UNIT -5

INTERNET JURISDICTION

STRUCTURE

5.1 INTRODUCTION

5.2 OBJECTIVES

5.3 SUBJECT

5.3.1 THE BASICS OF JURISDICTION

5.3.1.1 PERSONAL JURISDICTION

5.3.1.2 APPLICABILITY OF LAW

5.3.1.3 ENFORCEMENT OF JUDGMENTS

5.3.2 INTERNET AND THE GEOGRAPHICAL BOUNDARIES

5.3.3 THE OPTIMAL EXTENT OF AN ENTITY'S JURISDICTION OVER THE INTERNET

5.3.4 THE LAW OF THE SERVER

5.3.5 THE THEORY OF INTERNATIONAL SPACES

5.4 SUMMARY

5.5 GLOSSARY

5.6 SAQS

5.7 REFERENCES

5.8 SUGGESTED READINGS

5.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

5.10 ANSWER SAQS

5.1 INTRODUCTION

The Internet is an interstate and international medium. The global nature of the internet - both its global reach and its perceived "boundary less" architecture - presents a host of jurisdictional complexities for any sovereign seeking to define and / or enforce laws regulating its use. What are the proper boundaries of a sovereign's reach on the internet and how can these boundaries be implemented in practice?

In exploring this issue, this module first reviews the basics of jurisdiction. Functionally, cyberspace/Internet 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. 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 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. In previous unit the principals of international law have been discussed.

5.2 OBJECTIVES

After reading this unit you will be able to understand:

- Personal Jurisdiction
- Geographical boundaries and the internet
- What is the optimal extent of an entity's jurisdiction over the internet?
- Localized regulation and the optimal extent of control
- Rejecting Territoriality: "The Law of the Server"
- The Theory of International Spaces

5.3 SUBJECT

5.3.1 THE BASICS OF JURISDICTION

5.3.1.1 PERSONAL JURISDICTION

The requirement of personal jurisdiction prevents the courts of a sovereign from exercising authority over persons who have little or no relation to that sovereign. Personal jurisdiction is distinct from subject matter jurisdiction which governs the types of cases (e.g., traffic violations v. murder trials v. constitutional questions) that a court is competent to decide.

(i) United States

In the context of internet or cyber transactions, jurisdictions pose a major challenge in interpretations in countries like United States where there is a conflict of laws as it is not uniform throughout the country and States having their own laws. Finding personal jurisdiction in the United States requires a two-step inquiry. A typical statute might provide jurisdiction where:

-Defendant is incorporated in the state; or

- Defendant is registered to do business in the state; or

- Defendant has insured a resident of the state; or

- Defendant has engaged in a tort within the state

The exercise of jurisdiction authorized by state law must comport with the due process guarantees of the federal constitution. There are several ways to satisfy the requirements of due process: (1) general jurisdiction, (2) specific jurisdiction, (3) personal service, (4) consent, and (5) a valid forum selection clause. General jurisdiction arises when defendant has substantial

and continuous contacts with the forum state. For example, a state would have general jurisdiction over a company headquartered in that state or over an individual who is a citizen of that state. Specific jurisdiction arises when there are minimum contacts with the forum state, the suit arises from or relates to those contacts and the exercise of jurisdiction would be fundamentally fair. A defendant who does significant business in the forum state likely satisfies this minimum contacts requirement. Personal jurisdiction is also constitutional when a defendant explicitly or implicitly consents, as when he appears in court and defends his case on the merits. Finally, forum selection clauses can satisfy the constitutional due process requirements so long as they are not imposed to deter suit and are not a result of fraud. Several states have statutes authorizing personal jurisdiction whenever constitutional. In those states, as with federal courts, the issue of personal jurisdiction collapses into the single due process inquiry[1].

(ii) European Union

In the European Union, several Conventions govern the circumstances in which the exercise of jurisdiction is proper, and various scholars have recently suggested how those conventions would and should apply to internet-related disputes.

Under the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, the power of a state to assert jurisdiction over a person domiciled therein will be decided according to the law of that state. Several exceptions to this principle have been enumerated. For example, in contractual relationships, a person may be sued in the courts of the country where the obligation was to be performed. In the case of involvement of a branch, agency or other establishment, the courts of the place where such branch, etc. is situated have jurisdiction to adjudicate the matter. In consumer disputes, the complainant is entitled to bring proceedings against a supplier of goods or services or a creditor in the state where the consumer is domiciled. Finally, an entrepreneur can only bring proceedings against a consumer in the country where the consumer is domiciled.

The Romano Convention on the Law Applicable to Contractual Obligations deals with international private law. Parties are free to choose the law applicable to a whole contract or to parts of a contract. In the absence of any valid agreement regarding choice of law, the applicable law shall be that of the country most closely connected to the agreement. Here too, consumers are given special protection. A consumer's right under the law of his domicile cannot be overridden by a contractual choice-of-law provision if (1) the execution of the contract was preceded by specific invitations addressed to the consumer or by advertising directed towards the consumer; or (2) the seller or its agents received the order in the country of the consumer.

Agne Lindberg argues that, when these conventions are applied to internet-related disputes, the physical domicile of entrepreneurs acting on the internet will still be the determining factor when deciding which the competent courts are and which the applicable law within the E.U. countries is. He suggests that these Conventions are already well suited for the internet

[1]"Jurisdiction in Cyberspaceby" Jonathan Zittrain (Article)

transactions and that the European Court of Justice can and will apply them properly to the new medium. In the E.U. context the "country of destination rule," is also important which entitles a consumer to bring suit in his own domicile whenever the defendant has been pursuing business activities in the consumer's domicile or directing commercial activities towards that state. In relation to e-commerce, this rule, in view of Frederica Greggio and Andrea Platania, would mean that the proprietor of an interactive website based in an E.U. Member State would be subject to the jurisdiction of any E.U. Member State where his website is accessible.

The European Commission has proposed the targeting approach in its draft regulation to implement the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters as part of E.U. Law.

(iii) Australia

In Australia, a personal action typically is initiated by serving the defendant with a writ or other originating process. Such service generally establishes the court's adjudicative jurisdiction over the person served. Regarding interstate service, the Service and Execution of Process Act of 1992 provides for jurisdiction by initiating process in an Australian State or Territory to be served in another State without the need to show a nexus between the initiating State and the parties or the cause of action.

Gutnick v. Dow Jones & Co., [2001] V.S.C. 305, is an application of Australian law to an internet defamation case.

5.3.1.2 APPLICABILITY OF LAW

After the resolving of the question of jurisdiction over the parties, the next question is: what body of substantive law should be used to resolve the controversy? The laws in force in different countries pertaining to the internet vary considerably. Thus, the choice of law can be dispositive and almost always matters greatly. In the United States, the meta-doctrine that determines which substantive law should be applied in known as conflict of laws. In other countries it is more likely to be called private international law. This is a notoriously unstable, shifting field of doctrine, characterized by warring principles or tests. Some of the major contending principles include the 'the most significant relationship' test, the 'centre of gravity' approach, and the 'interest' approach.

It is far from clear how this body of law will or should be brought to bear on internet-related disputes. Paul Edward Geller focuses on lawsuits claiming infringement of intellectual property over the Net. Geller argues that, in such cases, cross-border infringing acts could be best localized by considering consequences for judicial remedies.

5.3.1.3 ENFORCEMENT OF JUDGMENTS

Naturally, the judgment of a court is only meaningful to the extent that it can be enforced. A sovereign can only enforce the judgments of its courts insofar as:

i) a defendant or his assets can be reached by the enforcement mechanisms of the sovereign,
ii) ii) the sovereign can get extradition of the absent defendant from some other sovereign, or
iii) iii) foreign states will enforce the judgment of the sovereign. Within the United States,

All three of these enforcement methods are available among states: the first by exercise of police power, the second for enforcement of criminal laws, and the third by requirement of the full faith and credit clause of the federal constitution. Internationally, the problem is more complicated and is governed by the doctrine of international comity. A state generally will not enforce a foreign judgment it views as manifestly unreasonable. If it wishes its judgment enforced, therefore, a state will only be able to exercise jurisdiction over defendants that have some significant tie to the forum state (e.g., the defendant is present there, has assets there, or causes significant harm there).[2]

5.3.2 INTERNET AND THE GEOGRAPHICAL BOUNDARIES

"The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behaviour; (2) the effects of online behaviour on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply… The internet has no territorially-based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location …. Location remains vitally important, but only location within a virtual space consisting of the "addresses" of the machines between which messages and information are routed. The system is indifferent to the physical location of those machines, and there is no necessary connection between an internet address and a physical jurisdiction. Although a domain name, when initially assigned to a given machine, may be associated with a particular internet Protocol address corresponding to the territory within which the machine is physically located (e.g., a "uk" domain name extension), the machine may move in physical space without any movement in the logical domain name space of the Net. Or, alternatively, the owner of the domain name might request that the name become associated with an entirely different machine, in a different physical location. Thus, a server with a ".uk" domain name may not necessarily be located in the United Kingdom, a server with a ".com" domain name may be anywhere, and users, generally speaking, are not even aware of the location of the server that stores the content that they read. Physical borders no longer can function as

[2] "Jurisdiction in Cyberspaceby" Jonathan Zittrain (Article)

signposts informing individuals of the obligations assumed by entering into a new, legally significant, place, because individuals are unaware of the existence of those borders as they move through virtual space."[3]

Since 1996 (when the article was written), however, technology efforts aimed at enabling the introduction of geographical boundaries have been somewhat successful. The most common approach involves "ip mapping," or the mapping of an internet user's ip address to a geographic region. Ip mapping is based on the fact that while, in theory, ip addresses need not correlate with geographic location at all, in practice, they do. Internet Service Providers ("ISPs") (through which most people access the internet) usually assign their customers ip addresses based on geographic location. A provider of ip mapping "technology" essentially assembles a massive directory of this information; ip addresses can be "looked up" in the directory and an associated geographic location provided, if available. Moreover, the directory can store other information about the user derivable from the ip address, like the identity of his / her ISP and the bandwidth of his / her connection to the internet. It is important to stress that ip mapping is not a science. It often requires business relationships with ISPs to uncover geographic data on their customers and a host of technological issues - largely a result of the fact that, fundamentally, the internet was not designed to preserve geographic information can make the data highly unreliable. The imperfect character of the technology is evident in the product descriptions crafted by its providers. For example, Quova, one of the leading developers of this technology, describes its GeoPoint product as follows:

"GeoPoint provides the geographic location of your Web site visitors in real time. It is the best geolocation service available……We combine automated technology with expert human analysis to provide unsurpassed global coverage and data quality….Each piece of information comes with a confidence factor representing the probability it is correct….GeoPoint is truly enterprise-class, with easy integration, an application management utility, reliable performance, and scalability to any business size. Finally, we stand behind our service. Accuracy, performance, and system availability are guaranteed by the industry's first Service Level Agreement."

Though imperfect, IP mapping can be very effective, particularly when users of the technology do not require a high degree of specificity / granularity in defining geographic locations. IP mapping can very accurately predict the country from which a viewer accesses your site where it might fail to reliably predict his / her town.

In the context of our discussion of jurisdiction on the internet, the most notable use of the technology is, naturally, using IP mapping to guarantee compliance with the regulations of the sovereign state in which a user resides. Given the ability to know the geographic location of its

---

[3]As Johnson and Post explain in their 1996 article, "Law and Borders: The Rise of Law in Cyberspace":

viewers, a company can construct its website so as to respond differently to viewers in different geographic regions as a function of the respective laws of those regions.

Beyond the use of techniques like ip mapping to predict geographic locations, some argue that the fundamental architecture of the internet should be augmented so as to preserve and report reliable geography data. While the internet as it is currently designed does not preserve geographic information, nothing says that it could not do so in the future.[4]

5.3.3 THE OPTIMAL EXTENT OF AN ENTITY'S JURISDICTION OVER THE INTERNET

The internet as its own international space

Johnson and Post (discussed above) argue that the internet, or "cyberspace", should be treated as a distinct territory or sovereignty subject to its own self-governance and worthy of deference from other sovereignties. According to him,"Global electronic communications have created new spaces in which distinct rule sets will evolve. The law of any given place must take into account the special characteristics of the space it regulates and the types of persons, places, and things found there. Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world. For example, the law of the Net must deal with persons who "exist" in Cyberspace only in the form of an email address and whose purported identity may or may not accurately correspond to physical characteristics in the real world. In fact, an e-mail address might not even belong to a single person. Accordingly, if Cyberspace law is to recognize the nature of its "subjects," it cannot rest on the same doctrines that give geographically based sovereigns jurisdiction over "whole," locatable, physical persons. The law of the Net must be prepared to deal with persons who manifest themselves only by means of a particular ID, user account, or domain name.

Similarly, the types of "properties" that can become the subject of legal discussion in Cyberspace will differ from real world real estate or tangible objects. For example, in the real world the physical covers of a book delineate the boundaries of a "work" for purposes of copyright law; those limits may disappear entirely when the same materials are part of a large

---

[4] http://cyber.law.harvard.edu/ilaw/juris.htm; as stated by Jonathan Zittrain in his article "Jurisdiction in cyber space"

electronic database. Thus, we may have to change the "fair use" doctrine in copyright law that previously depended on calculating what portion of the physical work was copied.

Localized regulation and the optimal extent of control

In considering the optimal extent of a sovereign's authority over the internet, one can look to two clear and opposite extremes. The rule might be that a defendant will only be subject to jurisdiction for his internet activities in his home forum, or the rule might be that a defendant will be subject to jurisdiction for his internet activities everywhere those activities are accessible or have a major effect.

The extreme of universal jurisdiction is immediately limited by practical considerations. While these practical limits are substantial limits, additional, theoretical problems remain. Consider, for example, the defendant who facilitates the sale of Nazi memorabilia through an internet auction site. Claiming the display of Nazi images is indecent and against its law, a foreign state orders the defendant to remove the Nazi images and the defendant complies. The notable side effect of this is that not only are citizens of the foreign state protected from the Nazi images, but also citizens of all states who previously might have accessed the images. Several authors have argued that these "overflow effects" of internet jurisdiction are undesirable. Whether or not one agrees with their position, the problem of overflow effects is not unique to internet cases. As other authors point out, U.S. antitrust regulations have substantial effects on the price of products and the structure of markets beyond U.S. borders. Moreover, as technology like ip mapping improves, or as fundamental changes to the internet's architecture are implemented, our hypothetical defendant may be able to effectively remove the Nazi images only for those viewers located in the foreign state. The overflow effect is, in short, a result of the "boundary less ness" of the internet. To the extent boundaries are introduced, the overflow effect is reduced. A second problem is notice. Defendant individuals or small businessmen will not know the laws of all the jurisdictions from which their web sites will be accessible and it therefore seems unjust to hold them accountable under those laws. This problem might suggest only that a warning or a cease and desist notice in internet suits should be issued before a defendant faces liability.

Territorial regulation of internet disputes is difficult and costly for states because of the international context of many internet disputes. There are feasible alternatives: voluntary alternative dispute resolution coupled with an international enforcement regime, international treaties or conventions such as those in force in the E.U. on the exercise of personal jurisdiction, and international treaties or conventions on rules of substantive law to be applied no matter which court exercises jurisdiction. Each of these three options requires progressively more surrender of local sovereign authority. In the first, a state must surrender its right to review and reject the judgment of an arbitrator or other alternative tribunal. In the second, a state must give up the power to decide when its courts will be able to hear international internet disputes. In the last, a state must surrender its very law-making power over internet disputes in favour of some international compromise. As international use of the internet increases, internet disputes will grow in number, size and complexity. This growth will impose greater costs on sovereigns

of maintaining local authority and we should therefore expect alternatives to sovereignty to increase in importance.

5.3.4 THE LAW OF THE SERVER

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 suits 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 up loader 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 up loader 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 up loader and the "location" of the webpage. As a practical matter, we know that data sent from an up loader 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 territorialisation of cyberspace through its servers would create jurisdictional havoc and may produce strange results if applied literally. For example, could an up loader 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 up loader and the downloader and insist on exercising territorial jurisdiction over webpages "located" at a server. Under the theory of the up loader and the downloader[5], the act of uploading is performed entirely at the computer terminal of the up loader, 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 up loader 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" 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 equalinterest 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[6] file containing pornography cannot be "obscene" until compiled and displayed on the

[5]See unit 4

[6]The term "gif" file refers to pictures saved in the CompuServe format.

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 create jurisdictional disorder. Surely, 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."[7]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 "up loader and downloader." The up loader and the downloader do not necessarily know who or where the other is. Persons traveling around cyberspace need to know what set of laws applies to their actions. If we reject the territorialisation of cyberspace and accept the theory of the up loader and the downloader, we must reject the broad form of the "law of the server."

By contrast, the theory of international spaces 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).[8] The rule of nationality incyberspace means that United States nationals and corporations cannot 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.

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

[7]See William Byassee, Jurisdiction of Cyberspace: Applying Real World Precedentto 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).
[8]Sysop means "system operator,"

sysop could be criminally liable for the content over which he has some measure of control, regardless of the nationality or location of the up loader, but an up loader would only be criminally liable if he was located within the territory of the forum state, or was a national of that forum state.

In 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 up loader. 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 favour of free speech on the Internet (a principle soundly upheld in *Reno*[9]), 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" will understand that a single person often cannot 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 up loaders.[10]

5.3.5 THE THEORY OF INTERNATIONAL SPACES

The theory of international spaces begins with one proposal: 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.[11]Other informal arrangements (for instance, the United States providing all air traffic control in Antarctica) weigh heavily in decisions about jurisdiction.

One approach is to treat these three areas as *sui generis* treaty regimes. Some scholars see international law as no more than the sum of various international agreements—a purely positivist approach. This has the facing of theoretical consistency, but only if we fail to recognize an evolving organic international legal system. The next theoretical and conceptual

[9]Reno v. ACLU, 117 S.Ct. 2329 (1997).

[10]Jonathan Zittrain in his article "Jurisdiction in cyber space"

[11]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].

hurdle is physicality. These three physical spaces are nothing at all like cyberspace which is a nonphysical 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 theorise three more dissimilar physicality —the ocean, a continent, and the sky. Their international, sovereign less quality makes them analogous, not the any physical similarity. 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.

5.4 SUMMARY

The Internet is an interstate and international medium. The global nature of the internet - both its global reach and its perceived "boundary less" architecture - presents a host of jurisdictional complexities for any sovereign seeking to define and / or enforce laws regulating its use.

The requirement of personal jurisdiction prevents the courts of a sovereign from exercising authority over persons who have little or no relation to that sovereign. In the context of internet or cyber transactions, jurisdictions pose a major challenge in interpretations in countries like United States where there is a conflict of laws as it is not uniform throughout the country and States having their own laws. Several states have statutes authorizing personal jurisdiction whenever constitutional. In those states, as with federal courts, the issue of personal jurisdiction collapses into the single due process inquiry.

In the European Union, several Conventions govern the circumstances in which the exercise of jurisdiction is proper, and various scholars have recently suggested how those conventions would and should apply to internet-related disputes. The European Commission has proposed the targeting approach in its draft regulation to implement the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters as part of E.U. Law.

In Australia, a personal action typically is initiated by serving the defendant with a writ or other originating process. Such service generally establishes the court's adjudicative jurisdiction over the person served. Regarding interstate service, the Service and Execution of Process Act of 1992 provides for jurisdiction by initiating process in an Australian State or Territory to be served in another State without the need to show a nexus between the initiating State and the parties or the cause of action.

After the resolving of the question of jurisdiction over the parties, the next question is: what body of substantive law should be used to resolve the controversy? The laws in force in different countries pertaining to the internet vary considerably. Thus, the choice of law can be dispositive and almost always matters greatly. In the United States, the meta-doctrine that determines which substantive law should be applied in known as conflict of laws. In other countries it is more likely to be called private international law. Naturally, the judgment of a

court is only meaningful to the extent that it can be enforced. A sovereign can only enforce the judgments of its courts insofar as:

i) a defendant or his assets can be reached by the enforcement mechanisms of the sovereign,
ii) ii) the sovereign can get extradition of the absent defendant from some other sovereign, or
iii) iii) Foreign states will enforce the judgment of the sovereign. Within the United States,

All three of these enforcement methods are available among states: the first by exercise of police power, the second for enforcement of criminal laws, and the third by requirement of the full faith and credit clause of the federal constitution. Internationally, the problem is more complicated and is governed by the doctrine of international comity. A state generally will not enforce a foreign judgment it views as manifestly unreasonable.

The rise of the global computer network is destroying the link between geographical locations. The system is indifferent to the physical location of those machines, and there is no necessary connection between an internet address and a physical jurisdiction. Although a domain name, when initially assigned to a given machine, may be associated with a particular internet Protocol address corresponding to the territory within which the machine is physically located (e.g., a ".uk" domain name extension), the machine may move in physical space without any movement in the logical domain name space of the Net. Or, alternatively, the owner of the domain name might request that the name become associated with an entirely different machine, in a different physical location. Thus, a server with a ".uk" domain name may not necessarily be located in the United Kingdom, a server with a ".com" domain name may be anywhere, and users, generally speaking, are not even aware of the location of the server that stores the content that they read. Though imperfect, IP mapping can be very effective, particularly when users of the technology do not require a high degree of specificity / granularity in defining geographic locations. IP mapping can very accurately predict the country from which a viewer accesses your site where it might fail to reliably predict his / her town.

Beyond the use of techniques like ip mapping to predict geographic locations, some argue that the fundamental architecture of the internet should be augmented so as to preserve and report reliable geography data. While the internet as it is currently designed does not preserve geographic information, nothing says that it could not do so in the future.

Johnson and Post (discussed above) argue that the internet, or "cyberspace", should be treated as a distinct territory or sovereignty subject to its own self-governance and worthy of deference from other sovereignties. According to him, “Global electronic communications have created new spaces in which distinct rule sets will evolve. The law of any given place must take into account the special characteristics of the space it regulates and the types of persons, places, and things found there. Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world. Similarly, the types of "properties" that can become

the subject of legal discussion in Cyberspace will differ from real world real estate or tangible objects.

In considering the optimal extent of a sovereign's authority over the internet, one can look to two clear and opposite extremes. The rule might be that a defendant will only be subject to jurisdiction for his internet activities in his home forum, or the rule might be that a defendant will be subject to jurisdiction for his internet activities everywhere those activities are accessible or have a major effect.

As international use of the internet increases, internet disputes will grow in number, size and complexity. This growth will impose greater costs on sovereigns of maintaining local authority and we should therefore expect alternatives to sovereignty to increase in importance.

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 suits 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 up loader 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 up loader is in a foreign jurisdiction, this analysis displays fatal shortcomings. 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 up loader, but an up loader would only be criminally liable if he was located within the territory of the forum state, or was a national of that forum state.

The theory of international spaces begins with one proposal: nationality, not territoriality, is the basis for the jurisdiction to prescribe in outer space, Antarctica, and the high seas. One approach is to treat these three areas as *sui generis* treaty regimes. Some scholars see international law as no more than the sum of various international agreements—a purely positivist approach. The next theoretical and conceptual hurdle is physicality. These three physical spaces are nothing at all like cyberspace which is a nonphysical space. 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.

5.5 GLOSSARY

1. RESTATEMENT (TEST) - 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."

2. SPAMMING - "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. 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).

3. *PERSONA NON GRATA* - a diplomat who is unacceptable to the government to which he is sent; a person who for some reason is not wanted or welcome

4. VICARIOUS LIABILITY- A master is vicariously liable for the tort of his servant, principal for the tort of his agent and partners for the tort of a partner. For detail see unit 2.

5.6 SAQS

1. TICK THE CORRECT ANSWER:

(i) The basics of jurisdiction includes:

(a) Personal Jurisdiction

(b) Applicability of law

(c) Enforcement of judgments

(d) All of above

(e) None of aove

(ii) In the European Union, which of the following Convention/Conventions govern the circumstances for the proper exercise of jurisdiction :

(a) Lugano Convention

(b) The Romano Convention

(c) The Brussels Convention

(d) All of above

(e) None of aove

(iii) Which of the following theories or laws is/are related to the Internet jurisdiction:

(a) Theory of up loader and downloader

(b) Theory of the International space

(c) Law of server

(d) All of above

(e) None of aove

(iv) Select the odd one:

(a) Antarctica

(b) Outer space

(c) High sea

(d) Cyberspace

2. True and false statement:

(i) The cost and speed of message transmission on the Net is almost entirely independent of physical location. True/False

(ii) Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world. True/False

(iii) Territorial regulation of internet disputes is difficult and costly for states because of the international context of many internet disputes. True/False

(iv) Cyberspace should be treated as fourth international space. True/False

(v) The rise of the global computer network makes difficult the power of local governments to assert control over online behaviour. True/False

(vi) The internet has its own territory and boundaries. True/False

5.7 REFERENCES

1. http://cyber.law.harvard.edu/ilaw/juris.htm

2.http://corporate.findlaw.com/litigation-disputes/standards-for-internet-jurisdiction.html#sthash.QQlP6KLp.dpuf

3. Article by Johnson and Post "Law and Borders: The Rise of Law in Cyberspace":

4. “Jurisdiction in Cyber space by” by Jonathan Zittrain (Article)

5. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

6. Jurisdiction in Cyberspace: A theory of International Spaces; *Darrel C. Menthe*

5.8 SUGGESTED READINGS

1. Jurisdiction in Cyberspace: A theory of International Spaces; *Darrel C. Menthe*
2. Gupta & Agarwal, Cyber Law; Ist edition, Premiere Publishing Company

5.9 TERMINAL QUESTIONS AND MODEL QUESTIONS

1. Explain the basics of jurisdiction in brief**.**

2. Discuss the various theories of Internet jurisdiction.

3. What are the major issues in Internet jurisdiction?

4. What do understand by the international spaces? Do you think that cyberspace should be treated as international space?

5.10 ANSWER SAQS

1. (i) (d); (ii) (d); (iii) (d); (iv) (d); (v) True;

2. (i) True; (ii) True; (iii) True; (iv) True; (v) False;