment. New technology inevitably creates new situations which existing law cannot control. At times, law can create a roadblock to progress by its lack of ability to adapt to new situations.

An interesting example is the phenomena of caching on the World Wide Web. Caching allows greater efficiency in the transmission of information on the networks by maintaining redundant copies close to those who access the information. For example, if a user in Germany browses a Web page in California, a computer somewhere in Europe may keep a copy of the page for the benefit of others that access the same information. Such caching not only has advantages in that individuals get quicker access to information, but also improves the ability of the network as a whole to handle more usage.

There are some who would maintain that, absent any fair use discussion, this form of "copying" is a copyright infringement (Samuelson, 1996). Legally, this may be correct, but caching is not governed by the discussions of copyright lawyers or law professors. If this type of restriction were enforced, it would place severe limitations on the usability of the technology. Any application of law to the network must be analyzed in terms of the impact to the technology and the progress of the Internet.

Some U.S. laws are impossible to apply to the Internet without creating substantial limitations on the technology. Current precedents gloss over the remarkable differences between the normal legal environment and the technological network. The need to address these separate technological issues is analyzed by Niva Elkin-Koren (1995). Elkin-Koren reviews the court's approach in recent BBS cases. Her discussion shows that the courts do not exercise the depth of investigation required in applying copyright law to digital technology. She applies her analysis to a number of cases including the Playboy v. Frena (1993) case in which a BBS operator was found liable for copyright infringement because his users had uploaded copyrighted Playboy images.

Elkin-Koren (1995) notes that the courts have found infringement without addressing preliminary issues such as "whether unauthorized copies were created" and "what constitutes a 'copy'". The court found that the BBS in the Playboy v. Frena (1993) case distributed a product while a BBS supplies services such as "access to electronic space for the exchange of information". The court appeared to have a basic misunderstanding of the nature of the BBS.

This failure to understand the digital environment is typical of current case law and the recently proposed NII legislation on copyright. Indeed, the analysis of the courts in the BBS cases reveal an attempt to manipulate the facts to fit the current parameters of copyright (Elkin-Koren, 1995). As Elkin-Koren points out, the existing framework may create legal outcomes that are not necessarily socially desirable (p. 356).
undesirable outcomes may include keeping the power of information in the hands of the few as opposed to disseminating new information and ideas to the many without media censorship or control.

Online communication promotes interaction and social discourse among users where access to previous technologies of communication has been controlled by an empowered elite. Whoever controls the communications system within a country has effective control of the government (Eco, 1986). This is one of primary reasons that communications systems historically have been centrally maintained by governments, except in the U.S., where a government regulated oligopoly was maintained instead.

The technological environment offered by computer-mediated communication promotes decentralization whereas the court procedures tend to promote centralization. While centralization was necessary in the environment of the printing press and publishers, the Networld facilitates individuals to self-publish, thus creating a wider assortment of information (Elkin-Koren, 1995). This new form of communication and wider access to information resources should be encouraged to grow.

The Internet Community

In 1969, ARPANET heralded the beginning of large scale computer-mediated communications and what would eventually be called the Internet (Rheingold, 1993). ARPANET was a creation of the Advanced Research Projects Agency within the Department of Defense.

It is doubtful that the original developers of the Internet fully conceived the extent of the networked communities that would evolve from ARPANET. Howard Rheingold (1993) notes that those involved with the creation of ARPANET did have visions of groups using the network for educational purposes. They referred to these groups as interactive multi-access computer communities.

A little less than thirty years later, the use of the Internet has grown tremendously. As mentioned in a recent legal case, it is a place which is home to Tibetan monks and Icelandic fishermen (Thomas v. U.S, 1995). Individuals from around the globe meet and discuss critical issues of science, law and philosophy. Users form friendships that open up diverse cultures and social traditions.

Can the Internet be defined as a community? A community has been defined as:

"...a set of persons involved in stable patterns of communication. Communities vary widely in the range of their interactions, the capacity of their networks, and the links between information and material exchanges" (Mandelbaum, 1982).

Communities are also distinguished by lively interaction and engagement on issues of mutual concern and the well-being of communities contributes to the well-being of the commonwealth (Schuler, 1994). Such communities have their share of the ills of society: jealousy, gossip and anger (Rheingold, 1993). Communities also create and enforce shared norms and values. Network communities can be caring groups in which members share personal triumphs and tragedies. Professor Henry Perritt (1993) noted that:

"An important part of the definition of a community is the method through which it expresses obligation and enforces compliance. Rights and responsibilities are defined by custom as well as by formal law, and
enforced by group pressure or exclusion as well as by legal sanctions. Quaker meetings, corporations and municipalities have distinctly different arrangements for making rules, determining instances of noncompliance and imposing punishment."

Historically, laws were created through community meetings wherein disputes were discussed and resolved according to the norms of the community (Perritt, 1993). This idea has gained new ground in a technology-based society. In Fall 1994, an open meeting was held on the World Wide Web by the National Performance Review. Several thousand federal workers participated in the online meeting to discuss proposals for bureaucratic reforms (Hurwitz & Mallery, 1995). The meeting illuminates the potential of the many-to-many form of communication created by digital technology. Unlike the mass media era in which on-to-many communication predominated, computer networks, and likewise network communities, allow for greater democracy and decentralization.

In 1969, the U.S. government sponsors of the ARPANET considered the groups interacting on the ARPANET to be communities. Yet prosecutors representing the same government now reject the notion of a cybercommunity within the context of an appeal for criminal pornography distribution in Thomas v. U.S. (1995). Thomas was found guilty of criminal pornography distribution after a Tennessee resident downloaded pornographic materials from the BBS. In the appeal, BBS sysop Robert Thomas of Amateur Action BBS argued that the trial court should have applied the community standards of the cybercommunity instead of the standards of the Tennessee community where the material was downloaded. The U.S. government's position was that the Internet creates a global community, and it is impossible to define community standards for such a large and diverse group of users. The prosecution also relied on previous holdings of the U.S. Supreme Court which found that since the U.S. is such a large country with a diverse populace there could not be a federal community standard (Thomas vs U.S., 1995). The prosecution failed to recognize that the Amateur Action BBS is also a community similar to a town or village.

The U.S. has gone a step further in attempting to prohibit pornography distribution on the Internet through the recently enacted Communications Decency Act (1996). The new act met with widespread opposition, and was the subject of heated debate on mailing lists such as Cyberia and other forums throughout the many communities of the Internet (See [2]). A bill to repeal the Act has been sponsored by Senators Leahy and Feingold.

We assert that the Internet is clearly a networked system of many communities. Within individual cybercommunities, participants can create and define law applicable to their community. This is similar to any association of people. Rules are created to govern the organization. Such rules generally set forth the rights and obligations of the specified group. The organization attempts to solve problems internally and problems are only sent outside when all internal channels of conciliation have been used.

Creating and Enforcing Community Norms

How do existing online communities express obligation and enforce compliance? There are several mechanisms for enforcing behavioral norms on the Internet, as noted in the proceedings of the National Academy of Sciences Conference Rights and Responsibilities of Participants in Networked Communities (1993). These devices vary from group to group. There are generally three methods of enforcement on the Internet:

1. Disconnect or exile rule breakers
2. Employ peer or social pressures
3. Apply the law.

Mechanisms for enforcement vary from formal, as in contract arrangements between users and commercial providers, and informal, as in self-policing on discussion conferences. On conferences, mailing lists and BBSs, a moderator often oversees the discussion (and may "disconnect" or "unsubscribe" a troublemaker). Exile of a rulebreaker may not always work on mailing lists as technically adept users can re-subscribe from a new e-mail account. The owner or maintainer of the mailing list may not catch the new subscription even if the trouble maker uses the same name.

More recently, discussions on mailing lists and BBSs have applied real world legislation when there is a violation of a community norm. An example of this behavior is the recent U.S. case of Stratton Oakmont, Inc. v. Prodigy Services (1995) The Stratton case revolved around an incident which occurred on "Money Talk" bulletin board of the Prodigy online service. A subscriber to the bulletin board posted a message regarding the Stratton firm. The Stratton firm considered the message to be defamatory and sued Prodigy for defamation.

Suggestions of application of real-world principles of law is also apparent in discussions regarding copyright and inlining of material on the Web (Norderhaug & Oberding, 1995). As described in the HTML Specifications (See [3]), inlining is a form of hypertext markup in which the creator of a Web page can embed other content such as an image by using a textual reference describing where on the network the material is located. On most browsers, the image will automatically appear as part of the page. Importantly, there is no copy made by the page creator: the inlined material will be taken from the original source each time it is used.

The general norm has become to ask permission before inlining. However, people sometimes inline without asking permission. This transgression of community norms is generally met with a combination of social pressure on a mailing list or conference, and threats of legal action.

It is difficult to determine where the crime occurred, or in some cases if there was a crime. For example, a rape in cyberspace occurred on the LambdaMOO. A participant on the MOO manipulated the software to use the identity of another participant. A virtual rape might not be considered a crime under U.S. law prior to the Communications Decency Act, but it might violate cybercommunity standards.

Online communities clearly maintain community norms and have the ability to create and enforce rights and responsibilities. Offenders are censored if they breach commonly accepted rules. The Internet contains a high number of communities which make and enforce individual rules and obligations. Can these multiple communities create the consensus for a single law of cyberspace and is it necessary to have one set of rules to govern the whole online community?

The Consensus Issue

The creation of law in a democratic society requires a consensus of the people. As pointed out at the National Academy of Sciences Conference Rights and Responsibilities of Participants in Networked Communities, many scholars believe that there can never be a consensus to support a common law for cyberspace. Contrary to this position, rules are being created and enforced in the digital communities. These common norms include social pressure where the offender is reprimanded by the group or community as
opposed to an outside force. Behavior is also being controlled by contract between users and commercial services in which the offender is punished by cancellation of services.

Such common standards have historically formed the core of the law. While there may be consensus as to the current methods of enforcement on the Internet, the National Academy of Sciences Conference found that there is no consensus as whether new legislation should be imposed on network communities by any nation state. Despite the lack of cohesive thought regarding the need for new law, consensus building takes place regularly within online communities. This is apparent from the informal creation of rules and enforcement of penalties. Such consensus building within the network is the fundament of any future legal regime or regimes.

However, there is a dichotomy between the community standards applied within the network as opposed to the legal standards applied from outside the Internet community. A network community standard may be accepted and followed by net citizens, but external legal standards can be flagrantly violated despite the fact that wrongdoers may be punished by the nation state. When there is no fear of punishment from the authorities, the nation state no longer has power to control the individual. Despite the wild reputation created by the media, the network communities mostly consist of law-abiding people. Many of these individuals want to work toward appropriate legal standards and within current political constraints.

Cyberspace is not a nation state. The community standards of the many network communities are not a formal legal system. There is a lack of consensus as to whether new laws should be created or if old laws can be applied to the digital realm. However, rules are being created and enforced by individual communities. Although community standards do not, alone, constitute a legal system, such standards create the basis for formal legal systems. The existence of such norms is evidence of the ability of the social system to create law.

**The Need for a Separate Jurisdiction**

In a recent article in Communications of the ACM, John Perry Barlow (1995) argues that the nature of copyright law is such that it can be enforced globally. Many, including Barlow, have argued that changes to copyright law proposed by the National Information Infrastructure White Paper will have a global impact. However, the nature of jurisdiction is such that it is limited to the territorial boundaries of the nation. While copyright law is fairly similar from country to country with noted exceptions, proposed changes to U.S. copyright law via the NII cannot be asserted globally in the absence of an international convention or heavy political pressure by Washington (Samuelson, 1996). Changes in U.S. law are limited to U.S. borders. As a result, crafty individuals could play a technological version of forum shopping by picking and choosing where to locate servers in order to obtain the best legal environment:

"The effectiveness of the state's sanction... is an inverse function of the ease with which the lower order controllers can "exit" from the regime defined by those laws- by evading detection of rule-violating behavior, evading the State-imposed sanctions for such violations, or somehow withdrawing from the rule-making jurisdiction of the State as controller" (Post, 1995).

The mere possibility that individuals might be able to escape the jurisdiction of one nation by relocating computer-mediated information and services to another nation is an insufficient reason to create formally a separate jurisdiction for cyberlaw. Certainly, there are some who would see this as a argument not to create any type of legal system.
solely for online communication. However, this is not the case. U.S. law and the law of
other nations does extend to cyberspace assuming certain legal requirements can be met
such as whether the person would anticipate being brought into the specific court for a
lawsuit. This is the first step in the jurisdiction analysis. Many argue that if a person
commits a crime in cyberspace, then he can be brought to court in the country where he
was located when committing the crime. The jurisdiction issue in computer-mediated
communication is not so simple, particularly if the victim is located in another country.

This blurs the meaning of the concept of "border". Certainly, piracy of real ships and
cargo on the sea is much different from piracy of intellectual property on the Internet.
One can usually determine when an act occurred on the sea, but where and when does a
specific act occur in cyberspace as opposed to real world? How would one pinpoint the
time and location of a given event without real world references? Jurisdiction may be an
anachronism in a borderless world where time and distance have little meaning (Katsh,
1995).

The method by which technology delivers online communication changes the impact of
the law. In the caching example, copies are made to improve the efficiency of the system
and are probably fair use under a copyright analysis. Yet an argument can be made that
these copies impede the ability of the Web page creator to earn revenue.

The companies that provide a Web presence for business clients often derive income
from their "hits" (i.e., the number of times a Web page is accessed). Some large Internet
service providers, such as America Online, regularly keep a copy of frequently accessed
Web pages on their own computers. When a page is cached, it will only be requested
once from the site even if a thousand people browse the page. As a result, the presence
provider will get a smaller hit-count to show to clients. This might create problems in
collecting a revenue, which would be considered by a U.S. court in analyzing a fair use
claim.

Does cyberspace require the formal creation of a separate jurisdiction? Probably not, as
an informal separate jurisdiction already exists based on the nature of network
computer-mediated communication. This is evident in several respects:

1. Laws are being created and enforced by cybercommunities;
2. The laws of the cybercommunities are generally inapplicable outside the online
   community;
3. The laws of the outside world are generally difficult to apply to the online world;
   and
4. The outside world must create new law to control the online world.

Caching is one example of the problem of applying real world law to the internet. In
order to deal with these problems, steps must be taken by cybercommunities to outline
the proper application of real world law to technology. While there has been plenty of
discussion on mailing lists such as CNI-Copyright, there have not been any real attempts
to develop a code for the Internet by legal scholars (See [4]). There are many questions
which deserve and require serious analysis to promote the progress of computer-
mediated communication. Scholars, technologists and lay people can work together to
create effective guidance for courts and governments in the application and creation of
law.

The Rule Makers

One might be tempted to argue that no laws should be created for the Internet. However,
this would ignore the fact that rules are already being created to govern specific communities in cyberspace. These rules range from the contracts between service providers and users to the simple rules for participation in a moderated mailing list discussion.

Who should create the laws for the Internet? The National Academy of Sciences sponsored a Conference in 1993 to investigate rule making in networked communities. Some of the issues considered regarding the rights and responsibilities of network participants included: Who is liable when someone posts a defamatory message, child pornography or copyrighted material on a public bulletin board? Debate is also occurring on these issues and others on mailing lists, online forums such as Lexis Counsel Connect, usenet groups and newsletters (see [5]). These are a few important issues discussed in the network society. Resolution of some of these issues has occurred in U.S. courts. However, these court decisions may not always make sense within the technical constraints of the digital network.

Recently, an organization was created to research important network issues and make recommendations to governments and other interested entities. This group, known as the Internet Law Task Force, can be the liaison between the network community and the state. The Task Force is composed of a wide variety of individuals from many backgrounds and will probably be more sensitive to community and technological issues. Peter F. Harter, former executive director and general counsel of the National Public Telecomputing Network, noted in a recent article that the Internet Law Task Force could be analogous to the Internet Engineering Task Force. The IETF is a volunteer body that meets regularly to discuss and determine... technical standards (Harter, 1995, p. 10). The group could go one step further and assist in conflict management. Conflicts could be mediated first within the network community system prior to any legal action.

The Task Force is in a position to impact potential legal issues without a separate jurisdiction. This group can serve to educate legislative and administrative officials regarding the technical and network ramifications of any pending legislation. Through the efforts of the task force, governments could avoid potential legislation which would be detrimental to the future of the network.

**Conclusion**

"It cannot be helped, it is as it should be, that the law is behind the times." (Oliver Wendell Holmes, 1934, p. 102)

The advent of computer-mediated communication has created a new world with new rules. The change in the presentation of information is not superficial but changes the culture and its institutions. The Gutenberg press resulted in the creation of many institutions including copyright law (Katsh, 1995). The key to change lies in understanding how a medium affects patterns in communication.

However, change in the medium does not necessarily mean that a new single system of law must be created to solve the problems on the Internet. Laws are already being created by cybercommunities. When the law changes with every new event, then there is no law (Katsh, 1995). The law cannot be made to ride on the back of the wind. Instead, the law should be like a sail; sturdy but flexible and able to navigate through use of the wind.

Groups such as the Internet Task Force can develop norms and determine how to resolve
conflicts in cooperation with technologists, service providers and others. Such norms can be used as guidance for courts and governments. Understanding technology is key to resolving the conflicts between law and technology. Efforts to develop norms can bridge the gap between old laws and new technology.

Footnotes


[2] Cyberia-L, an Internet mailing list maintained by Prof. Trotter Hardy.


[4] CNI-Copyright is a mailing list on the Internet. The focus of the discussion is copyright in general and usually from a U.S. perspective, although there are participants from many countries. The participants are composed of lawyers, law professors and laymen.

[5] There are many legal mailing lists, online journals, seminars, newsletters, etc. devoted to the issues of cyberlaw. Some of these resources are available from http://www.oberding.com/~juliet/resources.html

References


Communications Decency Act of 1996 47 USC section 223.

Creative Technology Ltd. v. Aztech System PTE ltd. 95 Daily Journal D.A.R. 9814


