Valedictory Lecture on 16th April,2010 at 12.00 noon at the Indian Law Institute on the Cyber Law and Intellectual Property Rights Law in the Training Programme for Government Attorneys of Nepal from 26th March,2010 to 16th April,2010 at the Indian Law Institute, New Delhi.

By

Justice Rajesh Tandon,
Chairperson
Cyber Appellate Tribunal
Ministry of Communications & Information Technology
Department of Information Technology,
Jeevan Bharti (LIC) Building, Connaught Place
New Delhi.

Subject

CYBER LAW AND INTELLECTUAL PROPERTY RIGHTS LAW.

The Information Technology Act,2000 came into force on 17th October, 2000. This Act was amended vide Notification dated 27th October, 2009.The definition of the Information Technology Act provides as under:

"Computer" means any electronic, magnetic, optical or other high speed date processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

Section 3 provides with regard to Digital signature and the Authentication of electronic records.

Section 4 provides the legal recognition of electronic governance. For short known as E. governance.

For adjudicating of the dispute under the Information Technology Act, Section 46 was enacted which has given the power for adjudication of the crimes. The power has been given to the Secretary, Information Technology and he has power to adjudge the quantum of compensation under Sections 46 and 47 of the Act. Sections 46 and 47 are quoted below:

46. Power to adjudicate.-

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made hereunder the Central Government shall, subject to the provisions of Sub-section (3),appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer or holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in Sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3)No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4)Where more than one adjudicating officer are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5)Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under Sub-Section (2) of Section 58, and-

(a)All proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code (45 of 1860)

(b)Shall be deemed to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974)

47. **Factors to be taken into account by the adjudicating officer.** -

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely-

(a)The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default.

(b)The amount of loss caused to any person as a result of the default;

(c) The repetitive nature of the default.

Sections 43 and 44 of the Information Technology Act,2000 provides penalties and their Adjudication. It reads as under:

Penalties and Adjudication

43. Penalty for damage to computer to computer, computer system etc.- If the person without permission of the owner or any other person who is in charge of a computer, computer system or computer network-

(a) Accesses or secures access to such computer, computer system or computer network;

(b) Downloads, copies or extracts any data, computer date-base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act. Rules or Regulations made hereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network.

He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.-For the purposes of this section-

(i)"computer contaminant" means any set of computer instructions that are designed-
(ii)to modify, destroy, record, transmit data or programme residing within a computer system or computer network;
by any means to usurp the normal operation of the computer, computer system or computer network;

(ii) "computer data-base" means a representation of information knowledge, facts, concepts or

instructions in text, image, audio, \ video that are being prepared or have been prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or system or computer network and are intended for use in a computer, computer system or computer network.

(iii) "Computer virus" means any computer instruction; information, data or programme that destroys, damages degrades or adversely affects the performance of a computer.

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information, return, etc.- If any person who is required under this Act or any rules or regulations made thereunder to-

(i) furnish any document, return or report to the Controller of the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(j) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(k) maintain books of account or records fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary penalty.- Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty five thousand rupees.

The offences under the Information Technology Act are as under:

Section 65. Tampering computer source documents.-Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment upto three years, or with fine which may extend upto two lakh rupees, or with both.

Section 66 . Computer related offence.- If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

.

Section 66A. Punishment for sending offensive messages through communication service etc. Any person who sends, by means of a computer resource or a communication device.-

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device. – Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C:Punishment for identity theft.-Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D:Punishment for cheating by personation by using computer resource.-Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E: Punishment for violation of privacy.-Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three yeas or with fine not exceeding two lakh rupees, or with both.

Section 66F. Punishment for cyber terrorism:-

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any computer contaminant; and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the

critical information infrastructure specified under section 70 or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise.

Commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.'

Section 67. Punishment for publishing or transmitting obscene material in electronic form.-Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form. Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent

conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B:Punishment for publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form.-Whoever-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuses or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Provided that provisions of Section 67, Section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form.

Section 67C. Preservation and retention of information by Intermediaries. (1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

Section 70. Protected system.-(1)The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub section (1).
(3)Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

Section 71.Penalty for misrepresentation.—Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or (Electronic Signature) Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72. Breach of Confidentiality and Privacy.- Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72A Punishment for disclosure of information in breach of lawful contract.—Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

Section 73. Penalty for Publishing (Electronic Signature) Certificate false in certain particulars.- (1) No person shall publish a (Electronic Signature) Certificate or otherwise make it available to any other person with the knowledge that-

(a) the Certifying Authority listed in the certificate has not issued it, or
(b) the subscriber listed in the certificate has not accepted it, or
(c) the certificate has been revoked or suspended.,

unless such publication is for the purpose of verifying a (electronic signature) created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

.

Section 78 of I.T. Act empowers Inspector of Police to investigate cases under the Act

JURISDICTION UNDER THE INDIAN PENAL CODE IN RELATION TO CYBER OFFENCES

(i)	Sending threatening messages by email	Section 503 IPC
(ii)	Sending defamatory messages by email	Section 499 IPC
(iii)	Forgery of electronic records	Section 463 IPC
(iv)	Bogus websites, cyber frauds	Section 420 IPC
(v)	Email spoofing	Section 463 IPC
(vi)	Web-jacking	Section 383 IPC
(vii)	E-Mail Abuse	Section 500 IPC
(viii)	Online sale of Drugs	NDPS Act
(ix)	Online sale of Arms	Arms Act

For adjudicating the aforesaid crimes, the power has been given to the Adjudicating Officer. After the decision of the Adjudicating Officer, the appeal lies to the Appellate Tribunal

under Section 48 of the Information Technology Act,2000. It reads as under:

"48.Establishment of Cyber appellate Tribunal.- (1) The Central Government shall, by notification, establishes one or more appellate tribunals to be known as the Cyber Regulation Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in Sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction."

He exercises the powers contained under Section 58 of the Information Technology Act, which reads as under:-

58. Procedure and powers of the Cyber Appellate Tribunal.-

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2)The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely-

(a)Summoning and enforcing the attendance of any person and examining him on oath;

(b)Requiring the discovery and production of documents or other electronic records;

(c)Receiving evidence on affidavits;

(d) Issuing commissions for the examination of witnesses or documents;

(e) Reviewing its decisions

(f) dismissing an application for default or deciding its ex parte;

(g) any other matter which may be prescribed.

(3)Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of Sections 193 and 228, and for the purposes of Section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of Section 195 and Chapter XXVI of the Code of Criminal Procedure.

Section 61 of the Information Technology Act, 2000 also debars the civil court in respect of the matters which are being tried by the Cyber Tribunal and directly the appeal goes to the High Court against the judgment of the Cyber Appellate Tribunal.

INTELLECTUAL PROPERTY RIGHTS IN INDIA

Intellectual property rights as a collective term includes the following independent IP rights which can be collectively used for protecting different aspects of an inventive work for multiple protection:-

Patents
Copyrights
Trademarks
Registered (industrial) design
Protection of IC layout design,
Geographical indications, and
Protection of undisclosed information

Nature of Intellectual Property Rights

IPR are largely territorial rights except copyright, which is global in nature in the sense that it is immediately available in all the members of the Berne Convention. These rights are awarded by the State and are monopoly rights implying that no one can use these rights without the consent of the right holder. It is important to know that these rights have to be renewed from time to time for keeping them in force except in case of copyright and trade secrets. IPR have fixed term except trademark and

geographical indications, which can have indefinite life provided these are renewed after a stipulated time specified in the law by paying official fees. Trade secrets also have an infinite life but they don't have to be renewed. IPR can be assigned, gifted, sold and licensed like any other property. Unlike other moveable and immoveable properties, these rights can be simultaneously held in many countries at the same time. IPR can be held only by legal entities i.e., who have the right to sell and purchase property. In other words an institution, which is not autonomous may not in a position to own an intellectual property. These rights especially, patents, copyrights, industrial designs, IC layout design and trade secrets are associated with something new or original and therefore, what is known in public domain cannot be protected through the rights mentioned above. Improvements and modifications made over known things can be protected. It would however, be possible to utilize geographical indications for protecting some agriculture and traditional products.

It has become fashionable to toss copyright, patents, and trademarks—three separate and different entities involving three separate and different sets of laws—into one pot and call it "intellectual property". The distorting and confusing term did not arise by accident. Companies that gain from the confusion promoted it. The clearest way out of the confusion is to reject the term entirely.

According to Professor Mark Lemley, now of the Stanford Law School, the widespread use of the term "intellectual property" is a fashion that followed the 1967 founding of the World "Intellectual Property" Organization (WIPO), and only became really common in recent years. (WIPO is formally a UN organization, but in fact represents the interests of the holders of copyrights, patents, and trademarks.)

The term carries a bias that is not hard to see: it suggests thinking about copyright, patents and trademarks by analogy with property rights

for physical objects. (This analogy is at odds with the legal philosophies of copyright law, of patent law, and of trademark law, but only specialists know that.) These laws are in fact not much like physical property law, but use of this term leads legislators to change them to be more so. Since that is the change desired by the companies that exercise copyright, patent and trademark powers, the bias introduced by the term “intellectual property” suits them.

The bias is reason enough to reject the term, and people have often asked me to propose some other name for the overall category—or have proposed their own alternatives (often humorous). Suggestions include IMPs, for Imposed Monopoly Privileges, and GOLEMs, for Government-Originated Legally Enforced Monopolies. Some speak of “exclusive rights regimes”, but referring to restrictions as “rights” is doublethink too.

Some of these alternative names would be an improvement, but it is a mistake to replace “intellectual property” with any other term. A different name will not address the term's deeper problem: overgeneralization. There is no such unified thing as “intellectual property”—it is a mirage. The only reason people think it makes sense as a coherent category is that widespread use of the term has misled them.

The term “intellectual property” is at best a catch-all to lump together disparate laws. Nonlawyers who hear one term applied to these various laws tend to assume they are based on a common principle and function similarly.

Nothing could be further from the case. These laws originated separately, evolved differently, cover different activities, have different rules, and raise different public policy issues.

Copyright law was designed to promote authorship and art, and covers the details of expression of a work. Patent law was intended to

promote the publication of useful ideas, at the price of giving the one who publishes an idea a temporary monopoly over it—a price that may be worth paying in some fields and not in others.

Trademark law, by contrast, was not intended to promote any particular way of acting, but simply to enable buyers to know what they are buying. Legislators under the influence of the term “intellectual property”, however, have turned it into a scheme that provides incentives for advertising.

Since these laws developed independently, they are different in every detail, as well as in their basic purposes and methods. Thus, if you learn some fact about copyright law, you'd be wise to assume that patent law is different. You'll rarely go wrong!

People often say “intellectual property” when they really mean some larger or smaller category. For instance, rich countries often impose unjust laws on poor countries to squeeze money out of them. Some of these laws are “intellectual property” laws, and others are not; nonetheless, critics of the practice often grab for that label because it has become familiar to them. By using it, they misrepresent the nature of the issue. It would be better to use an accurate term, such as “legislative colonization”, that gets to the heart of the matter.

Laymen are not alone in being confused by this term. Even law professors who teach these laws are lured and distracted by the seductiveness of the term “intellectual property”, and make general statements that conflict with facts they know. For example, one professor wrote in 2006:

> Unlike their descendants who now work the floor at WIPO, the framers of the US constitution had a principled, pro-competitive attitude to intellectual property. They knew rights

might be necessary, but…they tied congress's hands, restricting its power in multiple ways.

That statement refers to Article 1, Section 8, Clause 8 of the US Constitution, which authorizes copyright law and patent law. That clause, though, has nothing to do with trademark law. The term "intellectual property" led that professor to make false generalization.

The term "intellectual property" also leads to simplistic thinking. It leads people to focus on the meager commonality in form that these disparate laws have—that they create artificial privileges for certain parties—and to disregard the details which form their substance: the specific restrictions each law places on the public, and the consequences that result. This simplistic focus on the form encourages an "economistic" approach to all these issues.

Economics operates here, as it often does, as a vehicle for unexamined assumptions. These include assumptions about values, such as that amount of production matters while freedom and way of life do not, and factual assumptions which are mostly false, such as that copyrights on music supports musicians, or that patents on drugs support life-saving research.

Another problem is that, at the broad scale implicit in the term "intellectual property", the specific issues raised by the various laws become nearly invisible. These issues arise from the specifics of each law—precisely what the term "intellectual property" encourages people to ignore. For instance, one issue relating to copyright law is whether music sharing should be allowed; patent law has nothing to do with this. Patent law raises issues such as whether poor countries should be allowed to produce life-saving drugs and sell them cheaply to save lives; copyright law has nothing to do with such matters.

Neither of these issues is solely economic in nature, and their noneconomic aspects are very different; using the shallow economic overgeneralization as the basis for considering them means ignoring the differences. Putting the two laws in the "intellectual property" pot obstructs clear thinking about each one.

Thus, any opinions about "the issue of intellectual property" and any generalizations about this supposed category are almost surely foolish. If you think all those laws are one issue, you will tend to choose your opinions from a selection of sweeping overgeneralizations, none of which is any good.

If you want to think clearly about the issues raised by patents, or copyrights, or trademarks, the first step is to forget the idea of lumping them together, and treat them as separate topics. The second step is to reject the narrow perspectives and simplistic picture the term "intellectual property" suggests. Consider each of these issues separately, in its fullness, and you have a chance of considering them well.

The entire business is being transacted on the Internet and the Internet has become commercial organization to promote this and their products. For this purpose, they need the domain name to identify on the Computers which they are using. It comprises of groups of alphanumeric characters separated by dots. It consists of Trade name or a Trading name identifying the nature and sometimes the location of the organization. Marks and Spencer have a number of domain names, like marks-and-spencer.com. It will enable us to have and e-mail address is the form of johnsmith@marks-and-spencer.co.uk and a web site address in the http.//www.marks-and-spencer.c.uk.

A Domain name is an identification label that defines a realm of administrative autonomy, authority, or control in the Internet, based on the Domain Name System (DNS)

As per the definition clause (zb) of the Trade Mark At,1999, the

"Trade mark" means a mark capable of being represented graphically and which is capable of distinguishing the goods or services of one person from those of others and may include shape of goods, their packaging and combination of colours; and-

(i) in relation to Chapter XII (other than section 107), a registered trade mark or a mark used in relation to goods or services for the purpose of indicating or so as to indicate a connection in the course of trade between the goods or services, as the case may be, and some person having the right as proprietor to use the mark; and

(ii) in relation to other provisions of this Act, a mark used or proposed to be used in relation to goods or services for the purpose of indicating or so to indicate a connection in the course of trade between the goods or services, as the case may be, and some person having the right, either as proprietor or by way of permitted user, to use the mark whether with or without any indication of the identity of that person, and includes a certification trade mark or collective mark;

Intellectual Property is the most important part of the modern business. Intellectual property which is a combination of copyright, trademark, design, geographical indication, patent, industrial design, integrated circuit, is valuable assets of any Company.

Domain names are often referred to simply as domains and domain name registrants are frequently referred to as domain owners, although domain name registration with a registrar does not confer any legal ownership of the domain name, only an exclusive right of use.

Domain names are the most important means of identification for companies and businesses on the Internet. A domain name which mirrors a company name is a valuable corporate asset because it facilitates communication with the company's customer base. However, domain names; have been allocated very much outside the constraints of intellectual property law and only recently have efforts been made to restrain the registration and use of legal problematic domain names.

Domain names can be termed as the Addresses of computers connected to the Internet e.g. street, city, name and country. This unique identification number is called the Internet protocol address. The letter sent by post requires addressed envelops, digital post also requires a suitable digital padded envelop in which the message is encoded and sent. Typing the domain name in a web browser would cause the system to look up the destination address where data will be sent.

A domain name is a term used by Internet user to instruct their computers to obtain the Internet protocol number of a desire website.

Now we come to the Domain Name System.

Internet Protocol addresses (IP addresses) are the devices which provide access to web sites. These are represented as strings of four numbers, the combination of which uniquely identifies and specifies the location of some interface on the Internet.

Because of the difficulty of remembering IP addresses, the Domain Name System was created to provide alpha-numeric substitutes for these starting of digits. Domain names are thus simply mnemonics which allow

Internet users to access web sites more conveniently and allow owners of web sites to distinguish their sites more easily.

How is the Domain Name System controlled?

To prevent duplication of Second Level Domains, one body must be responsible for the co-ordination of the Domain Name System. This body is the Internet Assigned Numbers Authority (IANA), which controls both the allocation of IP addresses and of domain names. This latter responsibility has been delegated to the Internet Network Information Center (Inter NIC) which has contracted with Network Solutions, Inc (NSI) to allocate names in the most important gTLDs.

Domain names are used in various networking context and application-specific naming and addressing purposes. They are organized in subordinate levels (sub domains) of the DNS root domain, which is nameless. The first-level set of domain names are the top-level domains (TLDs), including the generic top-level domains (gTLDs), such as the prominent domains com.net and org. and the country code top-level domains (cc TLDs).

Domain names are also used as simple identification labels to indicate ownership or control of a resource. Such examples are the realm identifiers used in the Session Initiation Protocol (SIP), the Domain Keys used to verify DNS domains in e-mail systems, and in many other Uniform Resource Identifiers (URIs).

Domain name identifies an Web site. For example, “Microsoft.com” Web site. A single Web server can serve Web sites for multiple domain point to only one machine. For example, Apple Computer has Web sites at WWW.info.apple.com, and store.apple.com. Each of these sites could be served. Then there are domain names that have been registered, but are not connect common reason for this is to have e-mail addresses at a certain domain name.

Brands are greatly affected by the ability of the company to obtain the matching domain name. If a company builds a brand around a name to which it does not own the domain name, it can end up directing traffic to another domain owner's site. If it is a competitor, this would be a problem.

The importance of the role played by domain names in establishing online identity, is highlighted by the practice of cyber squatting, and abusive practice whereby one entity registers a domain name that includes the name or trademark of another, often famous or well known, in order to either block the legitimate user some registering its most intuitive domain name or in hope of selling the names for profit on the market. The practice of **cyber squatting i.e.** (Cyber squatting is registering, trafficking in or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else) has resulted in litigation in various for a-one of the most famous examples being one in a million case (Marks & Spencer Plc. V.One in a Million,1998 FSR 265) the United Kingdom in which the court granted an injunction to prevent the cyber squatting on domain names involving well known brands such as Sainsbury, Mark and Spencer, and British Telecom. The prices commanded by these cyber pirates, illustrate the commercial value accorded to domain names, as an online business identifier- the domain name business.com was reputedly purchased for US $ 7.5 million.

The vexed question of the legal status of an Internet domain name has engaged many legal academics and practitioners since Joshua Quittner registered, without any proprietary interest, the domain name mcdonalds.com in July 1994. The literature analyzing this issue may be classified as falling within one of three categories. The first comprises analyses, which focus upon propertization of the domain name system (DNS) while neglecting any normative analysis of the proprietary nature of domain names. These direct their attention to particular instances where one party is in active dispute with another over a domain name. They

focus upon the tensions arising from the dichotomy between the international and unclassified nature of domain names as opposed to the domestic, classified nature of the trademark system.

The second category encompasses analyses which review the normative role of a domain name with regard to the underlying addressing system of the Internet. Such analyses generally view the key conflicts between the trademark system and the DNS as being centered upon the unique role of a domain name as both an addressing protocol and a `badge' or identifier.

The focus of the third category is the legal basis of domain names and the DNS. This nascent socio-legal analysis is most clearly exemplified by the work of Milton Mueller. He argues that `control of the DNS root is being used to create new and expanded (property) rights to names', and that these rights are 'often stronger than… traditional legal rights in names.

Conflict between Domain Names and Trade mark Law.

Many domain names are the names of companies, which in turn are often registered trade marks. The use of a trade mark within a domain name allows for the easiest means of identification of a company's business for an Internet user. Some Internet browsers allow users to find a company's home-page simply by typing in the name of the company or its trade mark, and the browser adds the rest of the URL. A short, easily identifiable domain name which `includes a company's trademark ... ensures that its promotions, information and commercial offerings are easy to find.' Thus domain names can be said to serve similar functions to trade marks.

However, domain names cannot necessarily be *equated* with trade marks because of the different purposes they serve. Trademarks are signs used to distinguish goods or services dealt with or provided in the course

of trade. They facilitate identification of the sources of merchandise and are important vehicles for the creation of business goodwill in relation to particular commodities. Domain names on the other hand serve multiple purposes - they are like `postal addresses, vanity license plates and billboards all rolled into one'. In many cases, domain names are mere electronic addresses for web sites, rather than signifiers which seek to distinguish goods and services.

The World Intellectual Property Organization has noted two areas where domain names may come into conflict with trademark law:

Domain name allocation, and

Trademark enforcement.

The most fundamental question raised by the current policies of domain name allocation is whether and in what circumstances a domain name can infringe a registered trademark. In most countries, a trademark will generally be infringed when another party uses a sign that is substantially identical with the registered trademark in relation to goods or services in respect of which the trademark is registered. Infringement of a trademark by its use in a domain name may arise in four circumstances, when a domain name containing another party's trademark is registered:

- for purely non-commercial use;
- in order to prevent a competitor from using that name;
- for commercial purposes, and;
- to be held for `ransom' with the expectation that the trade mark holder will pay to obtain the name (a practice known as `cyber-squatting').

The US and UK courts have applied traditional trademark law in respect of the first two circumstances. However, in the latter two circumstances, they have applied the concept of trademark dilution to protect the rights of trademarks owners.

In the year 1999 the word `Intellectual property organization drafting International standard have resolved disputes over domain name. Those standards became the basis for the Uniform disputes Resolution Policy on which the Internet administration body has based its own draft rules.

In short we can say **WIPO** i.e. World Intellectual Property Organization where number of complaints are being filed.

Let us understand **ICANN Policy**: Internet Corporation of Assigned names and Numbers

It is this one context that one ought to appreciate the birth of the Uniform Domain Name Dispute Resolution Policy (UDRP), a policy which was adopted by the Internet Corporation of Assigned names and Numbers (ICANN) on 24th of October, 1999. The policy offers an expedited administrative proceeding for trademark holders to contest "abusive registrations of domain names," and may result in the cancellation, suspension or transfer of a domain name by the registrar.

The Role of WIPO (World Intellectual Property Organization)

WIPO was approved as a dispute resolution service provider under ICANN's policy on December,1999. The fact that from December,1999, when WIPO was so approved, till the current date there are 700 cases that have been filed before WIPO, of which about 270 have been decided, goes to show the popularity of ICANN's streamlined procedure as well as WIPO's role as a dispute resolution service provider.

The Yahoo Case

One of the most significant cases in this regard has been the Yahoo case (Yahoo Inc. V. Akash Arora @ Anr., (199 PTC 201)) where the Internet search engine Yahoo Inc. sued an Internet pirate who had not only

copied the domain name Yahooindia.com but had used Yahooindia as a trademark in a similar script on its web site and by offering directory services with information specific to India, was passing itself off as an extension of yahoo. The defendant had further copied the contents of the plaintiff's Web Page and consequently the HTML Code (Hypertext mark-up language)

Protection under Indian law: an analysis of the "Yahoo" case:

The "YAHOO" case: YAHOO Inc. v.Akash Arora & Anr. (78 (1999) Delhi Law Times 285. Facts of the case can be summed in a line: the defendant installed a web; site- `Yahooindia.com' nearly identical to plaintiffs' renowned `Yahoo.com' and provided services similar to those of the plaintiff. The plaintiffs alleged passing off.

A trademark is a sign which can distinguish your goods and services from those of your competitors. It can be for example words, logos or a combination of both. You can use your trademark as a marketing tool so that customers can recognize your products or services.

A trademark must be distinctive for the goods and services you provide. In other words it can be recognized as a sign that differentiates your goods or service as different from someone else's.

Trade marks are not registrable if they

i) describe your goods or services or any characteristics of them, for example, marks which show the quality, quantity, purpose, value or geographical origin of your goods or services;

ii) have become customary in your line of trade;

iii) are not distinctive;

iv) are three dimensional shapes, if the shape is typical of the goods you are interested in (or part of them), has a function or adds value to the goods;

v) are specially protected emblems;

vi) are offensive;

vii) are against the law, for example, promoting illegal drugs; or;

viii) are deceptive. There should be nothing in the mark which would lead the public to think that your goods and services have a quality which they do not.

A trademark includes any word, name, symbol, or design, or any combination used, or intend to be used, in commerce to identify and distinguish the goods of one manufacturer or seller from goods manufactured or sold by others, and to indicate the source of the goods. In short, a trademark is a brand name.

A service mark is any word, name, symbol, design, or any combination, used, or intended to be used, in commerce, to identify and distinguish the services of one provider from the services provided by others, and to indicate the source of the services.

A trademark owner may sue for trademark infringement under federal or state laws, which are well settled in the United States Trademark infringement under the federal Lanham Act can occur if a domain name similar to a trademark is used without permission in a commercial sense and in a way that is likely to cause confusion mistake or deception. The US District Courts have the power to adjudicate disputes between trademark owners and

domain name registrants including the power to enjoin the use of a domain name and to direct its reassignment to a trademark owner. Under state law use of a domain name in a manner that causes confusion or dilution with a trademark may be a form of infringement.

The UK Company Names Tribunal has issued its first decision under Section 69 of the Companies Act,2006.

Section 69 of the UK's Companies Act,2006 allows a brand owner to make a complaint against a company name that appears to have been registered in order to take advantage of goodwill built up by an existing brand or trademark. Previously, it was possible to object to a registered company name only on the basis that it was too similar to another registered company name. The new regime allows a brand owner to object to a registered company name if it is (i) the same as that associated with the brand owner and in which the latter has goodwill, or (ii) sufficiently similar to such a name that its use in the UK is likely to mislead by suggesting a connection between the company and the brand owner.

Although the Coca-Cola decision was in essence a default judgment, IT demonstrates that the Act can be useful to brand owners by preventing "opportunistic" company name registrations.

Trademark is a branch of Intellectual Property Right. A trademark includes any word, name, symbol, or device, or any combination, used, or intended to be used, in commerce to identify and distinguish the goods of one manufacturer or seller from goods manufactured or sold by others, and to indicate the source of the goods. In short, a trademark is a brand name. Trademark is a mark

or symbol which capable of distinguishing the goods or services of one from those of others.

Trademark provides protection to the owner of the mark by ensuring the exclusive rights to use in to identify them or services or authorize another to use it in return of payment. It works like a weapon in the hand of registered proprietor or owner of the mark to stop other traders from unlawful use of the mark of the registered owner. Under Section 28 of the Act, the registration of a trademark shall give to the registered proprietor of the trademark, their exclusive right to the use of the mark in relation to the goods in respect of which the mark is registered and to…. Relief in respect of the trademark in the manner provided under the Act. The proprietor of a trademark has a right to file a suit for infringement of his right and obtain injunction, damages and account of profits.

Protection against infringement of Trade Mark:

Under Section 29 of the Trade mark Act,1999, the use of a trade mark by a person who not being registered person of the trade mark or a registered user thereof which is identical with, or deceptively similar to a registered trade mark amounts to the infringement of trademark and the registered proprietor can take action or obtain relief in respect of infringement of trademark. In a matter Supreme Court has held that in an action of infringement if the two marks identical, then the infringement made out, otherwise the Court

The protection of Domain names in Cyber space or it may be termed, as protection of Intellectual property on the Internet remains a grey area.

Domain Name related Trade mark Infringement and Jurisdiction

In Maritz, Inc. v.CyberGold, Inc, operator of a Web site based in California registering the domain name "cybergold.com" was sued by a Missouri company for trademark infringement. The defendant's Web site provided information about the company and solicited Internet users who wanted to be on its mailing list to provide names and particular areas of interest. The defendant would then provide a personal electronic mailbox and forward advertisements and other related information to the user that corresponded with the selected interests. Plaintiff argued that this provided a state-wide advertisement for the defendant and that through the Web site, the defendant was soliciting customers from Missouri.

The vexed question of the legal status of an Internet domain name has engaged many legal academics and practitioners since Joshua Quittner registered, without any prior proprietary interest, the domain name mcdonalds.com in July1994. The literature analyzing this issue may be classified as falling within one of three categories. The first comprises analyses which focus upon propertization of the domain name system (DNS) while neglecting any normative analysis of the proprietary nature of domain names. These direct their attention to particular instances where one party is in active dispute with another over a domain name. They focus upon the tensions arising from the dichotomy between the international and unclassified nature of domain names as opposed to the domestic, classified nature of the trademark system. These analyses fail, though, to question the normative basis of such

disputes and, in particular, the issue of whether a property right may be asserted over a domain name. The second category encompasses analyses which review the normative role of a domain name with regard to the underlying addressing system of the Internet. Such analyses generally view the key conflicts between the trademark system and the DNS as being centered upon the unique role of a domain name as both an addressing protocol and a `badge' or identifier. Rather than adopting the conflicting values approach characteristic of the first category, papers focusing on this aspect of domain naming generally direct their attention to the 'fit' between trademark law as developed in real-space and the use of domain names in the electronic realm. These commentaries differ from those in the first category as they address the normative basis of the DNS. Nevertheless, this second approach also neglects to give sufficient consideration to issues pertaining to property rights in domain names and propertization of the DNS.

The focus of the third category is the legal basis of domain names and the DNS.