TOWARDS CONTAINING THE JURISDICTIONAL PROBLEMS IN PROSECUTING CYBERCRIMES: CASE REVIEWS AND RESPONSES[1]

Abstract
This enquiry does a case study of the havoc wreaked by cybercrimes on some nations' critical infrastructure with a view to fashioning comprehensive legal responses. Often, the suspect perpetrates his/her act from a jurisdiction, while the effects of that act are felt in another jurisdiction. The study discovers that these jurisdictional differences pose serious problem for investigation, evidence gathering and prosecution. It is also revealed that lack of double, triple, quadruple, and so on, criminality as the case may be, depending on the number of affected jurisdictions, further compounds the problem. As a result of the rising tide in cyber criminality in the world today, various theories have been proffered by courts and jurists. After due diligent consideration of these theories, this essay settles with a more universalist approach. Thus, in the light of the transnational nature of cyberspace and the dispersed nature of the Internet, this study strongly suggests a global multilateral treaty which settles the thorny issue of jurisdiction at least in relation to member states.

Key words: *Jurisdictional Problems, Cybercrimes, Prosecution, Internet, Cyber Law*

1. Introduction

The investigation of cybercrime within any given country is difficult enough. The need to ensure that evidence is available, secured and free from tampering, and admissible is sufficiently challenging. When an international cross-border element is added to the mix, the legal, evidentiary and jurisdictional problems are manifold.[2] A few cases highlighting the jurisdictional problem will be discussed below. This paper investigates further the various attempts made by scholars and jurisdictions to tackle the problem. The study examines the different theories proposed by jurists and courts in an effort to address the problem. The discourse will not only provide the theoretical epistemological framework for, but also will delineate the differential elements in, the appraisal of jurisdictional issues and problems in Cyberspace.

2. Case Studies

The 'Love Bug' virus, which was unleashed onto the Internet in 1999, wreaked havoc in many countries across the world. It affected systems owned by government agencies in the United States; it disabled Automated Teller Machines (ATMs) in Belgium; and affected many companies like Ford, Siemens and Microsoft. The virus is estimated to have affected over forty-five million users in more than twenty countries. The Federal Bureau of Investigation in the United States traced the virus to the Philippines. [3] It was later found that one Onel de Guzman, a former computer science student was responsible for creating and disseminating the virus.[4] Unfortunately, hacking and distribution of viruses had not been criminalized under the laws of the Philippines and because extradition requires double criminality, de Guzman could not be extradited for prosecution by other countries that had already criminalized distribution of viruses such as the United States. Despite having caused billions of dollars in damage to

[1]By **Ikenga K.E. ORAEGBUNAM, PhD (Law), PhD (Phil.), PhD (Rel. & Soc.), MEd, BL,** Senior Lecturer and Ag Head, Department of International Law & Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria. E-mail: ik.oraegbunam@unizik.edu.ng. Phone Number: +2348034711211.

[2] K.H. Tan, *Prosecuting Foreign-Based Computer Crimes: International Law and Technology Collide*, paper presented at High-Level Political Signing Conference for the United Nations Convention against Transnational Organized Crime and the Protocols Thereto Symposium on Rule of Law in the Global Village, December 12-14, 2000, Palermo, Italy. Available online at www.unodc.org/palermo/pdf/tan-paper.pdf . Last visited on 05-09-15.

[3] L. Grossman, "Attack of the Love Bug", *TIME EUROPE*, (May 15, 2000), available online at http://www.time.com/time/europe/magazine/2000/0515/cover.html. Last visited on 15-06-15.

[4] *Ibid.*

thousands of victims in numerous nations, de Guzman could not be prosecuted. To prevent a recurrence of another 'Love Bug' scenario, the Philippines quickly enacted a law to tackle cybercrimes including the creation and dissemination of viruses.[5]

Earlier on, in 1992, hackers from Switzerland attacked the San Diego Supercomputer Center.[6] The United States sought help from the Swiss authorities, but the investigation was also hindered by lack of dual criminality, that is, the two nations did not have similar laws banning the conduct, which became an impediment to official cooperation. Eventually, local police in Zurich did render informal assistance, and they prepared a list of questions for United States authorities to answer, transmitted through official channels, so that the case could be properly pursued. After the United States answered those questions, but before follow-up questions could be answered through official channels, the hacking stopped, the trail went cold, and the case had to be closed.

In another case that occurred in 1995, the Federal Bureau of Investigation (FBI) investigated a hacker named Julio Cesar Ardita[7] from Argentina who obtained unauthorized access to several computer systems in the U.S. Although the U.S. has an extradition treaty with Argentina, Argentina did not agree to extradite Ardita to the U.S. after investigation and arrest due to a lack of double criminality. In the *Ardita* case, the criminal act was 'unauthorized access to a computer system' which is not a crime under the laws of Argentina. Fortunately, though the U.S. was not able to have Ardita extradited, he eventually agreed in 1998 to come to the U.S. and he pleaded guilty to his crimes.

In the *Vladimir Levin* case,[8] a group of Russian computer hackers, between June and October 1994, attempted to steal approximately US$10.7 million from various Citibank customers' accounts in the United States by manipulating its computerized funds transfer system. One of them, Vladimir L. Levin, was working in a Russian firm, and gained access over 40 times to Citibank's funds transfer system using a personal computer and stolen passwords and account identification numbers. Using a computer terminal in his employer's office in St Petersburg, he authorized transfers of funds from Citibank's head office in New Jersey to accounts which he and his co-conspirators held in California, Finland, Germany, the Netherlands, Switzerland, and Israel. After Levin was identified as a suspect, an arrest warrant was issued in a Federal Court in the United States. At the time, there was however no extradition treaty between Russia and the United States. Levin, however, made the mistake of visiting England to attend a computer exhibition and was arrested at Stansted Airport in England on 3 March, 1995. There was an extradition treaty between the United States and the United Kingdom but it was necessary to establish that the offences charged in the United States had a counterpart in the United Kingdom. This did not present problems as the offences had equivalents under the Computer Misuse Act of the United Kingdom. After protracted legal proceedings which went to the House of Lords,[9] Levin was extradited to stand trial before the Federal District Court in

[5] *Ibid.*

[6] Cited in M.A. Sussman, "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium", (1999) 9 *Duke J. of Comp. & Int'l L*. 451 at 460.

[35] Cited in J. Godoy, "Computers and International Criminal Law: High Tech Crimes and Criminals", (2000) 6 *New England International and Comparative Law Annual*, available online at http://www.nesl.edu/intljournal/vol6/godoy.pdf . Last visited on 18-06-15.

[1o5] Cited in R.G. Smith, "Investigating Cybercrime: Barriers and Solutions", paper presented at the Pacific Rim Fraud Conference, Sydney, 11th September, 2003.

[8] *Ibid.*

[9] *In re Levin*, unreported, judgment delivered on the 19th of June, 1997 available online at www.publications.parliament.uk/pa/ld/199798/ldjudgmt/jd970619/levin.htm. Last visited on 17-08-15.

New York's Southern District. On 24 February 1998, he pleaded guilty to conspiracy to defraud and was sentenced to thirty-six months' imprisonment and to pay Citibank US$240,015 in restitution.

The jurisdictional difficulties in the above cases and more triggered off legal scholars into searching for solution to the problem. Jurisdiction is fundamental and pivotal to administration of legal justice in general and of criminal justice in particular. It is, therefore, trite law that no matter how well conducted a proceeding was, lack of jurisdiction on the part of the trial court would bring to nullity the entire adjudicatory process. Jurisdiction itself is an issue of law. Yet, hardly are there uniform laws across jurisdictions. Even if the substantive laws are similar, the adjectival laws and enforcement procedures may differ. It is observed that situations are all the more complex when related to crimes in cyberspace which knows no boundaries. In what immediately follow, this study examines the various attempts made by jurists and courts with a view to tackling the problem of jurisdiction in cyberspace for the purpose of prosecution of suspects.

3. Theories of Jurisdiction in Cyberspace

3. 1. 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, therefore, two distinct actors are discernible: the uploader and the downloader[10].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. 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 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,[11] with a gambling site in cyberspace. For example, the U.S. Supreme Court some time ago declared the 'Communications Decency Act' (CDA) unconstitutional for overbreadth and vagueness on a facial challenge[12], yet 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.

[10] What is meant here is "one-to-many" Internet communications, rather than direct ("one-to-one") communication over the Internet, such as email. Suffice it to say now that these direct communications do not present the same conflict of law problems as general postings to the world.
[11] Interacting may involve considerably more than downloading, but it always involves the act of downloading.
[12] *Reno v. ACLU*, 117 S.Ct. 2329, 2346-48 (1997).

Two American cases demonstrate how this theory would be manifest. The *Schooner Exchange*[13] 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. Again, the *Cutting Case*[14] provides an example of how an uploader 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 incarcerated on criminal libel charges. The United States Secretary of State instructed the U.S. ambassador in Mexico to inform the Mexican government that 'the judicial tribunals of Mexico were not competent under the rules of international law to try a citizen of the United States for an offence committed and consummated in his own country, merely because the person offended happened to be a Mexican.'[15] As a general proposition, where uploading certain material is a crime, it is an offence 'committed and consummated' in the state where the uploader is located.

3.2. Extraterritoriality Rule

By this practice, states seek to exercise jurisdiction over uploaders (and to a lesser extent, downloaders) outside their own territorial boundaries. Minnesota in the United States 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.'[16]

Since the Attorney General's memorandum was issued, the Minnesota courts 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.[17] The opinion in *Minnesota v Granite Gate Resorts* (a case argued for the state by the very same A.G.), 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.'[18] While this result may eventually be overturned by federal legislation or case law defining due process,[19] the federal case from Missouri, *Maritz v Cybergold*, is more troubling. In *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.

---

[13] *The Schooner Exchange v McFaddon, 11 U.S*. (7 Cranch) 116 (1812).

[14] *See* Letter, Secretary of State to United States Ambassador to Mexico. Department of State, Washington, November 1, 1887 (reprinted in part in, J. Sweeney, *Op.cit.*, 90-93)

[15] *Ibid.*

[16] Memorandum of Minnesota Attorney General (July 18, 1995). Available at http://www.state.mn.us/ebranch/ag.. Last visited on 12-09-15.

[17] *See Maritz v Cybergold*, 947 F. Supp. 1328 (E.D. Mo. 1996); *Minnesota v. Granite Gate Resorts, Inc.*, 568 N.W.2d 715 (1997).

[18] *Granite Gate*, 658 N.W.2d at 718.

[19] Minnesota's long-arm statute permits courts to assert jurisdiction over defendants to the extent that federal constitutional requirements of due process allow. Minn. State, § 543.19 (1997).

Granted that Minnesota's concerns are no doubt sincere, yet hardly can the memorandum itself be. It is common knowledge that all information in cyberspace may be downloaded in Minnesota, which eventuality is always foreseeable. Minnesota's rule thus makes all of cyberspace subject to Minnesota law. If every state took this, 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.[20] Since anyone who puts up a webpage knows that it will be visible from Minnesota, 'downloadable' in Minnesota, 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.'[21] 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,[22] and that presumption is possibly stronger against state legislatures[23]. Indeed, most provisions of U.S. foreign relations law are designed to keep international issues in federal hands. Of course, treaties, for monist nations, are the 'supreme law of the land,' superior to any state law.[24] 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.[25]

A proper exegesis of the Minnesota's approach reveals several problems. First, Minnesota has ignored the presumption against extraterritoriality 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. Under the theory of international spaces, 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'[26] 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*

[20] Minn. State. Ann. § 609.025(3) (West 1987).
[21] Florida Attorney General, Formal Opinion: AG0 95-70 (Oct. 18, 1995).
[22] See *Alexander Murray v. Charming Betsy*, 6 U.S. 64, 118 (1804).
[23] *Guaranty Trust Co. of New York v. United States*, 304 U.S. 126, 143 (1938); *but see Nielsen v. Johnson*, 279 U.S. 47, 52 (1929).
[24] U.S. Const. art. VI, cl.2.
[25]Comity is the respect courts accord one another and the laws of other sovereigns. Like *forum non conveniens*, it is (in common law countries) a judge-made doctrine for declining jurisdiction. Civil law countries invoke comity more with statute than *sua sponte* court action. *See generally* B. Pearce, "The Comity Doctrine as a Barrier to Judicial Jurisdiction: A U.S.-E.U. Comparison*", 30 Stan J. Int'l L. 525 (1994).*
[26]*International Shoe Co. v Washington*, 326 U.S. 310, 316 (1945).

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, that is, without considering whether jurisdiction to prescribe existed or not. From an international law perspective, what Minnesota's court and its Attorney General have actually done is chosen to rely on 'effects' jurisdiction or '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 Second Restatement 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.[27]

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 also because the act of uploading *per se* 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 Nigerien shooting a Nigerian) 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.

3.3. Anti-territoriality Principle: 'The Law of the Server'

Another approach to jurisdiction in cyberspace is to treat the server where webpages are physically 'located' (that as, 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 in Ghana is subject to Nigerian law, for instance. 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

[27] U.S. Restatement (Second) of Foreign Relations, 1965 § 18.

uploader is in a foreign jurisdiction,[28] 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 theory.

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' 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 [29] 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 in South Africa, for instance, it is difficult to decide for jurisdictional purposes whether a Nigerian accessing it comes to South Africa or the webpage 'travels' to Nigeria. 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

[28] 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 (See Menthe, *op.cit.*, footnote no. 31).

[29] The term "gif" file refers to pictures saved in the Compuserve format.

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 bedlam.[30] Fourth, as it is often overlooked, such interactivity is complicated by randomness and anonymity. Byassee argues persuasively that territoriality should refer only to the 'physical components of the cyberspace community', who are the 'sender and recipient.'[31] 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 sets of laws apply to their actions. If territorialization of cyberspace is rejected in favour of the theory of the uploader and the downloader, then the broad form of the 'law of the server' must be rejected.

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, that is, 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. The rule of nationality in cyberspace means that Nigerian nationals and corporations cannot circumvent domestic law by uploading from foreign jurisdictions, assuring the Nigerian government a distinct slice of control over the cyberspace content contributed by its citizens.[32]

The theory of international spaces thus converts the 'law of the server' into the law of the sysop[33]. 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,

[30] 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.

[31] *See* W. 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).

[32] 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* B. Anderson, *Imagined Communities: Reflections on the Origin and Spread of Nationalism*, Macmillan, London, 1983, p. 25.

[33] 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.

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 favour of free speech on the Internet (a principle soundly upheld in *Reno*[34]), 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'[35] 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 the night time. 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.

3.4. Nationality Theory

For nationality to work as a principle in cyberspace, an appropriate analysis peculiar to cyberspace is required. No doubt, nationality principle is firmly entrenched in jurisdictional considerations in relation to the open sea, in outer space, or in Antarctica. The issue may not fit cyberspace. 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.' 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, that is, what carries nationality into cyberspace? 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. This has recently been referred to as the principle of personal sovereignty of the nation over its citizens.[36] 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 that put them there, or perhaps by the one who controls

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

[35]"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 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

[36] See *Smith v. United States,* 507 US 197, 205-206 (1993) (Per Stevens, J., dissenting).

them. This analysis is relatively easy to undertake with regard to webpages.[37] 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 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 or 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.[38] 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. Cyberspace just like Antarctica, outer space, the high seas, are four international spaces that share the unusual characteristic, for jurisdictional purposes, of the lack of any territorial jurisdiction. In these four places, it seems, according to proponents, that nationality is, and should 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 international may be the panacea. It is becoming imperative.

3.5. Sliding Scale Test (*The Zippo*) *versus* Effects Test

In the United States, there have been diverse attempts[39] to develop uniform principles of jurisdiction in cyberspace. Two principal models for testing jurisdiction are discernible. One is the '*Zippo* test,' after the case in which it was first articulated, *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*[40] The *Zippo* test bases jurisdiction over a non-resident website on the degree of interactivity between the website and the forum. Since mere accessibility of a non-resident's website from the forum is the least interactive, under *Zippo* a passive website is insufficient to establish specific jurisdiction. *Zippo* created a 'continuum,' or sliding scale, for measuring

[37] 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.

[38] *The* reader should keep in mind that none of these observations about the outer limits of jurisdiction touch on the subject of what a state may be constrained from regulating by its own constitution and laws.

[39] For instance, the American Bar Association's Jurisdiction in Cyberspace Project 2000; and The Hague Convention on Jurisdiction and Recognition and Enforcement of Foreign Judgements in Civil and Commercial Matters.

[40] *Zippo Mfg. Co. v. Zippo Dot Com, Inc* 952 F. Supp. 1119 (W.D. Pa. 1996). Pennsylvania federal district court generated the first overall analytical framework for testing specific personal jurisdiction based on the level of Internet activity.'

websites, which fall into one of three general categories: (1) passive, (2) interactive or (3) integral to the defendant's business. The 'passive' website is analogous to an advertisement in Time magazine; it posts information generally available to any viewer, who has no on-site means to respond to the site. Courts ordinarily would not be expected to exercise personal jurisdiction based solely on a passive Internet website, because to do so would not be consistent with traditional personal jurisdiction law. An 'integral' website is at the other end of the continuum: it is used actively by the operator to conduct transactions with persons in the forum state, receiving on- line orders and pushing confirmation or other messages directly to specific customers. In such cases, traditional analysis supports personal jurisdiction. The middle category is the 'interactive' website, which falls between passive and integral. It allows a forum-state viewer to communicate information back to the site, by toll- free telephone number, regular mail or even e- mail.

Under *Zippo*, exercise of jurisdiction in the 'interactive' context is determined by examining the level of interactivity and the commercial nature of the site. Because in *Zippo* a non-resident California defendant operated an integral website that had commercial contacts with some 3,000 Pennsylvania residents and Internet service providers, the court had no difficulty finding a high level of interactivity and hence jurisdiction. In *Cybersell, Inc. v. Cybersell, Inc.*[41], the Ninth Circuit, in sharp contrast to the Connecticut federal court in the *Inset* case, rejected the notion that a home page 'purposely avails' itself of the privilege of conducting activities within a jurisdiction merely because it can be accessed there. The plaintiff in *Cybersell* was an Arizona corporation that advertised its commercial services over the Internet. The defendant was a Florida corporation offering web page construction services over the Internet. The Arizona plaintiff alleged that the Florida trademark infringer should be subject to personal jurisdiction of the Federal court in Arizona because a website which advertises a product or service is necessarily intended for use on a worldwide basis. In finding an absence of jurisdiction, the Ninth Circuit used the *Zippo*-type analysis and called the defendant's website 'essentially passive.' It also concluded that the Florida defendant had conducted no commercial activity over the Internet in Arizona. Even though anyone could access defendant's home page and thereby learn about its services, the court found that this fact alone was not enough to find that the Florida defendant had deliberately directed its merchandising efforts toward Arizona residents. Accordingly, defendant's activities over the Internet were insufficient to establish 'purposeful availment.' In so ruling, the court observed that, if all that were needed for jurisdiction was access in the forum to an infringing web page, 'every complaint arising out of alleged trademark infringement on the Internet would automatically result in personal jurisdiction wherever the plaintiff's principal place of business is located,' *Cybersell*. The court also rejected application of the effects test. It saw the passive website as different from a publication with a large California audience. It also distinguished between the effects in the plaintiff's residence when the plaintiff is a corporation 'which does not suffer harm in a particular geographic location in the same sense that an individual does' and an intentional defamation of a specific, real individual and the infringement of a trademark owned by a corporation, *Cybersell.* After *Zippo* and *Cybersell*, courts became increasingly reluctant to grant jurisdiction merely on the basis of the number of people in the forum jurisdiction who can access a passive website, even where accessibility is accompanied by other means of communicating with the site operator or by a small amount of other contacts with the forum. Indeed, the Connecticut Superior Court, without even a reference to the Connecticut federal court's opinion in *Inset*, ruled in 2000 that specific jurisdiction could not be based on the mere accessibility within Connecticut of a website operated from Georgia. When the Connecticut

[41] *Cybersell, Inc. v. Cybersell, Inc* 130 F.3d 414 (9th Cir. 1997).

federal district again considered jurisdiction based on a website in 2001, it wholly disregarded its own opinion in *Inset*, stating that 'most courts follow the lead of . . . *Zippo On-Line Technologies v Perkin Elmer Corp*.[42]. After the Ninth Circuit's implied endorsement of the *Zippo* model in *Cybersell*, five other federal circuits elected to recognize or adopt that model. The Fifth Circuit did so in *Mink v. AAAA Devel. LLC*,[43] finding that a printable mail-in form, a toll- free call- in number and a posted e- mail address were not enough to impose specific jurisdiction in Texas over a Vermont website operator. Because orders were not taken through the website, it was deemed to be nothing more than a 'passive advertisement.' In the same year, the Tenth Circuit used the *Zippo* analysis in holding that a 'passive' website was insufficient for exercise of jurisdiction in Utah over a British bank, *Soma Medical Intern v Standard Chartered Bank*[44] , The sliding-scale nature of *Zippo* becomes vulnerable to subjective results when applied. Sometimes the question as to whether to place a site in the 'interactive' or 'integral' category may turn more on a court's perception than on real differences in the manner in which the user employs the Internet. For example, a judge in the Southern District of New York, while acknowledging that plaintiffs' allegations that defendants' mobile telephone and two-way e-mail services were used in New York to be 'factually unsupported,' nevertheless found the mere availability of the defendant's website in New York made it 'intuitively apparent' that defendant's services were used by New York residents, thereby establishing a basis for jurisdiction as an interactive site, *Cable News Network, L.P. v. GoSMS.com, Inc*.[45]. In effect, this was judicial transposition of a passive website into a highly interactive website.

In addition to *Zippo*, courts have been analyzing Internet jurisdiction issues under 'effects' test which is derived from the pre-Internet case of *Calder v Jones* [46].This test does not focus on the

[42]*Zippo On-Line Technologies v Perkin Elmer Corp*. 141 F.Supp. 2d 246 (D.Conn. 2001).
[43] *Mink v. AAAA Devel. LLC* 1909 F.3d 333 (5th Cir 1999).
[44]*Soma Medical Intern v. Standard Chartered Bank* 196 F.3d 1292 (10th Cir 1999).
[45] *Cable News Network, L.P. v. GoSMS.com, Inc*.2000 WL 1678039 (S.D.N.Y.).
[46] *Calder v Jones* 465 U.S. 783 (1984). What has come to be referred to as the effects test originated in a U.S. Supreme Court decision in the context of print media, *Calder v. Jones.* Florida residents who had essentially no physical contacts with California wrote and edited an article in the *National Enquirer* which defamed Jones, a well-known movie actress residing in California. The *Enquirer* had greater circulation in California than any other state, and the material in the article was based on California sources. The Supreme Court in a relatively brief opinion found jurisdiction, holding that California was "the focal point both of the story and the harm suffered." The Court in doing so felt compelled to distinguish one of its earlier decisions holding that "foreseeability" of an impact in the forum, standing alone, is not basis for specific personal jurisdiction. The Court held that the instant facts involved *more* than foresee ability. Instead, allegedly defamatory articles were published under circumstances sufficient to establish that the defendants' actions were "*aimed* at California": defendants knew their article would have a "potentially devastating impact" on the California plaintiff and that "the brunt of that injury" would be felt by her in California, hence the defendants could have reasonably foreseen being brought into court in California. Since the unanimous opinion by Justice Rehnquist in *Calder* contains minimal explication, it is important to focus on exactly how and why the Court arrived at its result. First, the case involved defamation, the gravamen of which is damage to a person's reputation in the community. The "community" is therefore a factor in defining the tort. Second, presumably because California is among jurisdictions that require malice as an element of libel when a public figure (such as television actress Jones) is involved, the *Calder* defendants were accused of acting "maliciously and with intent to injure, defame and disgrace" Jones and cause her "to suffer humiliation and emotional and physical distress." Third, the general rule in California is that everyone who takes a responsible role in a defamatory publication is liable. Fourth, the Rehnquist opinion placed great stress on a fact not mentioned by the California court: that the *National Enquirer's* largest circulation was in California, where 600,000 copies ("twice the level of the next highest state") were sold. Fifth, defendant Calder not only edited the article in its final form, but once it had been published, he refused to print a retraction. This unique blend of law and facts produced an understandable result. It is also worth noting that in finding jurisdiction at the state level, the California Court of Appeal had been obliged to distinguish a prior California Supreme Court case holding that merely causing of an effect in California is not a basis for jurisdiction, pointing out that the prior case was a contract action not involving an "intent to cause a tortuous effect within the state."

degree of interactivity between forum resident and non-forum defendant, but rather on the effects intentionally caused within the forum by a defendant's online conduct outside the forum. There is, however, a general consensus among cyber lawyers and jurists that the effects test marks the wave of the future in cyberspace jurisdiction issues, because it can produce 'greater certainty' of outcome in jurisdictional matters. While the effects test clearly supplies a useful frame of reference whenever personal jurisdiction is an issue, the *Zippo* test is still often used to define jurisdiction. Through mid-June 2002, 164 decisions of federal and state courts involving Internet jurisdiction had cited *Zippo*, with 46 of these occurring since the start of 2001.Yet, the courts are not embracing the effects test[47] as a panacea to the dilemma of determining jurisdiction, but rather a combination of both the *Zippo* and the effects test is being employed[48]. Oftentimes a court will begin its case analysis with the *Zippo* test but complete the jurisdictional determination using the effects test[49].

Early cases involving jurisdiction in cyberspace in the U.S. were marked not only by inconsistencies, but also by failure to appreciate the technological realities of the new medium. One example was a decision of the Connecticut federal court in *Inset Systems, Inc. v. Instruction Set, Inc*[50]. Inset Systems sued Instruction Set (ISI) in Connecticut (*Inset's* home) for trademark infringement, even though ISI had no assets in Connecticut and was not physically transacting business there. The federal district court determined that it had specific personal jurisdiction over ISI in Connecticut, basing its determination on ISI's use of a toll-free telephone number and the fact that there were at the time 10,000 Internet users in Connecticut, all of whom had the ability to access ISI's website. It found the advertising to be 'solicitation of a sufficiently repetitive nature to satisfy' the requirements of Connecticut's long-arm statute, which confers jurisdiction over foreign corporations on a claim arising out of any business in Connecticut, *Inset*. The court also held that the minimum contact test of the due process clause of the Fourteenth Amendment was satisfied, reasoning that defendant had purposefully 'availed' himself of the privilege of doing business in Connecticut in 'directing' advertising and its phone number to the state, simply because subscribers could access the website.

With respect, the decision of the court does not represent the correct position of the cyberspace reality. The *Inset* court failed to appreciate adequately that any website can be accessed worldwide by anyone at any time. Moreover, it failed to give weight to the lack of evidence that any Connecticut residents actually had accessed the site or made a toll-free call to ISI. Under the court's line of reasoning, any website would be subject to jurisdiction everywhere just by virtue of being on the Internet. The notion that a passive website triggers jurisdiction over an alleged trademark infringer when it is accessible from the forum was subsequently rejected by the Southern District of New York in *Bensusan Restaurant Corp. v. King*,[51] without citing *Inset* , and the Second Circuit affirmed. The website in Missouri offered tickets to a local jazz club, but none had ever been ordered by any resident of New York, where a famous jazz

[47]The effects test will likely have a growing role in e-commerce disputes, but experience so far suggests that:1)it tends to be more applicable to certain kinds of non-commercial disputes than to others,2) it can pose problems of subjectivity comparable to those that have arisen in the *Zippo* test, and 3) in certain kinds of e-commerce disputes, particularly where the defendant operates an online business engaged in transactions in the forum, the *Zippo* approach may be more applicable than the effects test (See J. A. Gladstone, *Determining Jurisdiction in Cyberspace: The "Zippo" Test or the "Effects" Test?* Available at http://proceedings.informingscience.org/IS2003Proceedings/docs/029Glads.pdf). Last visited on 15-10-15.

[48] *Ibid.*

[49] *Ibid.*

[50]*Inset Systems, Inc. v. Instruction Set, Inc* 937 F. Supp. 161 (D. Conn. 1996) (*Inset*).

[51] *Bensusan Restaurant Corp. v. King* 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd* 126 F.3d 25 (2d Cir. 1997).

club with the registered mark was located. The district court held that 'creating a site, like placing a product into the stream of commerce without more is not an act purposefully directed to the forum state.'In an early Sixth Circuit decision involving combined trademark and copyright claims, the Sixth Circuit found extensive contacts warranting jurisdiction. *Compuserve Inc. v. Patterson,*[52] involved a computer information and network service which sued a subscriber with whom it had entered into an agreement to register the subscriber's 'shareware' computer software for third parties to use and purchase on the Web. Plaintiff sought declaratory judgment that it had not infringed on the subscriber's common law trademarks or otherwise engaged in unfair competition. After the federal district court had dismissed for lack of personal jurisdiction, the Sixth Circuit reversed. It found specific jurisdiction based on the fact that the defendant had not only entered into a written contract with the plaintiff which provided for application of Ohio law, but had 'purposefully perpetuated the relationship' via repeated communications with plaintiff's system in Ohio and by using plaintiff to market his wares in Ohio and elsewhere through plaintiff's Internet system. Defendant also repeatedly sent his 'goods' electronically to plaintiff in Ohio for ultimate sale, and after deciding that the plaintiff's product infringed on his software, repeatedly sent messages to Ohio outlining his claim.

The first decisions involving the effects test in cyberspace were decided the same year as *Zippo*. In *Edias Software Intern. v. Basis Intern. Ltd.*[53] , the Arizona federal district court sustained jurisdiction over a New Mexico software distributor which had allegedly posted on its website and e- mailed to Arizona material defaming plaintiff. The court held the allegations that the materials were directed at Arizona and allegedly caused foreseeable harm to plaintiff was a basis for jurisdiction under *Calder*. The Northern District of Illinois invoked the Seventh Circuit's relaxed interpretation of *Calder* in a trademark case, *Bunn-O-Matic Corp. v. Bunn Coffee Service Inc.*[54] Without citing *Zippo* (which had been decided over two months earlier), the court found defendant's website 'passive,' since no orders could be placed on the site, no Illinois residents had entered the site's contest online, its toll free numbers were inaccessible to Illinois residents and defendant did not advertise, sell or ship into Illinois. However, relying on the effects the court found jurisdiction, 'although Bunn-O-Matic does business all over the country, it is reasonable to conclude that the injury of trademark infringement will be felt 'mainly' in Illinois,' *(Bunn-O-Matic.)*

The Ninth Circuit was the first federal appellate court to invoke the effects test in the online environment, thus declining to find jurisdiction. In *Cybersell, Inc. v. Cybersell, Inc.*[55]. an Arizona plaintiff provided Internet marketing services through its website under the registered service mark 'Cybersell.' The Florida defendant provided business consulting services through its website under exactly the same name. At the time defendant chose the name 'Cybersell,' plaintiff's website was not operational, nor had the Patent and Trademark Office yet granted plaintiff's application for its service mark. Plaintiff instituted suit in the District of Arizona, alleging, *inter alia*, trademark infringement. The Ninth Circuit found no jurisdiction under the *Zippo* type continuum. It also determined there was no jurisdiction under the effects test, because defendant's website was 'not aimed intentionally at Arizona knowing that harm was likely to be caused there,' *Cybersell*. Thus, the mere act of registering another's trademark as a domain name and posting an infringing but passive site on the Internet should not, without more, subject a non-resident to personal jurisdiction in the forum state. The Ninth Circuit found

[52]*Compuserve Inc. v. Patterson, 89 F.3d 1257 (6th Cir 1996).*
[53]*Edias Software Intern. v. Basis Intern. Ltd* 947 F. Supp. 413 (D. Ariz. 1996).
[54] *Bunn-O-Matic Corp. v. Bunn Coffee Service Inc* 46 U.S.P.Q.2d 1375 (N.D. Ill. 1998) *(Bunn-O-Matic.)*
[55]*Cybersell, Inc. v. Cybersell, Inc* 130 F.3d 414 (9th Cir.1997) ("*Cybersell*")

the 'something more' that was lacking in *Cybersell* in a later case involving an Illinois resident who operated a 'cybersquatting' scheme.[56] The Illinois defendant registered exclusive Internet domain names that contained registered trademarks belonging to others. He demanded fees from Panavision, a well-known California resident, as his price for relinquishing rights to domain names that corresponded to Panavision's existing trademark registrations. The 'something more' consisted of defendant's efforts to 'extort' money from a plaintiff whose business and trademarks were particularly well-known in California. The court thus viewed defendant in Illinois as having committed a tort which 'is aimed at or has an effect in the forum state.' The result in this case demonstrates a positive outcome using the effects test. It was earlier suggested that the utility of the effects test may be greater with certain causes of action than with others.

4. Evaluation

The lesson learnt from the above study is that when one country's laws criminalize certain activities on computers and another country's laws do not, cooperation in fighting a crime and prosecuting the perpetrator may not be possible.[57] That is, when a criminal weaves his communications through three, four, or five countries before reaching his intended victims, inadequate laws in just one of those countries can, in effect, shield that criminal from law enforcement around the world.[58] While the Internet may be borderless for criminals, law enforcement agencies must respect the sovereignty of other nations. In a networked world, it has become increasingly easy for criminals to escape conviction by acting from another country where a conduct is either not criminalized or not prosecuted.[59] In spite of the staccato of theories of jurisdiction in cyberspace, it is still true that the emergence of cyber criminality in its networked and interconnected nature makes it imperative to achieve transnational consistency in criminal laws.[60] One way to do this would be to create a single code of law governing the issue of cybercrime. One giant step in this direction is the Council of Europe Convention on Cybercrime. Yet, there is a dire need for a global multilateral treaty for combating cyber criminality.

[56] *Panavision Int'l, L.P. v. Toeppen* 144 F.3d 1316 (9th Cir. 1998) (*Panavision*).
[57] C. Magnin, *The Council of Cybercrime Convention on Cybercrime: An Efficient Tool to Fight Crime in Cyberspace*, LL.M. Dissertation, Santa Clara University, 2011, pp.80-81. Available online at www.magnin.org. Last visited on 05-09-11.
[58] *Ibid*.
[59] *Ibid*.
[60] M. D. Goodman & S.W. Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace", (2002) *U.C.L.A. Journal of Law & Technology* 3 available at http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php. Last visited on 12-05-10.