5.1 CONCLUSION

The present research is divided into four main chapters. In this chapter the researcher has summarized the finding of all four chapters. Chapter no. I is ‘Introduction’, the research has introduced the research problem and stated the objectives, research questions, significance of research, methodology, sources of data, scope, limitations of research and scheme of chapterisation. As discussed in chapter no. I, on cyberspace, the accused can infringe the copyrights of other without disclosing his exact identity. The activities on cyberspace are not restricted by any territorial boundaries. The cyberspace is de-territorial in nature whereas the laws of nations preventing copyright infringement are territorial. The sovereign nations are free to enact, implement and give effect to their laws. The power to enact, apply and implement laws (criminal and civil) is considered as a sovereign power of the state. The customary international law does not allow interference in a sovereign state by any other (foreign) entity or state. It means the state is free to give extra-territorial effect to their laws but it shall not interfere in the sovereignty of others. De-territorial nature of cyberspace and territorial nature of law have posed a number of problems before sovereign nations and international law. The problems posed by cyberspace are addressed in chapter no. II, III and IV of the research.

Chapter no –II is on “Problem of jurisdiction in cyberspace and its impact on international and domestic laws.” In this chapter the author has discussed, the concept of jurisdiction, types of jurisdiction and problem of jurisdiction in dealing with cyberspace. The chapter also contained critical analysis of various principles of International Law and its applicability to cyberspace. Further, the author has deliberated upon laws and case laws from EU, US and India on jurisdiction in cyberspace. Summary of the findings on chapter no. II is as follows:

Problem of Jurisdiction

On research question 1 i.e. “Are established principles and doctrines of international law on jurisdiction applicable to the cyberspace?” the research after analysis of
existing data concluded that the existing principles of international law on jurisdiction are not applicable to the cyberspace. The findings on research question 1 are as follows:

The international community has developed and applied various principles and doctrines of jurisdiction to resolve the problem of jurisdiction. In majority of cases, the customary international law was working effectively to resolve problems of jurisdiction in pre-cyber era. In present era, number and nature of extra-territorial cyber crimes, including copyright infringement is totally different as compared to pre-cyberspace era. Now, because of multiple activities on cyberspace, nature of cyberspace and opportunity of conducting offences with the help of internet, the number of offences has increased multi-fold. The customary principles of international law are not able to resolve the problem of jurisdiction in cyberspace because of the peculiar nature of the internet. The activities of an accused may have an impact on different countries at a time. For instance, if the act has effect on 20 or more countries at a time, all the countries may not be able to take cognizance.\textsuperscript{440} In this scenario, the country having possession of the accused or movable or immovable property of the accused can take appropriate action. Other countries (without possession of the person or property) may not be able to provide any remedy to their nationals (victims). The existing principles and doctrines of international law do not recognize the need to share the property of the offender in instances of multi-territorial cyber offices or copyright infringements on cyberspace. At present, there is no international Treaty or Convention to compensate loss in proportion, if an act of the person (individual or corporation) is affecting the nationals of multiple nations, particularly when the value of the property of offender is less than actual loss caused. The application of traditional principles of international law on jurisdiction to cyberspace is summaries as follows:

The Traditional Principles and their Application to Cyberspace
The traditional principles of jurisdiction cannot resolve the problem of the jurisdiction in cyberspace. The traditional principles and doctrines of international law on

\textsuperscript{440} As discussed in chapter no. 2.3 there are many examples in which victims from 20 or more countries were involved.
jurisdiction are developed by keeping in mind the principle of territorial sovereignty. As discussed earlier, the cyberspace is de-territorial or borderless space, an offence in cyberspace can be committed by any person from anywhere. The offence may be conducted against multiple countries at a time. Therefore, territorial principle, nationality principle, effect doctrine, protective or security jurisdiction and universal jurisdiction cannot be used as an effective tool to resolve the problem jurisdiction in cyberspace.

The territorial principle cannot be a complete solution to deal with copyright infringement in cyberspace because the activities in cyberspace are not subject to any territorial limits. According to territorial principle the law should govern the activities happening in the territory of a sovereign state. The copyright infringement in cyberspace cannot be limited to territorial boundaries. Further, this principle cannot be used in order to pay compensation if victims are from multiple countries. Therefore, the territorial principle on jurisdiction cannot be a complete solution to resolve the problem of multiple jurisdictions in cyberspace.

The nationality principle (including passive and active nationality principles) on jurisdiction cannot be a complete solution to the problem of jurisdiction in cyberspace. Nationality principle can be used to protect or punish the nationals by a country. The nationality principle cannot be an effective solution to resolve problem of multiple jurisdictions in cyberspace. It also cannot be used to compensate the victims from multiple nations in cases of online copyright infringement.

The ‘effect doctrine’ may be used as a tool to resolve the problem of jurisdiction in cyberspace if the offence is against one country. In instances of copyright infringement against multiple countries, it cannot be used as an effective solution to the problem of jurisdiction. The multiple countries cannot take cognizance and punished the culprit according to ‘effect doctrine’ or there is no existing mechanism to pay compensation to the victims of multiple countries.

---

441 For a detailed explanation on principles of international law on jurisdiction refer chapter no. 2.2.1.1.
Protective or security jurisdiction may be useful in exceptional cases only. As discussed above, in chapter no. II, the protective or security jurisdiction cannot be claimed in every ordinary offence. It may be claimed when conduct abroad threatens the security, integrity or the proper functioning of the sovereign state. In instances of attack on the critical infrastructure or websites of the sovereign state including attacks upon the websites of the military or armed forces, the protective or security jurisdiction can be claimed. It means, in instances of online copyright infringements, the sovereign states cannot claim a jurisdiction under protective or security principle of international law.

The customary principle of the universal jurisdiction cannot be an effective remedy for copyright infringement in cyberspace. As analyzed earlier, in chapter no. II, the universal jurisdiction can be claimed over the crimes considered to be of concern to all states, i.e. *erga omnes* obligations owed to the international community or for violation of peremptory norms of international law (i.e. *jus cogens*). Ordinary cyber crimes, including online copyright infringements are not considered as *erga omnes* or violation of peremptory norms of international law (i.e. *jus cogens*). Therefore, according to customary international law, state practices, *opinion juris* or existing Conventions, the State cannot claim jurisdiction for ordinary cyber crimes or online copyright infringements under the principle of universal jurisdiction.

Therefore, findings of the author on research question 1 i.e. “Are established principles and doctrines of international law on jurisdiction applicable to the cyberspace?” are that existing principles and doctrines cannot be a complete solution to resolve the problem of jurisdiction in cyberspace.

Research question 2 i.e. “Do conflicting laws and self-centric judgments on the issue of jurisdiction create chaos in dealing with problems posed by cyberspace?” is analyzed in chapter no. II of the research. The findings on the research question 2 is that conflicting laws and self-centric judgments on the issue of jurisdiction in
cyberspace has created chaos, the judiciary has not laid down a universally acceptable solution to the said issue. Findings on research question 2 are as follows:

Analysis of Judgments of the Courts dealing with Jurisdiction in cyberspace

The role played by the courts to resolve the problem of jurisdiction in cyberspace is not satisfactory. The courts have laid down various principles and doctrines in order to justify the application of domestic laws to extra-territorial offences and copyright infringements on cyberspace. These principles and doctrines are either self-centric or are incomplete to deal with problem of jurisdiction in cyberspace. Analysis of doctrines and principles laid down by various courts is concluded as follows:

The ‘minimum contacts’ theory laid down in *International Shoe Co. v. Washington*, read with ‘purposeful availment’ doctrine recognized in *Asahi Metal Indus. Co. v. Superior Court*, has its own advantages and disadvantages. The ‘minimum contacts’ and ‘purposeful availment’ doctrines enable the defendant to foresee the probable action against him. If the ‘minimum contacts’ and ‘purposeful availment’ doctrines are applied to online copyright infringements a person doing activities on the internet would understand problem action to be taken against him or her. According to the prevailing legal philosophy, foreseeability metric lies at the heart of the reasonableness standard. Reasonable foreseeability doctrine is supported by traditional notions of fair play and substantial justice. The reasonable doctrine is also followed under due process clause of US and procedure established by law clause in India. Therefore, it would protect fundamental rights of the accused person in respective countries.

The ‘purposeful availment’ doctrine further supports territorial sovereignty principle recognized in international law and the traditional understanding of the domestic law. As discussed earlier, in chapter no. II, according to the traditional notion of the law, a person cannot be held responsible under laws of another sovereign state unless he/she either enters into that territory or the other sovereign territory is directly or indirectly affected. This notion was developed in order to protect an individual from application

447 For a detailed analysis on above doctrines refer chapter no. 2.4.1, Pp. 31-33.
of laws of other sovereign nations. The adoption of the ‘purposeful availment’ doctrine saves the individual actor from the application of the laws of all the countries at a time for copyright infringement on internet, though the material is accessed or downloaded in almost all the sovereign states. As discussed earlier, in chapter no. II, in some of the instances, it would minimize the problem of multiple jurisdictions. For example, in instances of multiple sovereign nations claiming jurisdiction at a time, the country which is able to prove minimum contacts and purposeful availment would get privilege to take the action against probable copyright infringement. Other countries which are not able to prove ‘minimum contacts’ or ‘purposeful availment’ would not able to take the cognizance of the case. Therefore, the problem of multiplicity of jurisdictions and prosecutions can be minimized by applying the above doctrines.

Though the application of ‘minimum contacts’ or ‘purposeful availment’ doctrines would minimized problem of multiple jurisdictions and prosecutions, it cannot provided remedy to every victim. In cases of online copyright infringements a wrongful loss to the author may be caused though requirements of ‘minimum contacts’ or ‘purposeful availment’ are not satisfied. For example, in instances of mere uploading the copyrighted material on internet may not fulfill the requirements of above doctrines. It means there would be wrongful loss without a legal remedy. The court would not take action on the ground that either ‘minimum contacts’ with sovereign state is not established or it was not purposefully directed towards the sovereign state.

Further, in instances of passive websites directed towards global community at large, there cannot be ‘minimum contacts’ more than mere accessibility with particular nation. The object of these types of websites may be to make material available or accessible to the globe at large. They are made accessible to the world community at large. In such cases, it is difficult to prove ‘minimum contacts’ more than mere accessibility with a particular country; and it is also difficult to prove ‘purposeful direction’ towards a particular country only. Thus, minimum contacts, if any, established in such instances is against the world at large. Therefore, application of these doctrines to the copyright infringement would make authors helpless. They may not be able to prove establishment of ‘minimum contact’ or ‘purposeful direction’
towards a particular country. In some of the instances, the ‘minimum contact’ or ‘purposeful availment’ may be claimed by multiple countries.

The above analysis on ‘minimum contact’ or ‘purposeful availment’ doctrines shows that there are many advantages of applying these doctrines but, these doctrines cannot be a complete solution to resolve the problem of jurisdiction in cyberspace.

In Sarl Louis Feraud International v. Viewfinder, Inc.\textsuperscript{448} and Yahoo Inc v. La Ligue Contre Le Racisme Et Antisemitisme\textsuperscript{449} cases the question of conflict of laws was raised. The application of the domestic laws to internet in these cases has posed the following basic questions: whether a person using the internet is bound to know the laws of every country? If the answer is yes, then is it really possible to know the laws of every country? If the act is not punishable in a particular country (or social and political set up), then it would be treated as a right of speech and expression of the citizens of that country. In this scenario, is there a need to put extra-restrictions on the speech and expressions on the internet? If the answer is ‘no’, then what shall be the solution to this problem (i.e. application of the domestic laws to cyberspace in above cases)?

The Sarl Louis Feraud International v. Viewfinder, Inc.\textsuperscript{450} case can be criticized on various grounds. According to several authors, the first implication of the District court judgment is that it has adhered to the customary rule of the territorial jurisdiction. According to them the District court has assumed that the laws of the territory are only binding on the territory and other territories’ law cannot be enforced on the said territory. If this approach is accepted under the garb of violation of the constitutional guarantees, it would be sufficient for the offender to find a country with appropriate legal regime and publish any content from there. Such content will remain accessible from the place where the publisher actually wanted it to be accessible. As Horatia Muir-Watt puts it, “there is no reason that the interests of the society in which the harmful effects of free-flowing data are suffered should subordinate themselves to

\textsuperscript{448} The judgment of appellate court is available at http://www.leagle.com/decision/2007963489F3d474_1962 (last updated Nov., 14, 2013).
\textsuperscript{450} The judgment of appellate court is available at http://www.leagle.com/decision/2007963489F3d474_1962 (last updated Nov., 14, 2013).
the ideological claim that the use of a borderless medium in some way modifies accountability for activities conducted through it". These authors expect different treatment to cyberspace. Further, the United States District Court for Southern District of New York dismissed the suit holding that the enforcement of the judgment of the French court is against ‘public policy’. The basic question about the ‘public policy’ is: whose ‘public policy’ should govern the internet activities? Should it be the US or a particular nation’s policy or a policy of the world community? The obvious answer to this question would be the policy of the world community at large. Therefore, there is a need to establish a supra-national forum to decide and implement the ‘public policy’ applicable to the internet.

The *Yahoo Inc v. La Ligue Contre Le Racisme Et Antisemitisme* case a fundamental cases on the conflict of laws and jurisdictions. In this case, the French court relied upon the accessibility doctrine. The US court gave self-centric decision by approving arguments based upon the First Amendment to the US Constitution. Many modern civilized countries including India have started interpreting domestic laws in the light of the International Law. In this case, the US court would have imposed reasonable restrictions upon the right of speech and expression in the light of the international law. Further, according to Rinat Hadas, the instant court did not attempt to discuss moral acceptability of Nazi propaganda. The US court would have applied the principle of comity by responding to the international obligation to act against racism. It further needs to be noted that the military tribunal led by US known as Nuremberg Trial punished the accused on the ground of violation of crimes against humanity. The said military tribunal laid down that in instances of crimes against humanity, responsibility can be imposed upon culprits irrespective of whether the act is punishable under the domestic law of the country or not. It simply means that the


453 See, Vishaka v. State Rajasthan (1997) 6 SCC 241

US is observing double standards while dealing with the crimes against humanity. The above verdict of the tribunal can be used to counter the argument based on the principle of ‘double criminality’. As discussed earlier, the offence against humanity (including offence involved in this case) can be punished irrespective of domestic law. Therefore, in the present case an extradition by US would not have violated the principle of ‘double criminality’.

The analysis of the judgments of the US courts shows that the US courts continuously adhered to the domestic constitutional guarantees and standards, rather than interpreting the same in the light of international legal obligations. Therefore, the decisions of courts are self-centric; the courts have protected their own interests rather than co-operating with the world community. It also reminds the international community about the need to have common standards and uniform rules to be applied to cyberspace. The above notion of the application of every state’s law to the borderless medium would give rise to other multiple problems.\textsuperscript{455}

Similarly, there are many problems in Indian laws dealing with jurisdiction in cyberspace. The analysis of India laws on jurisdiction is as follows:

**Indian Position on Jurisdiction in Cyberspace**

The critical analysis of the jurisdictional clauses under the Information Technology Act, 2000, and the Indian Penal Code, 1860, shows that only partial relief is provided to the Indian nationals under the said provisions. The amendment Act, 2008, of IPC, provides sub-section 3 to section 4 of the Indian Penal Code, 1860. As discussed earlier, for applying IPC to offences against computer resources, the computer resources shall be located in India. According to section 75 of the Information Technology Act, 2000 also, the computer resources should be located in the territory of India. The word ‘involves’ is used in section 75 of IT Act, 2000. It can be construed very broadly. It may include an offence committed by a foreigner against another foreigner involving computer network located in the territory of India. In these types of examples, the offence may be conducted from one sovereign state to another sovereign state via network located in India. In the above examples, neither

\textsuperscript{455} Other problems are discussed in chapter no.III, Pp.56-91.
Indian nationals nor interests of the territory of India are involved. Therefore, this type of broad wording of the legislation is in conflict with the territorial sovereignty principle of the international law.

It is pertinent to note that the word ‘targeting’ is used in sub-section 3 of section 4 of IPC, 1860. The word ‘targeting’ is not further defined or clarified by the legislature. The literal or dictionary meaning of ‘targeting’ is ‘aiming at’. The literal or dictionary meaning of words used in criminal law is needed to be stressed out because the rule of strict interpretation is applicable to criminal law. The rule of strict interpretation implies strict or literal interpretation of criminal law. It is submitted that, after applying the rule of strict interpretation, there is a doubt whether IPC would be applied when: a) aim or target is not a computer resource but a person. It means the intention is not to cause wrongful loss to the computer resources including computer or data per se but to the person via or with help of computer resources (for example, by publishing defamatory comments). In this example ‘means’ and ‘target’ are different. ‘Means’ is the computer resource and ‘target’ is a person. Therefore, in the above example, an offence is committed with the help of a computer resource and not by targeting it. b) the offence is committed by one foreign national against another foreigner from their respective countries via network located in India; c) wrongful loss is caused to the person by making data accessible to the entire world including India but data is copied from the computer located outside the territory of India. d) a passive website is registered and created outside India (for example photographic websites) but accessible in India. Similarly, a website with unauthorized copyrighted material may have access in India without targeting computer resources located in India. In these examples, the target is not the computer resources located in India per se. The intention is to make it accessible to the entire world. Incidentally, it would be accessible in India also.

Apart from the above, section 43A of the Information Technology Act, 2000, is relevant to determine the jurisdiction. According to Section 43A of the Information Technology Act, 2000: “where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls

or operates, in negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.”

It is submitted that according to Section 75 of IT, Act, 2000 or Section 4 of the IPC, the above mentioned body corporate should be located in the territory of India or shall use the computer resources located in India. In other words, Section 43A would not work in isolation. It is not an exception to the Section 75 of the Information Technology Act, 2000. It shall be interpreted along with Section 75 of the IT Act, 2000. It is submitted that reading Section 43A of IT, Act, 2000 in isolation would be inconsistent with basic rule of interpretation of statutes (i.e. statute shall be read as a whole). It is pertinent to note that Section 43A does not provide any liability of the actual offender (i.e. a third person committing offence from foreign jurisdiction with the help of computer etc. situated outside India). In an example of cloud computing or liability under section 43A of the Information Technology Act, 2000, if the body corporate was not negligent in implementing and maintaining reasonable security practices and procedures, then no liability can be imposed against the said body corporate.

In addition to above sections, section 13 of Information Technology Act, 2000 is also relevant to analyze the problem of jurisdiction in cyber space. Section 13 deals with time and place of dispatch and receipt of electronic record. Sub-Section 3 of the section 13 is worded as follows: “Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.” Section 13 of the IT Act, 2000 assumed the place of dispatch and place of receiver of electronic record at the place of business, irrespective of actual place of dispatch or receipts of the electronic record. This assumption is important because it provides jurisdiction to the Indian courts if

---

457 It is pertinent to note that word ‘Agreed’ is used in sub. 3 of Section 13, it means by agreement parties can decide the place of receiving and dispatching the electronic record. It is needed to be noted that parties cannot decide jurisdiction of criminal law (particularly in cognizable offences). Therefore, jurisdiction according to section 13 of IT, Act, 2000 cannot be applied to the criminal offences, including copyright infringements. Thus, sub. section 3 of Section 13 of IT Act, 2000 would be applicable to civil wrongs only.
the place of business of originator or addressee is in India. According section 13 the court will have jurisdiction though the electronic record in fact may or may not be received in or dispatched from the computer, computer systems or computer mechanism situated in India. Normally, the court gets jurisdiction at the place of business, place of dispatching of electronic record and place of receiving the electronic record. Section 13 of the IT, Act, 2000 will have overriding effect on CPC and Cr.P.C.\textsuperscript{458} As discussed above, according to statutory assumptions created under section 13 of IT Act, 2000 though the person is residing and dispatching an electronic message from the territory of India and if his place of business is outside the territory of India, the Indian court cannot exercise the jurisdiction. Similarly, according to said assumption created under section 13 the court can assumed jurisdiction though electronic message is dispatched or received outside the territory of India if the person receiving or dispatching an electronic message has place of business in India.

It needs to be noted that because of section 13 of the IT Act, 2000 the Indian court would not be able to take cognizance of the matter though act of dispatching electronic message is partially or fully conducted from the territory of India. Further, because of this statutory assumption the court would be unable to take cognizance of the matter even if the electronic message has an adverse impact on rights or interests of the citizen(s) of India. The assumption created under section 13 of IT Act, 2000 does not have any advantage as such because otherwise also according to general principles of jurisdiction and CPC and Cr. P.C the court was empowered to take cognizance of the matter at the place of the business of the person. Section 13 of the IT Act, is apparently inconsistence with territorial and passive nationality principles of International law on jurisdiction.

The Indian laws applicable to cyberspace do not provide jurisdiction against foreigners if they are not using computer resources located in India. The rights of Indian citizens can be infringed in cases of cloud computing when resources are located outside India or Indian nationals are carrying material with them outside the territory of India.

\textsuperscript{458} See, Section no. 81 of IT Act, 2000
Apart from above, section 1 (2) and section 62 of Indian Copyright Act, 1957 are relevant to analyze the problem of jurisdiction in cyberspace. According to section 1 (2) of the Indian Copyright Act, 1957, the Indian Copyright Act extends to the whole of India. According to section 62 (1) of the Indian Copyright Act, 1957, “Every suit or other civil proceeding arising under this chapter in respect of the infringement of copyright in any work or the infringement of any other right conferred by this Act shall be instituted in the district court having jurisdiction”. Further, according to section 62(2) of the Indian Copyright Act, 1957 for the purpose of sub-section 1 district court include a district court within the local limits of whose jurisdiction, at the time of the institution of the suit or other proceeding, the person instituting the suit or other proceeding actually and voluntarily resides or carries on business or personally works for gain. The explanation on above sections shows that the Indian Copyright Act, 1957 is made applicable to the Indian territories only. It does not provide any express provision for extra-territorial application of the Indian Copyright Act, 1957.

In other words, Indian laws of jurisdiction are location (territory)-centric rather than victim-centric. The IT Act and the IPC are apparent examples of non-application of the passive nationality principle recognized by the International Law. It is respectfully submitted that the Indian parliament lacks visualization of nature and probable offences committed with the help of cyberspace. The Indian laws on jurisdiction need to shift the offence-centric paradigm to the victim centric paradigm.

Research question 3 “Whether de-territorial nature of cyberspace has any impact upon the established principles of international law?” is analyzed in chapter no. II of the research. Findings on the research question 3 are that de-territorial nature of cyberspace has adverse impact on the established principles of International law. The findings on the question no. 3 is as follows:

**Technological Advancement and its Impact on established Principles and Doctrines of International Law**

The advancement of technology and technological inter-dependency has an adverse impact on the established principles of the International Law (such as the principle of Sovereign Jurisdiction; Non-Interference; Sovereign Equality, etc.). The foundation of
the doctrines of sovereignty, non-interference and sovereign equality are affected and the horizon of the national and international law is continuously widening because of the de-territorial nature of cyberspace. The information technology has not only increased inter-dependence between domestic laws and international law but has also changed the power structure, including the power to decide on matters affecting their nationals. The above mentioned powers, according to traditional doctrines or principles, were assigned to respective sovereign states. The technological advancements empowered the ICANN, a body established by US laws to assume the jurisdictional power regarding the domain name disputes, though it is not an international body established by UNO or approved by other sovereign nations. The internet also undermines the feasibility and legitimacy of laws based on territorial boundaries. The technologically powerful states are able to establish corporations like ICANN to control sovereign powers of other states. Since the ICANN is not legitimized in accordance with the established process of international law, it cannot be treated as an international or intra-national organization. Therefore, this type of controlling by ICANN is illegitimate and contrary to the established doctrines and principles of international law.

The cyberspace also undermines the principle of territorial sovereignty, sovereign equality and non-interference. The principle of territorial sovereignty cannot be applied in the strict sense in the era of cyberspace. Furthermore, the traditional international law does not compel a person to observe the law of other nations unless he/she enters into that territory or that territory is directly affected. But in the era of internet, it is difficult to observe as to how many countries are directly or indirectly affected. The principles such as ‘accessibility’ and ‘impact theory’ are allowing other sovereign nations to interfere with the activities of other nationals on the internet. Further, the US, under the garb of ICANN, controls the activities of the non-nationals in relation to the domain name such as registration, cancellation, transfer and change of domain name. ICANN is able to interfere with the rights of the nationals of a sovereign territory, which is one of the prerogatives of a sovereign state according to the established principles of international law. The technologically advanced states and non-state actors are able to interfere with the sovereignty of others. Thus, the principle of non-interference and sovereign equality is not strictly followed in
cyberspace. Therefore, the cyberspace has an adverse impact on the well-established principles of sovereignty, sovereign equality and non-interference.

Research question 4 i.e. “Whether the cyberspace has posed legal and jurisprudential challenges before the Adversarial Criminal Justice Systems in dealing and co-operating with cross-border copyrights infringements from Inquisitorial Criminal Justice Systems?” is analyzed in chapter no. III of the research. The findings on question 4 are that there are multiple problems before Adversarial Criminal Justice System in dealing and co-operating with cross-border copyrights infringements from Inquisitorial Criminal Justice Systems. The findings of the research are as follows:

Conflicting Principles followed in Common Law and Civil Law Systems: A Challenge in dealing with cross border Copyrights Infringements in Cyberspace

The working and principles followed in inquisitorial and adversarial systems are different. The expected roles of the judge in both the systems are different. In an adversarial system, the judge is a neutral umpire. The parties to the litigation are active. The neutrality of the judge is treated as one of the features of the adversarial system. It is a part of due process, natural justice principle and fair hearing. The judge in an inquisitorial system including most of European countries is active. In the instances of cyber crimes (including copyright infringement), if the accused from an adversarial system is tried in an inquisitorial system, his/her right to be tried by a neutral and passive judge would be violated. The adversarial countries may not be legally allowed or willing to extradite their own nationals in violation of the above mentioned rights.

In an adversarial system, the formal burden of the proof lies on the prosecution. The criminal litigation shall be proved beyond all reasonable doubts. In an inquisitorial system, no formal standard of proof is set, but definitely it is not beyond reasonable doubt. The standard followed in an inquisitorial system is inner satisfaction and conviction of judge. The proof beyond the reasonable doubt is not only the principle of fair play, but it is one of the requirements of the due process. The US court in Re Winship459 held that, the Due Process Clause, protects an accused “against conviction

---

except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime with which he is charged.” Due Process is one of the fundamental rights in the US. The due process requirement is also interpreted under Article 21 of the Constitution of India. The requirement of proof beyond all reasonable doubts is not expressly recognized under Article 21 of the Indian Constitution, but it is followed in criminal justice system. Justice Krishna, Iyer in Sunil Batra Case,\textsuperscript{460} held that though the Constitution had no ‘due process’ provision, yet after the Maneka Gandhi judgment the consequence was the same. Therefore, there is a very high probability of getting standard of proof beyond all reasonable doubt recognized under Article 21 of the Constitution of India.

According to the prevailing jurisprudential understanding, the fundamental rights are available against the state. In other words, the state shall not take any action in violation of fundamental rights. It means though the US or India wants to co-operate with the inquisitorial system, it cannot extradite a person from their jurisdiction. The extradition to an inquisitorial system would violate the above-mentioned Constitutional and legal guarantees (i.e. proving criminal charges beyond all reasonable doubts, which is a part of due process). The conflicts in the principles of the criminal justice systems (i.e. role of judge and constitutional guarantee, due process) is one of the legal challenges in co-operation before the adversarial criminal justice system.

Right against Self –incrimination, Right of Cross Examination and Right against Ex-post Facto Laws: A Challenge in dealing with Cross-border Copyright infringements

The right against self-incrimination is one the basic principles followed in adversarial systems including US and India. The right or privilege against self-incrimination is protected as one of the fundamental rights in India and US. The said right is not fully protected or recognized in inquisitorial systems, prevailing in most of European countries. Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, Section 34 of the Criminal Justice and Public Order Act, 1994 of UK, Section 89 of New South Wales Evidence Act, 1995, etc.

\textsuperscript{460} Sunil Batra (AIR 1978 SC 1675)
permits a court to draw ‘adverse’ or ‘appropriate’ inference in appropriate criminal cases. Further, inquisitorial courts and European Court of Human Rights recognized the limitations in drawing ‘appropriate’ inferences in Murray (John) v. UK\textsuperscript{461} and R. v. Argent.\textsuperscript{462}

The above deliberation demonstrates that in the adversarial system, the right against self-incrimination is considered a fundamental guarantee provided in the Constitutions of US and India. The authority to draw ‘appropriate’ or ‘adverse’ inference is not only against the standard of ‘beyond reasonable doubt’ (which is recognized as a part of due process); but also against the right against self-incrimination. Therefore, as discussed earlier, co-operation with the inquisitorial system, including extradition, would lead to violation of basic guarantee provided in the Constitutions of US and India. It also would lead to violation of basic principles followed in an adversarial criminal justice system including ‘nemo debet prodere se ipsum’\textsuperscript{463}. Therefore, the right against self-incrimination and ‘Nemo debet prodere se ipsum’\textsuperscript{464} are challenges before the adversarial criminal justice system with respect to co-operation with inquisitorial systems. The right of cross-examination is guaranteed as a fundamental right in US. It is followed as a statutory right and natural justice principle in India. In a number of cases, the judiciary in India held that the actions of authorities inconsistent with fundamental rights and natural justice principles are null and void. The judiciary in India also stated the exceptions to the right of cross-examination. The offences in cyberspace per se are not yet recognized as one of the exceptions to the right of cross examination. An action of the state (including extradition) in probable violation of fundamental rights or natural justice principles shall be null and void. Therefore, guarantee of cross-examination in adversarial system and absence of the said guarantee in the inquisitorial system, including European countries, is one of the challenges for the adversarial criminal justice systems.

\textit{Nullum crimen, nulla poena sine lege} or the principle of \textit{ex-post facto laws} has territorial applications. It means that though the act is punishable in other territories

\textsuperscript{462}R v. Argent [1997] 2 Cr.App. R. 27
\textsuperscript{463}i.e. ‘no one can be required to be his own betraye r’
\textsuperscript{464}i.e. ‘no one can be required to be his own betraye r’
the person cannot be held responsible in sovereign territory where it is not punishable. For the purpose of *ex-post facto laws* (Article 20 of the Constitution of India) or *nullum crimen, nulla poena sine lege* law means territorial law. The discourse on the nature of the cyberspace shows that the action on cyberspace cannot be circumscribed by physical boundaries of a sovereign territory. No legal entity or sovereign state has the capacity to control and confine offences on cyberspace in the territorial boundaries. The *ex-post facto laws* are protected as fundamental rights in India and US. Therefore, taking cognizance based on ‘accessibility principle’ and ‘impact doctrine’ may infringe the fundamental rights protected in India and US, if the act committed is not punishable in the said countries. According to prevalent jurisprudence, the state is bound to protect the fundamental rights of the citizens. Thus, implementation of the right against *ex-post facto laws* is one of the challenges because of the de-centralized nature of the cyberspace.

In the light of the above challenges, particularly violation of fundamental rights, the remedy left with a sovereign state recognizing the adversarial system is punishing its own nationals. To resolve the above-mentioned challenges, the international community needs to establish a supra-national forum. The supra-national criminal justice system needs to accommodate the features of both the inquisitorial and the adversarial systems.

In order to resolve the challenges posed by cyberspace, the present international law needs to play at least three-fold functions. Firstly, the international law has to protect the autonomy of every individual human being by preserving his freedom to access and disseminate the information on the internet with the help of technology, irrespective of his state territory. Secondly, the International law has to protect the autonomy of every individual state. Thirdly, the international community needs to lay down the principles and the standards to be followed in intra-national and international law to resolve the above problems and protect the copyrights in cyberspace.

Research question 5 i.e. “Do laws in India and US provide adequate protection to copyrights with regard to hyperlinking in cyberspace?” is analyzed in chapter no. IV of the research. The researcher found that right against hyperlinking has been not
declared as one of the exclusive rights of the author. Findings of the researcher are as follows:

**Hyperlinking vis-à-vis Copyrights Infringements in Cyberspace**

The analysis on hyperlinking and copyrights infringement shows that there can be a liability for direct infringement of copyrights on linking parties in the instances of framing and inline linking under US and Indian Copyright Laws. The linking parties cannot be held responsible for direct infringement in scenario of deep-linking (apart from framing and inline linking). Further, linking parties cannot be held responsible for contributory infringement because keeping linked resource on the internet is not a copyright infringement itself. The linked resource are normally kept by the author himself or by a person authorized by him. They (linking parties) cannot be held responsible for contributory liability when the copyrighted resource is either provided by the author or if it is provided with the permission of the author. Normally, the end-users of the internet cannot be held responsible for copyright infringement. Therefore, liability for indirect infringement cannot be imposed on linking party.

At present, in deeplinking, there is a wrongful loss to the author but there is no legal remedy available either under the Indian and US Copyright Laws. Therefore, the judiciary has an opportunity to declare at least framing and inline linking as copyright infringement under existing US and Indian laws by judicial interpretation. In the instances of deeplinking, apart from inline linking or framing, the existing US and Indian laws on copyright do not support the claim of the author. The practice of deeplinking is also inconsistent with the objectives to be achieved by the websites. The claim of implied authority does not hold water because it is limited by implied conditions or limitations.

Therefore, the framing, inline linking and deeplinking shall be declared as exclusive rights of the author of the work under Section 14 of the Indian Copyright Act and Section 101, Title 17, of US Copyright Laws. The linking by search engine shall not be made as an offence in order to balance the interest of society and the interest of the authors of the copyrighted material. The internet cannot work effectively at least without the linking by search engine. Therefore, prohibition of linking by a search engine would hamper the growth of internet and interest of society at large.
5.2 RECOMMENDATIONS

5.2.1 Short term recommendations

1) The laws on jurisdiction need to be victim centric—rather than object centric to protect copyrights in cyberspace.

2) The US, India and EU countries need to amend the principles followed in the respective states in order to increase co-operation in cyberspace in protecting copyrights.

3) Framing, Inline-Linking and Deep-Linking, except linking by search engines shall be declared as an exclusive right of the author under Section 14 of the Indian Copyright Act, 1957, and Section 101, Title 17, of Copyright Law of US.

4) There shall be special courts dealing with Intellectual Property infringements (including copyright infringements) at district level as nominated by Delhi government in India.

5) There is a need to consider bringing copyright infringement in cyber space under universal jurisdiction.

5.2.2 Long term recommendations

1) The cyberspace shall be recognized as entirely separate space/territory to address problem of copyright infringement in cyberspace.

2) Need to Establish Supra-National Organization
The international community shall establish a supra-national body to deal with cyberspace. The supra-national body shall have different departments such as: a) Department for rules and policymaking: This department shall lay down uniform rules and policy applicable to cyberspace. b) Department to deal with the use of technology to protect the rights of nations and nationals in cyberspace: This department shall have a Research and Development wing to find out and develop technological measures to prevent cyber crimes and IPR
infringements in cyberspace. The Research and Development wing shall share technology and know-how with the member states. c) Special department for investigation of transnational offences d) Department dealing with IPR infringements in cyberspace; e) Department dealing with and protecting critical infrastructure of sovereign states. This department shall help sovereign states in protecting critical infrastructures of the member states. It may include protection to the banking system, protection to the public key infrastructure and protection to military and other important digital infrastructures. The organization also needs to have a separate international tribunal with fora or benches at regional levels. The procedure for appointment of judges of such international tribunal and benches shall be at par with the procedure followed for the International Court of Justice.

The International law is a weak law. The basic problem faced by International Law is the problem of implementation. Establishment of a supra-national organization to deal with cyberspace would also pose the question of implementation of the judgments of supra-national tribunal and rules and policy laid down by such an organization. There can be the following ways to implement policies and judgments of such supra national body:

a) **Compensation Fund:** The member states shall pay a fixed sum of money to become a member of such supra-national organization. The said amount can be fixed based upon the economic conditions of the particular state. The fund paid by member states shall be divided into two parts: half of the fund provided by the member states shall be utilized for administration purposes and the remaining fund shall be kept as a compensation fund in the account of a particular member. If the state will not be ready to take cognizance or to pay compensation to the victims of cyber crimes or copyright infringements from other nation(s). The compensation out of interest or from the principal amount of the said state’s compensation fund shall be paid. In case of exhaustion of the compensation fund, the said member states’ membership shall be terminated. It will have a deterrent effect on the defaulting state and it will force other member states to cooperate with the supra-national organization.
b) **Special incentives and privileges**: The member states, implementing rules and policies shall get special concession and technological help to build digital infrastructure. Such member states shall get a special concession in know-how about the technology.

c) **Awards and recognitions**: The supra-national organization shall declare some awards for members adhering to its rules and policies.

d) **Economic Sanctions**: Any sovereign state violating rules and policies with respect to critical digital technology shall be subject to economic sanctions by the member states.

e) **Use of Force**: The supra-national organization shall have power to use military force against the state attacking the critical infrastructures, including military and other institutions of any member state. The use of force can be done with the help of Security Council of UNO.

f) **Awareness and educational drives**: The supra-national organization shall spend a sum of money on awareness and education drive about cyber crimes and copyright infringements.

3) The law made by the supra-national organization must address whether a particular event in cyberspace is controlled by the laws of the state or country where the website is located or by the laws of the state or countries where the internet service provider is located, or perhaps by all of these laws.

4) There shall be a Central Website alerting the authors about the Linking to the copyrighted material in cyberspace.

5) There shall be a system alerting the end-user whether particular linking is with or without the consent of the author of the copyrighted material. For example, the end-user may get a pop-up stating the status of linking to particular resource.

6) The linking party (party providing link to online material) shall get alert from central website that linking may lead to technological torts or copyright infringement to avert abuse such as links to online material.
5.3 SCOPE FOR FURTHER STUDY
Scope to conduct further research exists in following areas:

a) Problem of jurisdiction and the civil wrong in instances of copyright infringement in cyberspace

b) Problem of policing in cyberspace and copyright infringement

c) Problems with regard to digital evidences, computer forensics and copyright infringement

d) Problem with regard to investigation in instances of cross-border offences

e) Problem with respect to implementation of the law protecting copyrights in cyberspace

f) Linking in cyberspace vis-a-vis trademark infringement and violation of the law of torts

g) Linking and infringement of the criminal laws such as mis-appropriation of the digital property in cyberspace

h) The problem of extradition in the instances of copyright infringement in cyberspace

i) Critical analysis of the existing International framework of copyright protection including TRIPS and WIPO.