LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +918255090897 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

ASCERTAINING LIABILITY IN THE REALM OF CYBERSPACE*

Abstract

The transactions in the cyber world are not geographically based as the Internet greatly curtails the significance of physical location of the parties. The rapid advancements in science have exposed the majority of the world's population to the Internet and it's far reaching consequences. Moreover, the Internet hinders the balance of power between the consumer and distributor, because consumers now have access to information and sophisticated analytical tools. This affects the basis on which courts have enforced choices of law and forums. The crux of the problem is that an online corporation can be called to any court and every website would have the unenviable task to conform to laws of different jurisdictions. Therefore, any matter regarding the jurisdiction of cyberspace requires courts to consider a plethora of factors before hearing the matter. The precursors of jurisdiction to prescribe, adjudicate and enforce must exist. Information over the internet passes through a myriad of networks, some intertwined with other networks and computers, some not. This particular grey area of the law over the issue of jurisdiction in cyberspace has given rise to a number of cases of online harassment and cyber bullying. The authors seek to provide a twofold view in this paper. Firstly, the issue of jurisdiction in cyberspace will be analysed by delving into the realms of international law and freedom of speech in the cases of Yahoo and Cybersell. Secondly, the paper also aims to throw light on the abuse doled out across online gaming platforms. An issue which is as serious as cyber bullying and cyber stalking, it chiefly goes under the radar. Comparisons of various gaming companies' policies on this issue will be done to clearly understand the legal stand on the same. Finally, the authors aim to put forth a uniform standard of dealing with these questions and bring to the fore the far-reaching impact of cybercrimes and the gravity of its impact on society.

* **Mr. Aditya. R, 3rd year, B.B.A. LL.B., Symbiosis Law School, NOIDA,**

1) Introduction

In today's era, where the internet has become an indispensable part of our lives and majority of communications and transactions happen over the instantaneous use of the internet, a plethora of activities take place in cyberspace. In the initial days when the World Wide Web was introduced only governments, professionals and academicians had access to it, but with the advancement in technology, the use of the internet has become accessible to billions of people around the globe. This very real time nature of Internet communication not only offers new opportunities for the expression of ideas[1], but also allows for the rapid dissemination and accumulation of information.[2]

Everyday users become easy targets of cyber criminals and get exploited on the internet. Cyber attacks take place on various levels. Firstly, it can take place through a deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks. Secondly, cyber exploitation or cyber espionage takes place by the penetration of adversary computers and networks to obtain information for intelligence purposes; this is espionage, not a destructive activity.[3] Therefore, cyber attacks not only take place against an individual but even against banks, large corporations as well as nations and pose a major threat to the society on the whole. Cyber crimes also include cyber bullying, cyber stalking, and cyber abuse that happen over social media websites, online gaming platforms, and even on mobile phones. These crimes target individuals of all age groups from children to adults.

To resolve the problems that arise in the cyberspace domain, cyber security has to be maintained for the interest and protection of the users. The cyberspace has for quite some time been comprehended as a boundless, non-material space, where the gravitational laws do not have any significant bearing and where of course everything without exception is conceivable.[4]

Since the cyberspace cannot be considered as a physical entity, the question that arises is who has jurisdiction over this space? But in the context of cyberspace, the concept of territorial jurisdiction assumes importance with respect to the challenges posed by the internet.

---

[1]Steven R. Salbu, *Who Should Govern the Internet? Monitoring and Supporting a New Frontier*, 11 Harv. J.L. & Tech. 429, 434 (1998).
[2]Julia A. Gladstone, *Survey of the Law of Cyberspace: Introduction*, 54 The Business Lawyer, 347 (1998)
[3]Cyber Attacks, *Available at: https://www.dsci.in/taxonomypage/242 (last visited on 23.04.17)*
[4] Charles Ess & Ruth Hagengruber, *The Computational Turn: Past, Presents, Futures*, International Association of Computing and Philosophy (2011).

2) Rule of Law & Jurisdiction in Cyberspace

Jurisdiction to prescribe laws and adjudicate disputes historically has been based on territorial principles: if a country found a person within its territory, it exercised jurisdiction over that person. The Internet greatly diminishes the significance of physical location of the parties, because transactions in cyberspace are not geographically based. While general jurisdiction has not been based on any reported decision solely upon the operation of a website, some courts have used only little additional activity as a crutch to support a general jurisdiction finding.

International law limits a country's authority to exercise jurisdiction in cases that involve interests or activities of non-residents. First, there must exist "jurisdiction to prescribe." If jurisdiction to prescribe exists, "jurisdiction to adjudicate" and, "jurisdiction to enforce" will be examined.[5]"Jurisdiction to prescribe" means that the substantive laws of the forum country are applicable to the particular persons and circumstances. Simply stated, a country has jurisdiction to prescribe law with respect to:

1) conduct that, wholly or in substantial part, takes place within its territory;

2) the status of persons, or interests in things, present within its territory;

3) conduct outside its territory that has or is intended to have substantial effect within its territory;

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

5) certain conduct outside its territory by persons who are not its nationals that is directed against the security of the country or against a limited class of other national interests.[6]

On the other hand, in the United States, the Due Process clause of the Constitution's Fourteenth Amendment sets the outermost limits of personal jurisdiction. If a party has substantial systematic and continuous contacts with the forum, a court may exercise jurisdiction over a party for any dispute, even one arising out of conduct unrelated to the forum. This is known as general jurisdiction.[7] For example, a corporation or person can always be sued in its state of residence or citizenship or its principal place of business, regardless of whether or not the

[5] Restatement (3rd) Of the Foreign Relations Law Of The U.S., Sec. 401,
[6] Id. Sec. 402.
[7] U.S. Constitution., Amendment XIV.

claim arose there. If a party is not present in the state or does not have systematic and continuous contacts with the state, courts may exercise jurisdiction over a party for causes of action arising out of his contacts with the state, or arising out of activities taking place outside the state expressly intended to cause an effect within the state. This "effects" test is described from the American Law Institute's Restatement (Second) of Conflict of Laws (1971), which provides: "A state has power to exercise judicial jurisdiction over an individual who causes effects in the state by an act done elsewhere with respect to any cause of action arising from these effects unless the nature of the effects and of the individual's relationship to the state make the exercise of such jurisdiction unreasonable."[8]

What is applicable to international transactions involving the internet, could well apply to domestic transactions as well. The law as developed in the USA has had to reckon with both situations, i.e., internet transactions across countries and those across states. The enforcement of issues would of course be more complex when it comes to international transactions. However, the principles applied by courts to assert or negate jurisdiction in either instance have remained more or less similar.[9]

2.1) Heil Yahoo!

The difficulties faced by courts in dealing with this new medium are acutely exemplified by a decision of a French trial court. Culminating a series of earlier rulings by the same court, it ordered Yahoo! Inc. to put filtering systems in its U.S. website so as to prevent access by French residents to portions of the Yahoo! Inc. auction site on which persons offer to sell WW II memorabilia containing Nazi symbols.[10] In its initial ruling (May 22, 2000) the court had held that the U.S. website for Yahoo! Inc. was subject to French jurisdiction simply because it could be accessed from France.[11] Under doctrines which have become prevalent in most judicial interpretations in the U.S. and elsewhere, France could not have jurisdiction over Yahoo! Inc.'s auction website: the site is not located in France, is not targeted at France and, indeed, offers only a venue in which persons other than Yahoo! Inc. offer goods for sale. To cap the matter, Yahoo!

[8]Betsy Rosenblatt, *Principles of Jurisdiction, Available at: https://cyber.harvard.edu/property99/domain/Betsy.html (*Last visited:13.03.17)
[9]Justice S. Muralidhar, *Jurisdiction Issues in Cyber Space*, 6 IJLT 2 (2010)
[10]Ordonne du 20 Novembre 2000, VEJF and LICRA v. Yahoo! Inc. and Yahoo France (Tribunal de Grand Instance de Paris). The French judge ruled that Yahoo! must put a three-part system in place that includes filtering by IP address, the blocking of 20 keywords and self-identification of geographic location. The system follows the recommendations of an expert panel appointed by the court to investigate such technologies, which revealed its findings earlier this month. Yahoo! was given three months to put the system in place, after which time the company would be subject to a fine of $13,000 a day if the system has not been implemented.
[11]*Ibid*.

Inc. has a subsidiary resident in France which complies with the French law forbidding sale of Nazi-related goods on its French website, namely Yahoo.fr.[12]

The uncharacteristic French decision, unless reversed on appeal or uniformly rejected by other French courts could undermine the harmony and predictability of jurisdictional questions in cyberspace. Such harmony and predictability is crucial to the flowering of E-Commerce. As stated in the E.U. Commission's October 2000 proposal, "differences between national rules governing jurisdiction and recognition of judgments hamper the sound operation of the internal [E.U.] market."[13]

Yahoo! and free speech advocates claim that the case could set a dangerous precedent by granting one country the right to reach across borders and impose its laws on web sites based in other nations. Free speech advocates claim that the French approach would lead to a lowest common denominator world where the most restrictive rules of any country would govern all speech on the Internet. The French court's ruling highlights the difficulty in developing an international Internet legal code for cyberspace, given nations' differing policy imperatives.[14]Yahoo! had fought the case primarily on the grounds that its English-language Yahoo.com services are U.S.-governed and that auctions of Nazi material cannot be barred because of U.S. constitutional rights to freedom of speech. Yahoo's French-language portal Yahoo.fr does not host such auctions, but French surfers, like all others, can switch over to Yahoo.com with a click of the mouse. Yahoo! also argued that there was no fail-safe way to identify French surfers and block access. However, three web security experts told the French court that a filtering system could work by testing the Internet Service Provider address of web surfers as well as the keywords they used. Such a system would work for up to 90% of users.[15]

2.2) The Curious Case of Cybersell

[12] Marc H. Greenberg, *A Return To Lilliput: The Licra V. Yahoo! Case And The Regulation Of Online Content In The World Market,'* 18 (11), Berk.Tech.L.J. 91(2003).
[13] Commission of the European Communities, Amended Proposal for a Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters. (Oct. 26, 2000)
[14] Elissa A. Okoniewski, *Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet,'* 18(1), A.U. Int'l L.R. 56-89(2002).
[15] Christine Duh, *Yahoo Inc, vs. LICRA'* 17(1), Berk.Tech.L.J. 117-129 (2002).

The first decision by a federal court of appeal involving specific jurisdiction in cyberspace was Cybersell, Inc. v. Cybersell, Inc.[16]Here, the Ninth Circuit, in contrast to the Connecticut federal court in the Inset case and the French trial court in the Yahoo! Inc. 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.[17] In Cybersell, the plaintiff 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 allege 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.

The court articulated a three-part test for determining whether a district court may exercise specific jurisdiction over a non-resident defendant:

"(1) The non-resident defendant must do some act or consummate some transactions with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections [;] (2) the claim must be one which arises out of or results from the defendant's forum-related activities [; and] (3) exercise of jurisdiction must be reasonable."[18]

Cybersell AZ argued that the test was met because trademark infringement occurs when the passing off of the mark occurs, which happened when the name "Cybersell" was used on the Internet in connection with advertising. Cybersell FL contended that a party should not be subject to nationwide, or perhaps worldwide, jurisdiction simply for using the Internet. The Ninth Circuit further explained that "purposeful availment" is satisfied if the defendant has taken deliberate action within the forum state or if he has created continuing obligations to forum residents. It is not required that the defendant be physically present within, or have physical contacts with, the forum, provided that his efforts are purposefully directed toward forum residents.[19]

[16]130 F.3d 414 (9th Cir. 1997)
[17] David R. Johnson and David Post, *'Law and Borders: The Rise of Law in Cyberspace,'* 48 (5), Stan.L.R. 87 (1996),
[18]*Supra* note 7.
[19] Tu Phan, *Cybersell, Inc. v. Cybersell, Inc.'* 14 (1), Berk. Tech. L. J. 52-70 (1999).

> Cybersell FL conducted no commercial activity over the Internet in Arizona. Cybersell FL had an essentially passive home page on the web, using the name "Cybersell", which Cybersell AZ was in the process of registering as a federal service mark. There is no question that anyone, anywhere could access that home page and thereby learn about the services offered, but the court could not see how, from that fact alone, it could be inferred that Cybersell FL deliberately directed its merchandising efforts toward Arizona residents. Cybersell FL did nothing to encourage people in Arizona to access its site, and there is no evidence that any part of its business was sought or achieved in Arizona. No Arizona resident except for Cybersell AZ "hit" Cybersell FL's web site.[20] Cybersell FL entered into no contracts in Arizona, made no sales in Arizona, earned no income from Arizona and sent no messages over the Internet to Arizona. Cybersell FL did not do any act or consummate any transaction or perform any act by which it purposefully availed itself of the privilege of conducting services in Arizona, thereby invoking the benefits and protections of Arizona law.[21]

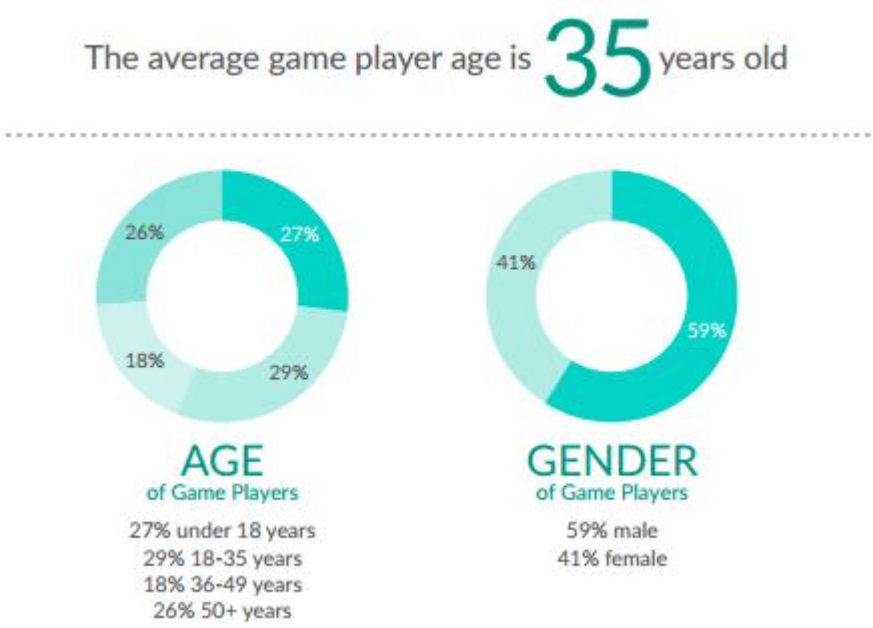
3) Problems Galore in Gaming

Online anonymity is important to free speech and privacy, just as anonymity and anonymous speech have been used for thousands of years in society to bring to the fore instances of human rights violations by various governments. Although anonymity has extremely important benefits to human rights, anonymity is often tied with cybercrimes or it is claimed that anonymity would allow criminals to use the Internet without the possibility of detection.[22] Internet-based activities should be treated consistently with physical world activities and in a technologically neutral way to further important societal goals of achieving integrity and instilling accountability in every citizen. Although the need for anonymity for the legitimate needs has been recognised, it has been described as "the proverbial double-edged sword" since "they add new complexities to identifying online lawbreakers" apart from protecting privacy.[23]

This leads us to the raging issue of abuse doled out across online gaming platforms and the murkiness of the issue of jurisdiction surrounding this area. Sadly, this is an issue which tends to go under the radar due to the misperceived notion that gaming is a juvenile pursuit. The

[20] Michael J. Weber, *'Jurisdictional Issues in Cyberspace,'* 36 (3), TILJ 245(2001).
[21] *Ibid.*
[22] Michael Whine, *Islamists Organisations on the Internet,* 11 (1), Terrorism & Political Violence 67-80 (1999).
[23] Yaman Akdeniz, *Anonymity, Democracy & Cyberspace,* 69(1), Social Research: Privacy in Post-Communist Europe 124 (2002).

Entertainment Software Association (ESA)[24] states that more adults between the ages of 18 and 49 are playing video games than adolescents. The increase in the popularity of online games and their ease of access has invoked scrutiny from parents and legislators as there is unadulterated communication amongst players from all across the globe. [25] The figure below shows the actual age of gamers. A figure which is alarmingly deviating from the notion that videogames are only for kids:[26]



Online gamers have a reputation for hostility. In a largely consequence-free environment inhabited mostly by anonymous and competitive young men, the antics can be downright nasty. Players harass one another for not performing well and can do innumerable things to intentionally ruin the experience for others, a practice that gamers refer to as griefing.[27] Racist, sexist and homophobic language is rampant; aggressors often threaten violence or urge a player to commit suicide; and from time to time, the vitriol spills beyond the confines of the game. In the notorious 'Gamergate' controversy that erupted in late 2014, several women involved in the

[24] The Entertainment Software Association (ESA) conducts business and consumer research, and provides analysis and advocacy on issues like global content protection, intellectual property, technology, e-commerce and the First Amendment in support of interactive software publishers. ESA represents the video game industry's interests on federal and state levels.
[25] Entertainment Software Association, Report on Sales, Demographic and Usage Data About the Computer and Videogame Industry (2016).
[26] *Ibid.*
[27] Sal Humphreys, *Griefing, Massacres, Discrimination, and Art: The Limits of Overlapping Rule Sets in Online Games*, 2 (2), UC Irvine L.R. 80-91(2012).

gaming industry were subjected to a campaign of harassment, including invasions of privacy and threats of death and rape.[28]

The Xbox Live Code of Conduct does not mention any harassment other than "severe racial remarks" as basis for permanent suspension, so it sounds to me like the "lifetime ban" and "zero tolerance" approach mentioned in the original interview were misrepresented, at least in terms of official XBL policy.[29] A lot of Xbox players have been calling for improvement for a long time, and there are many gamers (male and female) who find the environment so toxic that they avoid multiplayer entirely. If players are choosing to ignore an entire feature of a game because certain individuals are making the experience unpleasant to such an extent, it is time to take the issue more seriously.[30]

Sony Entertainment's EULA (End User License Agreement) lists a plethora of activities players cannot do on the PlayStation Network: "You may not take any action, or upload, post, stream, or otherwise transmit any content, language, images or sounds in any forum, communication, public profile, or other publicly viewable areas or in the creation of any [username] that [Sony and its affiliates] find[s] offensive, hateful, or vulgar. This includes any content or communication that SNEI or its affiliates deem racially, ethnically, religiously or sexually offensive, libellous, defaming, threatening, bullying or stalking."[31]

It would be an instance of redundancy to delve into the terms of use of other gaming giants. This is because if one were to superimpose the policies of these companies, they aspire to paint a picture wherein they seem to have complete control over online proceedings. But all the interactions among the users are unfiltered, rendering the policies useless.

The futility of having such policies in place can be explained by the following bifurcation, firstly, what can be considered "offensive content" can be debated ad infinitum in a courtroom, costing companies' money. Second, staffing shortages lead to prioritization, and actively policing user content usually ends up at the bottom of priority lists, as it's a problem without a concrete deadline. These two situations combined to form the user policing system used by nearly all of the aforementioned services: It's up to players to notify company staff that something is amiss.

---

[28] Caitlin Dewey, *The only guide to Gamergate you will ever need to read*, The Washington Post, October 14, 2014.

[29] Microsoft Code of Conduct for Xbox Live, *Available at* http://www.xbox.com/en-IN/legal/codeofconduct, *(last accessed on 13/3/2017).*

[30] Jason Moore, Ibrahim Baggili, Andrew Marrington and Armindo Rodrigues, *Preliminary Forensic Analysis of the Xbox One,* 11 (1), The International Journal of Digital Forensics & Incident Response (2014).

[31] Sony Terms of Service & User Agreement, *Available at* http://legaldoc.dl.playstation.net/ps3-eula/psn/u/u_tosua_en.html *(last accessed on 13/03/2017.)*

4) Existing Legal Framework

The Convention on Cybercrime at Budapest was the first ever-international treaty on criminal offences committed against or with the help of computer networks such as the Internet. The Convention deals with offences related to infringement of copyright, computer-related fraud, child pornography and offences connected with network security. It also covers a series of procedural powers such as searches of, and interception of material on computer networks. Its main aim is to pursue "a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international co-operation."[32]

The United Nations in July 2010 organised a meeting where government cyber-security specialists from fifteen countries (including major cyber-powers like the United States, China, and Russia) submitted a set of recommendations to the U.N. Secretary-General as "an initial step towards building the international framework for security and stability that these new technologies require."

The recommendations called for: -

1) Further dialogue among States;

2) Confidence-building, stability and risk reduction measures including exchanges of national views on the use of [information and communication technologies] in conflict;

3) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;

4) Identification of measures to support capacity-building in less developed countries; and

5) Finding possibilities to elaborate common terms and definitions.[33]

The role of the United Nations at present with respect to Cyber Security is quite limited and vague, these recommendations suggest a possibility of multilateral treaties in the near future.

[32] Council of Europe: Budapest Convention on Cybercrime (November, 2001).
[33]Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 4, U.N. Doc. A/65/201

Examining the current existing framework, the clear conclusion is that a new, comprehensive legal framework is needed to cement the position of courts with respect to issues of jurisdiction.

5) Suggestions

Based on the analysis of extensive secondary material conducted, the following points can be taken into consideration hereinafter by courts while determining who is really liable in under the jurisdiction of cyberspace:

1) Firstly, the developers in the gaming industry may be permitted to designate any law that has a substantial connection to the online interactions. The problem is that the consumer may not know or be able reasonably to determine his rights under such law. This could create apprehension on the part of the consumer and may hamper the growth of the gaming industry. For example, the developer can club people of the same age group together during online gaming, so that people below the age of 18 are not exposed to online abuse and harassment by adults.

2) Secondly, the contract can specify the law that will apply to the transaction but would not trump mandatory consumer protection rules. This creates confusion and increases the cost of compliance because the merchant is required to be familiar with the mandatory rules of each jurisdiction. Under such a system, a party would still be subject to jurisdiction in its home state or nation, but not in a foreign jurisdiction unless the party sought out an audience in that foreign jurisdiction. Such a system would put the burden on state and local authorities to prevent the viewing of illegal material and to focus on laws regarding the use of illegal material, rather than laws the provision of such material.

3) Finally, the most conducive alternative found for determining the jurisdiction in cyberspace was the harmonisation of natural consumer protection laws. This would create a lower cost mechanism, similar to the model rules enjoyed by other areas of uniform law. Merchants would not have to learn the law of each jurisdiction and consumers would know their rights irrespective of choice of law. Although harmonisation is a monumental task, this is the only present low cost solution.

6) Conclusion

The law hasn't been updated to reflect the realities of the internet. Formal mechanisms and agreements will help promote the general welfare of citizen's dependent on the Internet and computer systems. In formal co-operation mechanisms among services, software providers also can provide powerful means of response. It is in the realm of law enforcement and diplomacy, however, where formality can enable the protection of cyber safety. Apart from defence strategies that are adopted against abusive practices, multilateral treaties can create a basis for improved electronic commerce and an increasing sense of safety, or at least protection, in the online environment.[34]

If the current legal system is to maintain effective and fair control over the Internet, courts all over the world must make a clear move toward a new test for jurisdiction, and a consistent test for resolving choice of law disputes. If courts could agree to exercise jurisdiction based on an effects test like done by the United State with a much stronger element of purposefully availing, than that which exists in the current system, the current style of legal governance might be able to serve the Internet in an effective and consistent way, without the excessive and unpredictable elements that it currently suffers from.[35] For the purposes of fairness, mere awareness that a site could be accessed at a location would not be enough to trigger jurisdiction; rather, in order to be subjected to jurisdiction in a place other than his domicile or its primary place of business, a party would have to display intent to reach the audience in that location through advertising or special targeting subject matter, or a positive awareness of an audience's locations by way of interactions involving the exchange of information about real space location.[36] Under such a system, a party would still be subject to jurisdiction in its home state or nation, but not in a foreign jurisdiction unless the party sought out an audience in that foreign jurisdiction. Such a system would put the burden on state and local authorities to prevent the viewing of illegal material and to focus on laws regarding the use of illegal material, rather than laws the provision of such material.

[34]Vinton G. Cerf, *"Safety in Cyberspace"* 140 MIT Press 68 (2011)
[35]*Supra* note 7
[36]*Ibid*