EXECUTIVE SUMMARY

Introduction
Copyright Infringement in cyber era is a global phenomenon. Development of science and technology and the increasing need to gain access to information have broadened the horizons of cyberspace. A person sitting or working in any remote corner of the world can violate copyrights of any other individual residing anywhere in the world. The cyberspace has bestowed many gifts upon humanity; but at the same time it has become a place to do all sorts of activities which are prohibited by law. The Cyberspace is a borderless space and has led to many legal and jurisprudential problems and challenges for the enactment, enforcement and interpretation of laws. To meet changing demands of cyberspace, various sovereign countries have enacted a number of domestic legislations. On international level too, there are various Conventions enacted in the arena of cyberspace and intellectual property rights. At the same time, some international organizations are working in order to meet challenges posed by cyber crimes and IPR violations. Domestic courts of states have been dealing with the problems posed by cyberspace, but have come up with inconsistent answers. The present research is intended to critically analyze the existing legal framework of EU, US and India with respect to problems raised by cyberspace and copyright infringements in cyberspace.

Problem Statement
The cyber crimes in various forms and Intellectual Property violations in particular on and through the internet are continuously on the rise. In 1999, business PC application software accounted for worldwide revenues of $21.6 billion – a 19% increase over the last year. A research undertaken by hankooki.com in 2003 has shown that cyber crimes increased 500-fold in 5 years. The Federal Computer Crime Unit registered a

3 Such as, WTO, Council on TRIPS, WIPO, ICANN, etc.
4 See, JUSTICE YATINDRA SINGH, CYBER LAWS, 4 (3rd ed. 2007). Some of the basic controversial cases are discussed in this book.
45% increase in the Internet based crime compared to 2004. In 2003 the loss was $30 billion and it increased to $32.6 billion in 2004. Legal Week Survey published in May, 2013 shows that as many as 80% believe that their firm is likely to be hit by web hackers. An increasing rate of cyber crime and Intellectual Property is shocking though all cases are not registered. All cases are not registered because the owners of Intellectual Property are either not aware of the infringements or they do not bother about their rights.

The de-territorial nature and *modus operandi* of cyberspace have posed various legal and jurisprudential problems such as problem of jurisdiction, challenges for territory-based criminal justice system while dealing with extra-territorial copyright infringement in cyberspace, problems with regard to linking and copyright infringement in cyberspace. The cyberspace also has an impact on the traditional principles of international law and these impacts are applicable to copyright infringement too.

**Summary of the research is as follows**

**Problem of jurisdiction in cyberspace**

The problem of jurisdiction in cyberspace is analyzed in chapter no. II of the research. Summary of the chapter no. II is as follows:

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. 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 jurisdiction are developed by keeping in mind the principle of territorial sovereignty. 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.\(^\text{10}\) 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.

\(^{10}\) For a detailed explanation on principles of international law on jurisdiction refer chapter no. 2.2.1.1.
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.

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. \textit{erga omnes} obligations owed to the international community or for violation of peremptory norms of international law (i.e. \textit{jus cogens}). Ordinary cyber crimes, including online copyright infringements are not considered as \textit{erga omnes} or violation of peremptory norms of international law (i.e. \textit{jus cogens}). Therefore, according to customary international law, state practices, \textit{opinion juris} or existing Conventions, the State cannot claim jurisdiction for ordinary cyber crimes or online copyright infringements under the principle of universal jurisdiction.

**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*,\(^\text{11}\) read with ‘purposeful availment’ doctrine recognized in *Asahi Metal Indus. Co. v. Superior Court*,\(^\text{12}\) 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 ‘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
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.
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.

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.

The *Sarl Louis Feraud International v. Viewfinder, Inc.* 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 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.

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

---

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

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 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’. 18 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).

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.

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.

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

Conflicting Principles followed in Common Law and Civil Law Systems are analyzed in Chapter no. III of the research. Summary of on conflicting principles and problem posed by cyberspace is as follows:

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. 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{19} and R. v. Argent.\textsuperscript{20}

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{21} Therefore, the right against self-incrimination and ‘Nemo debet prodere se ipsum’\textsuperscript{22} 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.

Nullum crimen, nulla poena sine lege or the principle of ex-post facto laws has territorial applications. It means that though the act is punishable in other territories the person cannot be held responsible in sovereign territory where it is not punishable.

\textsuperscript{20} R v. Argent [1997] 2 Cr.App. R. 27
\textsuperscript{21} i.e. ‘no one can be required to be his own betrayer’
\textsuperscript{22} i.e. ‘no one can be required to be his own betrayer’
For the purpose of \textit{ex-post facto laws} (Article 20 of the Constitution of India) or \textit{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 \textit{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 \textit{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.

**Hyperlinking \textit{vis-à-vis} Copyrights Infringements in Cyberspace**

Hyperlinking and copyright infringement is analysed in chapter no. IV of the research. Summary on hyperlinking and copyright infringement is as follows:
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 may be a wrongful loss caused 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.