Prof:Siddhesh Zele's

IPR
UNIT 1,2,3,4,5,6

TYBSC(IT) SEM 6

COMPILED BY
ILQA NARKAR

302 PARANJPE UDYOG BHAVAN, NEAR KHANDELWAL SWEETS, NEAR THANE STATION , THANE (WEST)

PHONE NO: 8097071144 / 8097071155 / 8655081002

UNIT 1

INTRODUCTION

Intellectual Property (IP) is a legal concept which refers to creations of the mind for which exclusive rights are recognized. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property rights include copyright, trademarks, patents, industrial design rights, and in some jurisdictions trade secrets.

Many of the legal principles governing intellectual property rights have evolved over centuries, it was not until the 19th century that the term intellectual property began to be used, and by 20th century it was the common place in the globe.

Intellectual property is something you create that's unique.

It includes copyright, patents, designs and trademarks, and can be:

- Something you manufacture, like a new product.
- A product's design or look.
- A brand or logo.
- Written work, like content on a website.
- Artistic work, like photography or illustrations.
- Film recordings or musical compositions.
- Computer software like applications.

You can't protect an idea - but you can often protect what you do with it.
For example, you can't protect an idea for a book. But if you write it, you can protect the words you've write.

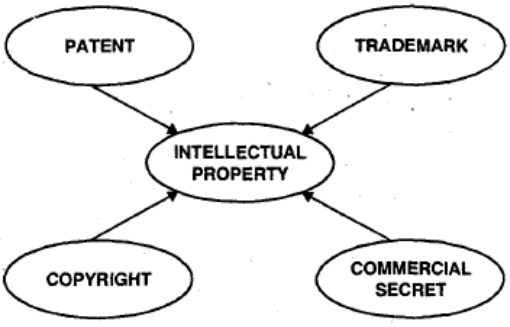

Fig. 1.1

Modern usage of the term intellectual property goes back at least as far as 1867 with the founding of the North German Confederation whose constitution granted legislative power over the protection of intellectual property (Schutz des geistigen Eigentums) to the confederation. When the administrative secretariats established by the Paris Convention (1883) and the Berne Convention (1886) merged in 1893, they located in Berne, and also adopted the term intellectual property in their new

combined title, the United International Bureaux for the Protection of l Intellectual Property.

The organisation subsequently relocated to Geneva in 1960, and was succeeded in 1967 with the establishment of the World Intellectual Property Organization (WIPO) by treaty as an agency of the United Nations. According to Lemley, it was only at this point that the term really began to be used in the United States (which had not been a party to the Berne Convention), and it did not enter popular usage until passage of the Bayh-Dole Act in 1980.

"The history of patents does not begin with inventions, but rather with royal grants by Queen Elizabeth I (1558-1603) for monopoly privileges..,. Approximately 200 years after the end of Elizabeth's reign, however, a patent represents a legal obtained by an inventor providing for exclusive control over the production and sale of his mechanical or scientific invention the evolution of patents from royal prerogative to common-law doctrine."

Types of IPR:

Common types of intellectual property rights include patents, copyright, industrial design rights, trademarks, trade dress, and in some jurisdictions trade secrets. There are also more specialized varieties i.e. exclusive rights, such as circuit design rights (called mask work rights in USA law, protected under the Integrated Circuit Topography Act in Canadian law, and in European Union law by Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products), plant breeders' rights, plant variety rights, industrial design rights, supplementary protection certificates for pharmaceutical products and database rights.

Protecting your Intellectual Property Rights:

Protecting your intellectual property allows you to:

- Stop others using what you've created without your permission.
- Charge others for the right to use what you created.

Getting the Right Type of Protection:
The type of protection you need depends on what you've created. For example, artistic works are protected by copyright, while inventions are protected by patents.

You can use more than one type of protection for the same product.

For example, you can patent your product and register its name as a trademark.

You can check which type of intellectual property protection best suits you and how to make the most of it by using the Intellectual Property Office's.

1.2 COPYRIGHT:

Copyright protects original:

- Literary and written work, like novels
- Dramatic, musical and artistic works and their performances.
- Television, film, sound and music recordings.
- Computer software.
- Illustration and photography.

You automatically get copyright protection when you create something original ^ you need not to register it.
But before making your work public, you should mark it with:

- The copyright symbol (©).
- The copyright holder's name.
- The year the work was created.

This gives you more protection, as it shows others that it's covered by copyright and who owns it.

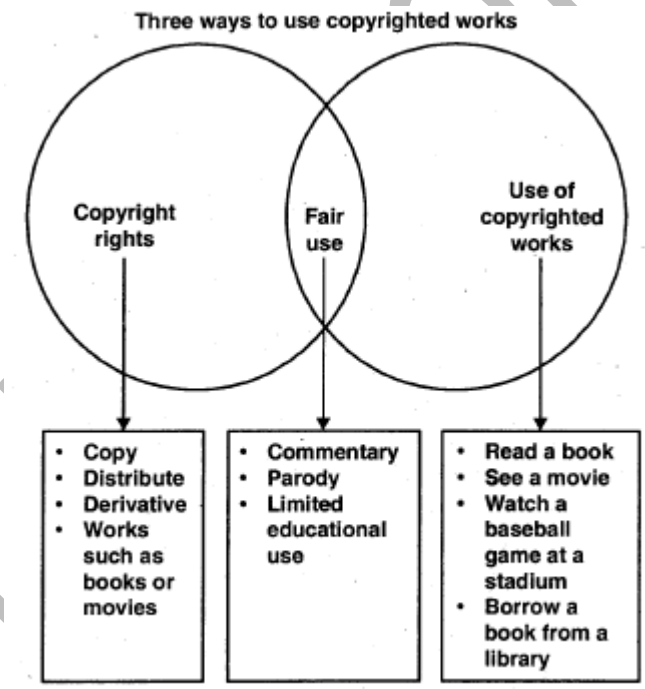

Fig. 1.2

Copyright is a legal concept, adopted by most governments, giving the creator of an original work exclusive rights to it, usually for a limited time, with the intention of enabling the creator of intellectual wealth (e.g. the photographer of a photograph or the author of a book) to get compensated for their work and be able to financially support themselves. Generally, it is "the right to copy", but also gives the copyright

holder the,right to be credited for the work, to determine who may adapt the work to other forms, who may perform the work, who may financially benefit from it, and other related rights. It is a form of j intellectual property (like the patent, trademark, and trade secret) applicable to any expressible form of an idea or data that is substantive and discrete.

Copyright initially was conceived as a way for government to restrict printing; the contemporary intent of copyright is to promote the creation of new works by giving authors control of and profit from them. Copyrights are said to be territorial, which means that they do not extend beyond the territoiy of a specific state unless that state is a party to an international agreement. Today, however, this is less relevant since most countries are parties to at least one such agreement. While many aspects of national copyright laws have been standardized through international copyright agreements, copyright laws of most countries have some unique features. Typically, the duration of copyright is the whole life of the creator plus fifty to a hundred years from the creator's death, or a finite period for anonymous or corporate creations. Some jurisdictions required formalities to establishing copyright, but most recognize copyright in any completed work, without any registration. Generally, copyright is - enforced as a civil matter, though some jurisdictions do apply criminal sanctions.

Most jurisdictions recognize copyright limitations, allowing "fair" exceptions to the creator's exclusivity of copyright, and give users certain rights. The ^development of digital media and computer network technologies have prompted reinterpretation of these exceptions, introduced new difficulties in enforcing copyright, and inspired additional challenges to copyright law's philosophic basis. Simultaneously, businesses with great economic dependence upon copyright have advocated the extension and expansion of their intellectual property rights, and sought additional legal and technological enforcement.

When your work is Protected by Copyright:

To be protected by copyright, your work must:

- Be original (you will need to be able to prove that you've made a significant creative contribution to it)
- Physically exist (it can't be just an idea)

Copyright in the UK lasts for the rest of the creator's life plus 70 years.

Copyright Overseas:

How long copyright lasts in these countries varies, but it's usually a minimum of 50 years (25 years for photographs).

1.3 DESIGN RIGHT:

Design right automatically protects the physical shape of something original that you design.

For example, if you design a vase with a unique shape, the design is automatically protected in the UK by design right.

Your design must be unique - the law says it can't be 'commonplace, everyday or ordinary'.

Design right doesn't cover any two-dimensional elements of a design, e.g. a pattern on a product's surface.

How Long Design Right Protection Lasts?

Design right protects your design in the UK until the earlier of:

- 15 years after the design was first created.
- 10 years after the design was first marketed and sold.

Automatic Protection for Designs:

A unique design you create in the UK will automatically become an 'unregistered community design'.

Unregistered community designs are protected across the EU for up to 3 years after you make the design public.

Unregistered community design also protects twodimensional elements to a design, like a decorative pattern on an object.

Getting Stronger Protection for Your Designs:

If anyone uses your design without permission, defending design right and unregistered community design can be difficult. You need to prove:

- Your work is original.
- You created it first.
- Any copying was deliberate.

For that you have to prove all these things, you can try to stop or reach an agreement with whoever's using your design without permission.

1.4 PATENTS:

You can protect something you've invented by patenting it. A patent registers your invention and stops anyone making, using or selling it without your permission.

What You Can and Can't Patent?

Your invention has to be:

- New.
- Inventive (not just an obvious modification to something that already exists).
- Something that can be made or used. Things you can't patent include:
- Literary, dramatic, musical or artistic works.
- Schemes, rules or methods (including medical treatment methods).
- Anything that's solely an idea (e.g. a way of thinking, a scientific or mathematical discovery).
- New types of plants, seeds or animals.
- The way information is presented

Registering a Patent in the UK:
Patent registrations can be complicated and are often handled by patent attorneys. It can take more than 4 years for a patent to be granted.

You can do it yourself - but mistakes in your application • could slow it down or mean you have to reapply.

A patent attorney can be expensive, but if you're not sure about the process, using one may save you money in the long term.

These are the basic steps to apply for a patent:

1. Prepare your patent application including a written description of your invention and legal statements that define its distinctive technical features.
2. Search for similar or identical patents.
3. File your application.
4. The Intellectual Property Office (IPO) will check your application and do its own search to make sure your invention doesn't already exist.
5. Your patent application is published by the IPO to give other people the chance to object.
6. Your application is granted or refused.

After your patent has been granted, you can licence it to other people or defend it against infringements.

How long a Patent Lasts?

A patent can last for 20 years from the date you ' apply for it. After you've held a patent for 4 years, you must renew it every year if you want to keep it.

Getting Patents Overseas:

A patent protects your invention in your own country where your patent is registered.

1.5 TRADEMARKS:

A trademark is a something that your brand known to everyone, like a logo or a sound.

Registering a trademark lets you stop other people from using it without your permission.

To register a trademark, it must be clearly different from any trademarks already registered for the same type of products or services.

A trademark registration lasts 10 years and is only valid in the country of registration. You can renew it every after 10 years.

Company and Domain names:

Company names and domain names aren't automatically trademarks. You register:

- Company names with Companies House.
- Domain names with domain name registrars.

Once you've done that, you may be able to register company or domain names as trademarks.

Registering a trademark in Use UK:

These are the basic steps:

1. Check that your brand qualifies as a trademark - you can't change it after it's registered.
2. Find out if an identical or similar trademark already exists - it's your responsibility to do a thorough search.
3. Register your trademark.
4. The Intellectual Property Office (IPO) will check your application.
5. Your application will be made public to give other people the chance to oppose it.
6. The IPO grants or refuses your trademark application.

A trademark attorney can help with searches and registrations.

After your trademark is granted it will be published in the IPO database and you 11 get a certificate.

The IPO doesn't police trademark infringement. If someone is using your trademark without permission, you 11 need to get them to stop.

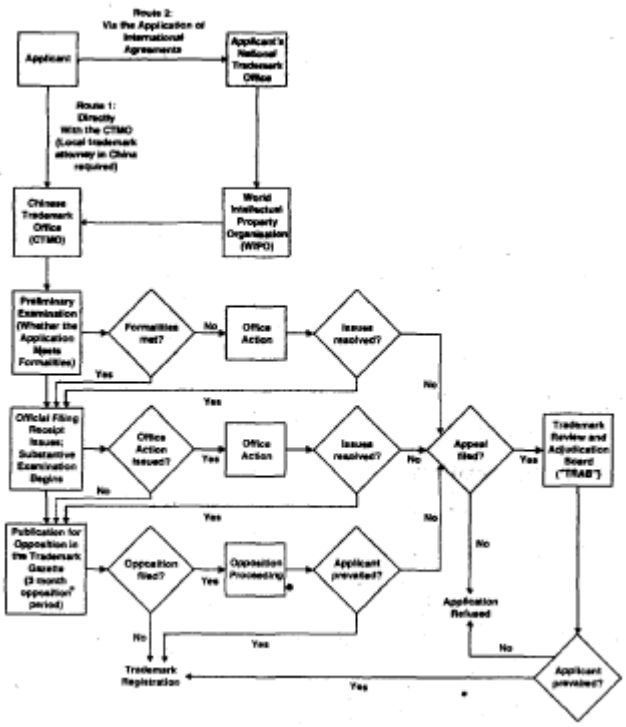

Fig. 1.3

1.6 RELATED RIGHTS:

The purpose of related rights is to protect the legal interests of certain persons and legal entities who contribute to making works available to the public; or who produce subject matter which, while not qualifying as works under the copyright systems of all countries, contain sufficient creativity or. technical and organizational skill to justify recognition of a copyright-like property right. The law of related rights deems that the productions which result from the $ activities of such persons and entities merit legal protection in themselves, as they are related to the protection of works of authorship under copyright. Some laws make clear, however, that the exercise of related rights should leave intact, and in no way affect, the protection of copyright.

Unfair Competition:

- What is “unfair competition”? “Any act of competition contrary to honest practices in industrial and commercial matters” - Paris Convention Art.
- UC, in principle, destroys the trust in the development of markets and products.
- “Honest practices”? To draw a line between what are, and what are not, honest practices, fa ir and unfair competition in industrial and commercial matters will depend on the circumstances of the case and the business approach proper to the country or region.
- Such practices include acts that:

- Create or are capable of creating confusion as to the enterprise, the goods or the industrial or commercial activity of a competitor;
- Formulate fa lse allegations in the course of trade so as to discredit the enterprise, the goods or the industrial or commercial activity of a competitor;
- Indications or allegations that in the course of trade are capable of misleading the public as to the nature, manufacturing process, characteristics, suitability for their purpose, or quantity of goods.

Protection against Unfair Competition:

- The repression of unfair competition along with patents, . utility models, trademarks, industrial designs and appellations of origin are the objects of industrial property protection.
- Acts of unfair competition prejudice competitors and harm consumers:
  - Competitors lose customers and market share = there is economic prejudice,
  - Consumers are misinformed and deceived = economic and personal prejudice (including health hazard).

UNIT 2

2.1 COMPUTER SOFTWARE AND INTELLECTUAL PROPERTY-OBJECTIVE:

The intellectual property protection of computer software has been highly debated at the national and international level. For example, in the European Union (EU), a draft Directive on the Patentability of Computer-implemented Inventions has been discussed in order to harmonize the interpretation of the national patentability requirements for computer softwarerelated inventions, including the business methods carried out via the computer. Such type of discussions show various views among stakeholders in Europe. Furthermore, the Internet raises -complex issues regarding the enforcement of patents, as patent protection is provided on a country-by-country basis, and the patent law of every country will effect in its own boundaries.

IT will not clear all the questions and uncertainties of software patents but rather provide five tips or suggestions which should be kept in mind when considering patent protection of software-related inventions.

Copyright Protection:

In many countries, computer programs, are protected under copyright. The major advantage of copyright protection lies in its simplicity. Copyright protection does not depend on any formalities such as registration, the deposit of copies in the 151 countries party to the Berne Convention for the Protection of Literary and Artistic Works. This means that international copyright protection is automatic - it i begins as soon as a work is created. Although a copyright owner enjoys a relatively long period of protection, which lasts, in general, for the life of the author plus 50 or, in certain countries, 70 years after the author's death.

Question is that many people seek to patent their software-related inventions Why? The answers is manifold. But one of the strongest reasons is that copyright protection extends only to expressions, and not to ideas, procedures, methods of operation or mathematical concepts. Although copyright protects the "literal expression" of computer programs, it does not protect the "ideas" underlying the computer program, which often have considerable commercial value.

Reproducing:

Software may be incorporated in a computer , such as a household appliance or a car. But often, such software is created, reproduced and distributed on media (such as diskettes, CD-ROMs or an online network) which are separate from the hardware. Software may provide technical functions, such as controlling a machine or regulating the room temperature. It ' may be used to monitor communication network systems or provide interfaces between a computer and a human being. Or, it may be used to process scientific, financial, economic or social data in order to, for example, explore a new scientific theory or seek the highest possible return on an investment.

Depending on how the software is used together with the hardware, what you wish to protect from your competitor may differ. The core part of your software related innovation may lie in an apparatus, a system,, an algorithm, a method, a network, the processing of data or the software itself.

Patent Protection:

In many countries, any inventions of softwares are patentable subject to if they have a technical character or involve technical teaching, i.e., an instruction addressed to a person skilled in the art on how to solve a particular technical problem using particular technical means, it is necessary to examine whether the conditions of patentability are fulfilled.

In contrast, a patent must be applied for, in principle, in each country in which you seek patent protection. In order to enjoy patent protection, an application for a patent shall comply with both formal and substantive requirements, and a patented invention shall be disclosed to the public. These requirements can be legally and technically complex,- and their compliance often requires a legal expert's assistance. Compared with copyright protection, the term of protection is much shorter, namely, in general, 20 years from the filing date of the application.

However, due to the complex requirements for the grant of patents, the costs for obtaining and enforcing a patent may be costly. Unless you have important financial resources, it may be worth considering whether patenting your software-related innovation is the test way to protect your product. The simple way of using other types of intellectual property, such as trademarks, industrial designs and trade secret protection may also be considered.

Database:

To store the protected works in computer memories is a reproduction which falls within the right of reproduction. Another question is, whether databases as such enjoy protection under copyright.

Article 2(5) of the Berne Convention provides as follows: "Collections of literary and artistic works such as encyclopedias and anthologies which, by reason of the selection and arrangements of their contents, constitute intellectual creations shall be protected as such, without prejudice to the copyright in each of the works forming part of such collections." The provision does not indicate any specific category of works to which the level of protection shall be assimilated. Accordingly, it should be assumed that the level of protection to be granted is that which, in general, is granted to literary and artistic works under the Berne Convention.

The WCT contains in its Article 5 a provision on copyright protection of databases, which, under the title "compilations of Data (Databases)" provides as follows: "Compilations of data or other material, in any form, which by reason of the selection

or arrangement of their contents constitute intellectual creations, are protected as such. The Diplomatic Conference which adapted the WCT also adopted, by consensus,, the following agreed statement: “The scope of protection for compilations of data (databases) under Article 5 of this Treaty, read with Article 2, is consistent with Article 2. of the Berne Convention and on a par with the relevant provisions of the TRIPS Agreement.” Article 2 of the WCT, to which the agreed statement refers, states, under the heading “Scope of Copyright Protection”: “copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.”

2.2 DATA PROTECTION:

Data Protection it is the most important tasks faced by any business personnel. Your data can be in different formats and saved on different media - paper, files or a database.. No matter where your data resides or in what format your data is, you have to protect it. This article discusses digital data protection – data Stored in any digital format and on any digital medium. Data protection has to be well thought strategy including hardware and software redundancy, data backup, and data security.

The hardware redundancy is the first step in protecting your data. You can make your applications and data highly available by using clustering and server load balancing. Hardware or software RAID will help you protect your data from hard disk failure.

Data backup should be critical part of your overall data protection strategy. You need data backups in order to restore the protected data in case it is damaged or irrestorable. There are many software data backup solutions, which will help you protect your data. Some examples of data backup software are Norton Ghost, Handy Backup, Backup MyPC, and Data Protection Manager from Microsoft. Data backup software capabilities vary greatly between vendors and particular products.

Another part of your data protection plan should be securing the data, protection from unauthorized access. With the help of access control policies we can protect the data in operating system, Another option for securing your data is encrypting the data. You can install hardware or software firewall to protect your system and data from unauthorized access. You can install anti virus software to protect your system from viruses and prevent data damage and loss. You should control the physical access to your server room and/or data center.

Data protection should be part of the overall IT strategy of any business.

Data Protection Act 1998:

“An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information”. [16th July 1998] Be it enacted by the Queen’s most Excellent Majesty,

by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same.

The Data Protection Act 1998 ("the Act") gives effect in the UK law to EC Directive 95/46/EC (the "Directive"). The Act replaces the Data Protection Act 1984 (the "1984 Act") and was brought into force on 1 March 2000. There are, however, two transitional periods, the first of which expires on 24 October 2001 and the second of which expires on 24 October 2007, which provide that the processing of certain personal data does not become fully subject to the Act until these dates. Subordinate legislation came into force on or after 1 March 2000 and a full schedule of the relevant Statutory Instruments can be found at the end of this publication. For ease of reference, throughout the text, the full title and number of each Statutory Instrument ("S.I.") is provided.

This publication provides a broad guide to the Act as a whole. Whereas, an indication of the view of the Commissioner as to how certain provisions of the Act should be interpreted has been included and in some cases this may only involve reiterating guidance established under the previous legislation.

The Act uses some familiar and some unfamiliar words and phrases. It is particularly important to review the meaning of the familiar words and phrases as, under the Act, their definitions differ from those used in the 1984 Act.

There are eight Data Protection Principles (the "Principles") in the Act. Except to the extent that any data controller is able to claim an exemption from any one or all of them (whether on a transitional or outright basis), all of the Principles apply to all data controllers who must comply with them.

The Act gives legal rights to individuals (data subjects) in respect of personal data processed about them by others.

Data Protection Principles:

1. Personal data shall be processed fairly and lawfully and, shall not be processed unless.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner for those purposes.

    a. at least one of the conditions in Schedule 2 is met, and
    b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
    c. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

3. Personal data shall be accurate and it should be up to date.

4. Personal data processed for any purpose shall not % be kept for longer than is necessary for that purpose or those purposes.
5. personal data shall be processed in accordance with the rights of data subjects (individuals).
6. Appropriate technical and organisational measures should be taken against unauthorised processing of personal data and against accidental loss or destruction or damage to, personal data.
7. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory, ensures an adequate level of protection for the rights and freedoms of data . subjects in relation to the processing of personal data.

US Safe Harbor Principle:

US-EU Safe Harbor is a streamlined process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data.

Intended for organizations within the EU or US that store customer data, the Safe Harbor Principles are designed to prevent accidental information disclosure or loss. US companies can opt into the program as long as they adhere to the 7 principles outlined in the Directive.

The process was developed by the US Department of Commerce in consultation with the EU.

These principles must provide:

- Notice: Individuals must be informed that their data is being collected and about how it will be used.
- Choice: Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- Onward Transfer: Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- Security: Reasonable efforts must be made to prevent loss of collected information.
- Data integrity: Data must be relevant and reliable for the purpose it was collected for.
- Access: Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- Enforcement: There must be effective means of enforcing these rules.

Enforcement:

The Enforcement Acts were three bills passed by the United States Congress between 1870 and 1871. They were criminal codes which protected blacks' right to vote, to hold office, to serve on juries, and receive equal protection of laws. These

acts were passed following the ratification of the Fourteenth Amendment to the U.S. Constitution, which gave full citizenship to anyone born in the United States or freed slaves, and the Fifteenth Amendment, which banned racial discrimination in voting. At the time, the lives of all newly freed slaves, and their political and economic rights were being threatened. This threat led to the creation of the Enforcement Acts.

The section from the Enforcement Act of 1870 states that every person despite race, color, or previous condition of servitude must be granted equal opportunity to become qualified to vote. If any person or government official fails to recognize this as the law, there will be a minimum fine of five hundred dollars, and at the discretion of the court, could be sentenced to jail for a period of one month up to one year.

The Enforcement Act of 1871 (formally, “an Act to enforce the rights of citizens of the United States to vote in the several states of this union”), permitted federal oversight of local and state elections if any two citizens in a town with more than twenty thousand inhabitants desired it.

The Enforcement Act of 1871 (second act) and the Civil Rights Act of 1875 are very similar to the original act as they all have the same goal, but revised first act with the intention of being more effective. The final act, and the most effective, was also a revision. Although the fines lowered again, and the prison sentences remained approximately the same, this act was the best enforced by the government.

2.3 PROTECTION OF SEMI-CONDUCTOR CHIPS:

The Semiconductor Chip Protection Act of 1984 (or SCPA) is an act of the US Congress that makes the layouts of integrated circuits legally protected upon registration, and hence illegal to copy without permission.

The SCPA uses a modified copyright approach to protect the topography of integrated circuits against copying. There is no patent-like examination process; the “mask work” is registered with the Copyright Office. However, the SCPA has a novelty standard somewhat higher than the mere “originality” standard of copyright law: protection is not available for a mask work that "consists of designs that arc staple, commonplace, or familiar in the semiconductor industry or variations of such designs, combined in a way that, considered as a whole, is not original.

The Act provides for a 10-year term of protection. The bundle of rights is also somewhat different from that granted under copyright law, and copies of the “mask work” made in the course of reverse engineering are not infringing, in spite of proof of unauthorized copying and striking similarity, so long as the resulting semiconductor chip product was the result of study and analysis and contained technological improvement.

The SCPA provides for remedies similar to those " associated with copyright protection, does not allow for criminal penalties, and maintains a higher limit on statutory damages than that provided for in the Copyright Act.

2.4 WIPO TREATY:

The World Intellectual Property Organization Copyright Treaty, (WIPO Copyright Treaty or WCT), is an international treaty on copyright law adopted by the member states of the World Intellectual Property Organization (WIPO) in 1996. Additional protections for copyright deemed necessary due to advances in information technology since the formation of previous copyright treaties before it. The computer programs are protected as literary works, and that the arrangement and selection of material in databases is protected. It provides authors of works with control iover their rental and distribution in which they may not have under the Berne Convention alone. It also : prohibits circumvention of technological measures for ' the protection of works and unauthorized modification of rights management information contained in works.

There have been a variety of criticisms of this treaty, including that it is too broad (for example in its prohibition of circumvention of technical protection measures, even where such circumvention is used in the pursuit , of legal and fair use rights) and that it applies a 'one size fits all' standard to all signatory countries despite widely differing stages of economic development and knowledge industry.

2.5 TRIPs:

The Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) is an international agreement administered by the World Trade Organization (WTO) that sets down minimum standards for many forms of intellectual property (IP) regulation as applied to nationals of other WTO Members. It was negotiated at the end of the Uruguay Round of the General Agreement on Tariffs and Trade (GATT) in 1994.

The TRIPS agreement introduced intellectual property law into the international trading system for the first time and remains the most comprehensive international agreement on intellectual property to date. In 2001, developing countries, concerned that developed countries were insisting on ah overly narrow reading of TRIPS, that resulted in the Doha Declaration. The Doha declaration is a WTO statement that clarifies the scope of TRIPS, stating for example that TRIPS can and should be interpreted in light of the goal "to promote access to medicines for all."

TRIPS requires WTO members to provide copyright rights, covering content producers including performers, producers of sound recordings and broadcasting organizations; geographical indications, including appellations of origin; industrial designs; integrated circuit layout-designs; patents; new plant varieties; trademarks; trade dress; and undisclosed or confidential information. TRIPS also specifies enforcement procedures, remedies, and dispute resolution procedures. Protection and enforcement of all intellectual property rights shall meet the objectives to contribute to the

promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations.

2.6 SCPA:

The School for Creative and Performing Arts (SCPA) is a magnet arts school in Cincinnati, Ohio, United States, and part of the Cincinnati Public Schools (CPS). SCPA was founded in 1973 as one of the first magnet schools in Cincinnati and became the first school in the country to combine a full range of arts studies with a complete college-preparatory academic program for elementary through high school students. Of the approximately 350 arts schools in the United States, SCPA is one of the oldest and has been cited as a model for both racial integration and for arts programs in over 100 cities.

SCPA had three different homes in its first four years, including a makeshift campus in the Mount Adams neighborhood and another in Roselawn. In 1976, it occupied the Old Woodward High School building, on the site of one of the oldest public schools in the country. The school rose to national prominence in the 1980s, but was nearly closed in the 1990s following a series of scandals, leadership struggles, and an arson fire which destroyed the auditorium. Its reputation recovered in the years that followed and in 2009-10, the school was featured in the MTV reality series Taking the Stage, filmed at the school and featuring SCPA students. In 2010 SCPA combined with the Schiel Primary School for Arts Enrichment to create the first kindergarten through twelfth grade (about ages five to seventeen) arts school and first private sector/public arts school in the US. A new facility in Over-the-Rhine was championed by the late Cincinnati Pops Maestro Erich Kunzel and funded through a unique public-private partnership that raised over $31 million in private contributions to match public funding. The building features specialized facilities for the arts and three separate theaters and is the key to redevelopment plans for the area.

Students must audition for admission; fewer than 20 percent of those who apply each year are accepted. SCPA is free to CPS students but also attracts tuitionpaying students from outside the district and the * state. The newly combined school will serve approximately 1,300 students in 2010, offering a curriculum designed to prepare students for professional careers in creative writing, dance, drama, music, technical theater, and visual art. The emphasis is on performance, and students in every field are required to perform or present their work in public regularly. Students compete successfully in arts competitions locally and internationally. On standardized tests, SCPA ranks second among Cincinnati public schools. Ninety percent of graduating seniors continue on to college, and those students receive one of the highest levels of scholarship funding in the city. A limited number of extracurricular activities are offered, as students are expected to commit significant after-school time to training

and performance. SCPA has produced notable graduates in a wide range of artistic fields, including award-winning actors, singers, directors and technicians.

2.7 DOMAIN NAME PROTECTION:

Most businesses consider their domain name one of their most valuable assets. Indeed, the first contact many consumers have with a particular business is through the company Web site. Critically, domain names enable consumers and potential customers to quickly and easily connect with a particular business over the Internet.

To assist clients in policing their intellectual property on the Internet, MBHB attorneys regularly set up watch services to identify potentially adverse domain names and trademark uses. These services periodically search for identical or confusing domain names (and other trademark uses) and provide information regarding the registrant. By proactively identifying potentially adverse domain names, we often successfully resolve domain name disputes with a carefully worded letter to a registrant.

Other cases require resort to the courts or to other proceedings. Below is an overview and comparison of four methods for resolving domain name disputes: ICANN anticybersquatting proceedings, the Anticybersquatting Consumer Protection Act, the Lanham Act, and the Federal Trademark Dilution Act. ICANN provides the simplest and quickest method of resolving domain name disputes, but is limited in its available remedies.

Domain Name and Intellectual Property:

A domain name is a name by which a company or organization is known on the Internet. It usually incorporates the company name, or other identifier.

To register a domain name you must apply to an accredited Registrar.

A list of accredited and accreditation-qualified Registrars can be found on the ICANN (Internet Corporation for Assigned Names and Numbers).

Being the owner of a registered trade mark, does not automatically entitle you to use that mark as a domain name. The main reason being, that the same trade mark can be registered for different goods or services and by different proprietors. Also, someone may have already, and quite legitimately, registered the domain name, perhaps with its use being connected with unregistered goods or services.

The opposite also applies, if your domain name has been properly registered, it does not automatically follow that a similar trade mark will satisfy the requirements for trade mark registration, and/or it may be confusingly similar to someone else's earlier trade mark.

If you feel that a domain name has been registered unlawfully or maliciously we suggest that you take appropriate legal advice. Alternatively, you can get advice from Nominet UK who also offer a Dispute Resolution Service.

There are other dispute resolution procedures operated by, for example, the World Intellectual Property Organization (WIPO) Arbitration and Mediation Center.

There are other dispute resolution procedures operated by, for example, the World Intellectual Property Organization (WIPO) Arbitration and Mediation Center.

Registration of Domain Names:

Registering a proper domain name is essential for creating the right online identity. Although there will be many names and combinations of phrases coming into your mind for the same, it is essential to follow certain guidelines and steps to register one that works for your website. Listed below are the steps to be followed for registering a domain name.

- **Choosing a domain name:** Think of several domain names which you would like to use. It is no use thinking of only one as it might be already taken.
- **Paying for tire domain name:** Domain names can be either free or paid. You will need either a credit card or a PayPal account to pay for the domain. This is a requirement of most registrars. It will allow you to claim and get the domain name immediately after applying.
- Web hosting: It is a type of Internet hosting service allowing individuals and organizations to upload their own website on the World Wide Web. If you already have a web host, obtain from them the names of their primary and secondary name servers. This information is needed to point your domain name to your website after you buy it. In case, you do not have a web host, you can always ask the registrar to park your domain name at a temporary website specially set up for you. In this way, you can quickly secure your domain name and still take your time in setting up the other aspects of your site.

There are numerous domain name registrars. In addition, a number of commercial web hosts will give you a free domain name if you are hosting with them, as will many (if not all) of the registrars above. Once you decide on a domain name, do not procrastinate as there is a chance of losing a perfectly good one.

2.8 DISPUTES UNDER INTELLECTUAL PROPERTY RIGHTS:

This dispute resolution mechanism has been incorporated into the new GTLDs process to safeguard the interests of brand, trademark and other rights holders. Any objection by a right holder would be analysed by a pre defined and qualified panel of experts in the relevant subject area. Further, even dispute resolution service providers

have also been notified by ICANN and all disputes would be referred to these providers alone.

Objection can be filed in the categories of String Confusion, Legal Rights Objections, Limited Public Interest and Community. If you want to file a formal objection to a new GTLD application, you must contact , the appropriate dispute resolution service provider and file your objection electronically. The language to be used is English. If your objection falls in different categories, you have to file each objection separately and pay the accompanying filing fees for each.

While filing such objection(s), you must add your name and contact information as the objector along with a statement as to why you believe you meet the standing requirements. Further, a description of the basis for your objection must be given that must include a statement giving the grounds on which you are objecting and a detailed explanation of the validity of your objection and why it should be upheld. Do not forget to add copied of relevant documents that support your objection. Objections are limited to 5000 words or 20 pages, which ever is less.

You may also be on the receiving end. You may have to defend the objections raised by others against your new GTLDs applications. Within thirty days of the closing of the objections filing window, ICANN will post a Dispute Announcement and notify the providers to begin the objection proceedings. If you are an applicant and have received notice from a provider that you have had an objection filed against your application, you will have 30 calendar days to file your response. If you do not respond within 30 days, you will be in default and the objector will prevail.

If your application has been objected to, you can work to reach a settlement with the objector. This would result in either a withdrawal of the objection or a withdrawal of your new GTLD application. You can also file a response to the objection and enter the dispute resolution process. You can withdraw your new GTLD application, in which case the objector will prevail by default and your application will not proceed.

2.9 JURISDICTIONAL ISSUES:

Jurisdiction (from the Latin ius, iuris meaning “law” and dicere meaning “to speak”) is the practical authority granted to a formally constituted legal body or to a political leader to deal with and make pronouncements on legal matters and, by implication, to administer justice within a defined area of responsibility. The term is also used to denote the geographical area or subject-matter to which such authority applies.

Jurisdiction draws its substance from public international law, conflict of laws, constitutional law and the powers of the executive and legislative branches of government to allocate resources to best serve the needs of its native society.

The Jurisdiction between and within States:

This concerns the relationships both between courts in different jurisdictions, and between courts within the same jurisdiction. The usual legal doctrine under which questions of jurisdiction are decided is termed forum non conveniens.

International:

To deal with the issue of forum shopping, states are urged to adopt more positive rules on conflict of laws. The Hague Conference and other international bodies have made recommendations on jurisdictional matters, but litigants with the encouragement of lawyers on a contingent fee continue to shop for forums.

Supranational:

At a level, countries have adopted a range of treaty and conventions obligations to relate the right of individual litigants to invoke the jurisdiction of state courts and to enforce the judgments obtained. For example, the member states of the EEC signed the Brussels Convention in 1968 and, subject to amendments as new states joined, it represents the default law for all twenty-seven Member States of what is now termed the European Union on the relationships between the courts in the different countries. In addition, the Lugano Convention (1988)* binds the European Union and the European Free Trade Association.

In effect from 1 March 2002, all the member states of the EU except Denmark accepted Council Regulation (EC) 44/2001, which makes major changes to the Brussels Convention and is directly effective in the member states. Council Regulation (EC) 44/2001 now also applies as between the rest of the EU Member States and Denmark due to an agreement reached between the European Community and Denmark. [2] In some legal areas, at least, the CACA enforcement of foreign judgments is now more straightforward. At a state level, the traditional rules still determine jurisdiction over persons who are not domiciled or habitually resident in the European Union or the Lugano area.

National:

Many nations are subdivided into states and provinces (i.e. a subnational “state”). Federation (as can be found in Australia, States of Brazil, India, Mexico and the United States) and these subunits will exercise jurisdiction through the court systems as defined by the executives and legislatures.

When the jurisdictions of governmental entities overlap, one another - for example, between a state and fee federation to which it belongs - their jurisdiction is shared or concurrent jurisdiction.

Otherwise, one government entity will have exclusive jurisdiction owner that shared area. When jurisdiction is concurrent,- one governmental entity raiay have supreme

jurisdiction over the other entity if their laws conflict. If the executive or legislative powers mthin the jurisdiction are hot restricted or restricted dnly fey a number of limited restrictions, these government branches have plenary power such as a national policing power. Otherwise, an enabling act grants only limited or enumerated powers.

The problem of forum shopping also applies as between federal and state courts.

UNIT 3

Patent(Ownership and enforcement Intellectual Property)

Patent is a monopoly right granted by the State to an inventor for a limited period, in respect of the invention, to the exclusion of all others. A system of patents serves many useful purposes. If the invention is commercially utilized, the patent ensures just reward in terms of money and recognition for the inventor, for all the time and effort, knowledge and skills, money and other resources invested to come up with the invention. For the society, commercial exploitation of an invention means newer and better products, higher productivity, and more efficient means of production. The main objective of patent include worked together and further research and development made inside the country. A patent system encourages technological innovation and dissemination of technology. This in turn stimulates growth and helps the spread of prosperity and better utilization of resources. In an age when technology and knowledge are the greatest generators of wealth, the number of patents filed and granted nationally and internationally is a good indicator of the health of science and technology in a country. Patent is granted by a State and hence has territorial applicability. That is, it is valid only in the country, which grants the patent. The patent mechanism is not global means it is not the same all over the world and you have to apply separately in all the countries where you want the invention to be protected.

3.1 OBJECTIVES:

- After studying this unit, you should be able to:
- recognize the patentable inventions;
- understand the inventions which cannot be the subject-matter of patents and the reasons thereof;
- understand the meaning of specifications;
- there are many step included in patent processing;
- spell out the acts which amount to infringement of patent; and
- understand the procedure for getting the relief in case of infringement of patent.

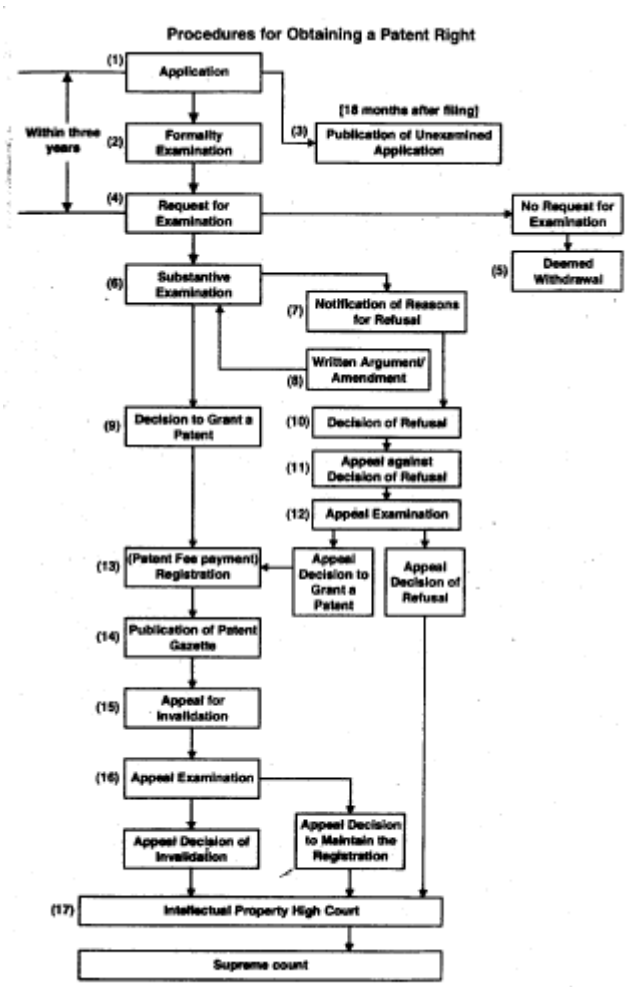

Fig. 3.1

3.2 RIGHTS OF A PATENTEE:

(1) Right to exploit the patent:

If the invention is a product, the patent confers the exclusive right to make, use, sell or import for these purposes, the invention in India. If the patent is for a method or process of manufacturing an article or substance, it confers the exclusive right to use or exercise the method or process in India. The patentee has the right to prevent third parties, from exploiting the patented invention in any such manner without the consent of the patentee. The term of every patent granted under the IPA is twenty years from the date of filing of the application for the patent. This includes the patents, which had not expired when the IPA came into force i.e. on May 20, 2003. It is necessary to renew the patent annually on payment of fee for it to remain valid throughout its term of 20 years. Failure to renew the patent results in loss of all patent rights.

(2) Right to grant licence etc.:

To enter into another arrangement for a consideration we need patentee power to assign licenses. A licence or an assignment to be valid must be in writing and registered with the Controller of Patents right to surrender.

The patentee is given the right to surrender the patent at any time by giving notice in the prescribed manner to the Controller. The Controller, before accepting the offer of surrender will advertise the same so as to give an opportunity to the interested parties to oppose the offer of surrender. The controller has all the rights.

(3) Right to sue for infringement:

A patentee is given the right to institute proceedings for infringement of the patent in a District Court having jurisdiction to try the suit.

Limitations on Patentee's Rights:

There are certain limitations on the rights of the patentee. They are as follows:

- Any patented product or process or a product made using patented process may be used by or on behalf of the Government for its own use only - all invention are used for purpose of government, used, exercised or vended for the purposes of the Central Government, State Government or a Government undertaking;
- A patented article or article made by use of patented process may be used by any person for experiment, research or for imparting instructions to pupils; and
- In case of a patent in respect of any medicine or drug, the medicine or drug may be imported by the Government for its own use or for distribution in any dispensary, hospital or other medical institution maintained by or on behalf of the Government.

3.3 ASSIGNMENT:

An assignment means transfer of interest in the patent by the patentee to another person in whole or in part valid over entire or a part of India. There are two types of people assignee and assignor. Assignee means the person whom the rights in patent to assign and assignor is the person who assign the rights.

There are three kinds of assignment:

Legal Assignment:

When the assignor assigns the right in a patent through an agreement duly registered, the assignment is called a legal assignment and the assignee's name will be entered in the Register of Patents maintained by the Patent Office as the proprietor of the patent. The legal assignee have all the rights.

Equitable Assignment:

When the patentee agrees to give another person certain defined right in the patent with immediate effect, by a document (e.g. a letter), and not by an agreement, the assignment is termed as an equitable assignment. However, such an assignment cannot be. registered in the Register of Patents. The assignee have the rights to change equitable assignment to legal assignment by getting the document in writing and getting it duly registered.

Mortgage:

When the patentee transfers the patent rights either wholly or in part to the mortgagee to secure a specified sum of money, such assignment is called mortgage. The patentee can get the patent re-transferred on refund of the consideration money.

Patent Assignment Instructions:

The following provision-by-provision instructions will help you understand the terms of your assignment. The numbers and letters below (e.g., Section 1, Section 2(a), etc.) correspond to the provisions in the agreement. Please review the entire document before starting your step-by-step process.

- Introduction of Parties: The following entries should be clarified that is Identifies the document as a patent assignment. Write in the date on which the agreement is signed. Identify the parties and, if applicable, what type of organization(s) they are. Note that each party is given a name (e.g., "Assignor") that will be used throughout the agreement. The Assignor is the party that is giving ("assigning") its ownership interest and the Assignee is the party receiving it.
- Recitals: The "whereas" clauses, referred to as recitals, define the world of the assignment and offer key background information about the parties. In this agreement, the recitals include a simple statement of the intent to transfer rights in the patent. Remember that the Assignor can transfer all or part of its interest in the Patents. If the entire property is being transferred, use the word "all." If only part of an Invention or Patent is being transferred, specify the amount being assigned (e.g., one-half, one-quarter, etc.).

Section 1: Assignment of Patents. This constitutes the assignment and acceptance of the assignment of the Patents and Inventions. Note that the property being assigned is not described in the agreement itself. The description located on the schedule should be assignment references "Schedule 1". Be as complete and clear as possible in your description of the property being transferred.

Section 2: Consideration. In most agreements, each party is expected to do something. This obligation may be to perform a service, transfer ownership of

property, or pay money. In this case, the Assignee is giving money (sometimes called "consideration") to receive the Assignor's property. Enter the amount to be paid, and indicate how long the Assignee has to make that payment after the agreement is signed

Section 3: Authorization to Director. The Assignor's authorization to issue any Patents in the Assignee's name. In other words the assignee tells the head of the USPTO that the transfer is valid and that ! ownership is changing hands by virtue of the Assignment. The bracketed last sentence is only j applicable if the assignment is being recorded before a patent application number has been issued by the USPTO. It allows this application number to be written in after the assignment is recorded. If the applications have already been filed, and there have been application numbers issued, delete this bracketed sentence.

Section 4: Assignor's Representations and Warranties. The Assignor's promises about the property being sold. More specifically, the Assignor is swearing that:

4(a): it is the sole owner of the Inventions and the Patents. If there are other owners who are not transferring their interests, use the bracketed phrase. This means that the only part being transferred is the Assignor's part.

4(b): it has not sold or transferred the Inventions and the Patents to any third party.

4(c): Assignor have the authority to enter into another agreement.

4(d): does not believe that the Inventions and the Patents have been taken from any third party without authorization (e.g., a knowing copy of another company's invention).

4(e): does not know of any permissions that have to be obtained in order for the assignment to be completed. In other words, once the agreement is signed, the assignment will be effective without anyone else's input.

4(f): the Patents weren't created while the creator was employed by a third party. In many cases, if an individual was employed by a company and came up with a product, the company will own that product. This section offers assurance to the Assignee that there are no companies that will make that claim about the Patents being sold. You can also add additional representation and warranties.

Section 5: Assignee's Representations and Warranties. The Assignee's promises about the transaction. More specifically, the Assignee is swearing that it:

5(a): has the authority to enter the agreement.

5(b): has enough funds to pay for the assignment.

Section 6: No Early Assignment. Prevents the Assignee from re-transferring the inventions or patents, or using any of them as collateral for loans, until it has made complete payment of the money due under the agreement.

Section 7: Documentation. The Assignor's promise to help with any paperwork needed to complete an assignment (e.g., filing information about the assignment with the USPTO and transferring document titles). The bracketed phrases make the additional promise that the Assignor will help with transfer paperwork for filings outside of the country. If this is not relevant to your agreement, delete the bracketed phrases.

Section 8: No Further Use o f Inventions or Patents. Indicates that after the effective date of the agreement, the Assignor will stop using aQ of. the inventions and patents being transferred and will not challenge the Assignee's use of those inventions or patents.

Section 9: Indemnification. A description of each party's future obligations, if the patent or any application is found to infringe on a third party's rights. There are two options provided, and you should choose the one that best fits with your situation. In the first, the Assignor takes all responsibility for infringement, promising to pay all expenses and costs relating to the claim. In the second, the Assignor makes its responsibilities conditional, greatly limiting its obligations if a claim is brought.

Always select only one option at one time their no other option.

Section 10: Successors and Assigns States that the Parties' rights and obligations will be: passed on to successor organizations (if any), or organizations to which rights and obligations have been permissibly assigned.

Section 11: No Implied Waiver. Explains that even if one Party allows the other to ignore break an obligation under the agreement, it does not mean that Party waives any future rights to require the other to fulfill those (or any other) obligations.

Section 12: Notice. Lists the addresses to which all official or legal correspondence should be delivered. Write in a mailing address for both the Assignor and the Assignee.

Section 13: Governing Law. Allows the parties to choose the state laws that will be used to interpret the document. Note that this is not a venue provision. The included language will not impact where a potential claim can be brought. Write the applicable state law in the blank provided.

Section 14: Counterparts/Electronic Signatures. The title of this provision sounds complicated, but it is simple to explain: it says that even if the Parties sign the agreement in different locations, or use electronic devices to transmit signatures (e.g., fax machines or computers), all of the separate pieces will be considered part of the same agreement. In a modem world where signing parties are often not in the same

city - much less the same room - this provision ensures that business can be transacted efficiently, without sacrificing the validity of the agreement as a whole.

Section 15: Severability. Protects the terms of the agreement as a whole, even if one part is later invalidated. For example, if a state law is passed prohibiting choice-of-law clauses, it will not undo the entire agreement. Instead, only the section dealing with choice of law would be invalidated, leaving the remainder of the assignment enforceable.

Section 16: Entire Agreement. The Parties' agreement that the document they're signing is "the agreement" about the issues involved. Unfortunately, the inclusion of this provision will not prevent a Party from arguing that other enforceable promises exist, but it will provide you some protection from these claims.

Section 17: Headings. Every document should me with suitable heading, and should not be considered operational parts of the note.

3.4 INFRINGEMENT OF PATENT:

What Amounts to an Infringement?

A patentee has an exclusive monopoly rights over the patented invention to make, use, sell or distribute the invention in India. If any person, other than the patentee or assignor or mortgagor, violates this exclusive right, there will be infringement of patent rights. Whether the alleged act of a person amounts to an infringement or not depends upon the extent of the monopoly right conferred by the patent. These can be inferred from the specification and claims made by the patentee contained in the patent application. An important provision pertains to the burden of proof in case of infringement. If the patent pertains to a process for making a product, and a person makes an identical product, then in a case of infringement he is obliged to prove that the process used to make the product, is different from the patented process. However, the patentee has to prove that the product being made by the infringer is identical to the product from his process. He also has to prove that he is not able to determine the process used by the infringer through reasonable efforts. The following acts of the defendant can amount to infringement:

- Colorable imitation of patented invention; or
- Copying essential features of patented invention; or
- Their are lots of variation inside patented inventions; or
- Chemical or mechanical equivalents.

Suit for Infringement:

When any person infringes the rights of the patentee, a suit for infringement of patent should be instituted in the District Court having jurisdiction to try the suit. A suit for infringement can be instituted only if the patent has been sealed. The patentee cannot

institute a suit for infringement during the period between date of advertisement of acceptance of the complete specification and the date of sealing of patent. However, he can claim damages sustained due to infringement during the said period in a separate suit after sealing of patent. A suit for infringement of a patent, whose term has expired, can be instituted for claiming damages if the infringement occurred during the term of patent. In case the patent was wrongfully obtained by the patentee and was later granted to the true and first inventor, a suit for infringement occurring before the grant of patent cannot be instituted. Where a patent had lapsed but was subsequently restored, the proceedings for infringement cannot be instituted against any infringement committed between the date on which the patent ceased to have effect and the date of advertisement of application for restoration.

Acts not Constituting Infringement:

Where the patented invention is merely used for the purpose of experiment or research or for imparting instruction to pupils, it does not amount to infringement of patents. Similarly, any act of making, using or selling a patented invention solely for development of information required under any relevant law does not amount to infringement. Also the importation of patented products by any person from a person who is duly authorised by the patentee will not constitute infringement.

Limitation Period and Institution of Infringement Suit:

There is max to max 3 years from date of infringement. However, it is not necessary to send a notice of infringement to the defendant before filing the ' suit for infringement.

Relief in Suit for Infringement:

The patentee, on being successful in a suit for infringement is entitled to an injunction (or restraining), damages or accounts, and otherwise. Injunction' is a normal remedy, though discretionary on the part of the Court. It stops the infringement during the pendency of the proceedings. 'Damages' account for the loss in money terms suffered by the owner of the patent due to infringement. 'Accounts' relates to the account of net profits earned by the defendant (infringer). If there are no profits, 'accounts' is not a remedy. Damages and Accounts are alternative remedies; the owner can chose only one of them, not both. 'Otherwise' as a remedy is a general provision which authorises the court to grant such other reliefs as it may deem necessary for complete redressal of the complaint. For example, the court may order that the infringing goods or materials and implements shall be seized, forfeited or destroyed.

What Is Copyright?

Copyright is protection provided by law (title 17, U.S. Code) to the authors/creators of "original works Patents of authorship," expressed in any tangible medium. When we add copyright all the information must be private and no one can hack that information. This protection is available for original works from the moment they are

created and expressed in a tangible , medium, and it applies whether they are published, unpublished, or registered with the U.S. Copyright Office.

Copyright ownership and protection is available for an author/creator if three requirements are met:

(1) Fixation: The work exists in a medium from which the author's expression can be read, seen, or heard, either directly or by the aid of a machine.

(2) Originality: The work owes its origin and independent creation to an author.

(3) Minimal Creativity: The work is the product of at least a minimal level of creativity.

Objectives:

This course will teach you the following basics of copyright law, fair use, and the copyright/licensing issues involved in using a wide variety of materials protected by copyright in your many situations. By the j end of this course, you will:

(1) Increase your knowledge and understanding of copyright and licensing issues; and know what it means to say that someone owns the copyright to a creative work.
(2) Learn more about why copyright law exists and where it all started (the history of copyright.
(3) Know how to resolve basic copyright/licensing questions and when, and who to ask for more help.
(4) Realize and respect the ethical /moral aspects involved in using materials protected by copyright.
(5) Their should be variety of copyrights question and specific case studies.

3.5 EXCLUSIVE RIGHTS IN COPYRIGHTED WORKS:

(1) to reproduce the copyrighted work in copies or phonorecords.
(2) to prepare derivative works based upon the copyrighted work.
(3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending.
(4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other Patents audiovisual work, to display the copyrighted work publicly; and
(5) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

Transfer of Copyrights:

A copyright transfer agreement is a legal document containing provisions for the

conveyance of full or partial copyright from the rights owner to another party. It is similar to contracts signed between authors and publishers but does not normally involve the payment of remuneration or royalties. Such agreements are a key element of subscription-based academic publishing, and have been said to facilitate the handling of copyright-based permissions in print- only publishing. In the age of electronic communication, the benefits of copyright transfer agreements have been questioned, and while they remain the norm, open licenses as used in open access publishing have been established as an alternative. Copyright transfer agreements became common in the publishing business after the Copyright Act of 1976 in the United States and similar legislation in other countries redefined copyright as accruing to the author from the moment of creation (rather than publication) of a work. There are lots of countries involve in that. This required publishers to acquire copyrights from the creator in order to sell the works or access to it, and written statements signed by the rights owner became necessary in order for the copyright transfer to be considered valid. Granting publishers the permission to copy, display and distribute the work is necessary for publishers to act as such, and copyright transfer agreements across a wide range of publishers have such provisions. The reach of copyright transfer agreements can go well beyond that, and "some publishers require that, to the extent possible, copyright be transferred to them." This means that no one, including the authors, can reuse text, tables, or figures in other publications without first getting permission from the new copyright owner. Copyright transfer agreements also ask that the authors confirm to actually own the copyright for all of the materials pertaining to a given act of publishing, and that the item for which the copyright is to be transferred has not been previously published and is not under consideration to be published elsewhere, to limit the frequency of duplicate publication and plagiarism.

Defences for infringement:

The primary defense to copyright infringement is "fair use." 17 U.S.C. § 107. The fair use doctrine allows the reproduction and use of work, notwithstanding the rights of the author (17 U.S.C. §§ 106 and 106A), for limited purposes included criticism, comment, news and scholarship. Fair use may be described as the Patents privilege to use the copyrighted material in a reasonable manner without the owner's consent. In deciding whether a copier's actions were fair, judges will consider

(1) The purpose and character of the copying (certain types of educational copying is allowed)
(2) The nature of the original (originals made for commercial reasons are less protected from copying than their purely artistic counterparts)
(3) The amount and substantiality of the portion copied (one may not copy the "heart" of a work without the author's permission); and
(4) The effect that such copying may have on the market for the original (copying may be permitted if it is unlikely to cause economic harm the original author).

Examples of activities that may be excused as fair use include: distributing copies of a section of an article in class for educational purposes; providing a quotation in a book review; and imitating a work for the purpose of parody or social commentary.

Trademarks-Objectives:

The trademark search is the most important step in the process of selecting a new mark. Since trademark rights are granted on a first come basis, it is important to determine whether anyone else has prior rights in the same or similar mark. If you do not do a comprehensive search, you run the risk of infringing someone's mark. In addition to defending an unnecessary lawsuit, you may be required to change your mark, destroy your inventory, or pay significant licensing fees.

A comprehensive trademark search includes a search of state and federal trademark applications and registrations, common law uses, including business directories, company names,, and domain names. Ideally, a trademark search should be done by a professional search firm close to the time you plan to adopt the mark. However, you can rule out certain marks by conducting a "knock-out" or "screening" search. You can do this yourself using, for example, trade directories and the Internet.

An assessment of whether a mark is confusingly similar is best done by a trademark attorney who can decode the results of your search. Bear in mind that "clearing" a corporate name with the secretary of state is not the same thing as determining its availability for commercial use. Moreover, relying on the records of the United States Patent and Trademark Office (www.uspto.gov/) alone is not enough, since trademarks arise out of use and may not be federally registered. Assuming the mark is available and there are no potentially conflicting marks, you can register it on the federal or state level, or use it without registration.

TIP:

When selecting a trademark, two key points to remember are: (I) not use descriptive words; and (ii) order a trademark search to screen-out confusingly similar marks already being used by others. Rights of

Trademarks:

The extent to which a trademark owner may prevent unauthorized use of trademarks which are the same as or similar to its trademark depends on various factors such as whether its trademark is registered, the similarity of the trademarks involved, the similarity of the products or services involved, and whether the owner's trademark is well known or, under U.S. law relating to trademark dilution, famous.

If a trademark has not been registered, some jurisdictions (especially Common Law

countries) offer protection for the business reputation or goodwill which attaches to unregistered trademarks through the tort of passing off. Passing off may provide a remedy in a scenario where a business has been trading under an unregistered trademark for many years, and a rival business starts using the same or a similar mark.

If a trademark has been registered, then it is much easier for the trademark owner to demonstrate its trademark rights and to enforce these rights through an infringement action. Unauthorized use of a registered trademark need not be intentional in order for infringement to occur, although damages in an infringement lawsuit will generally be greater if there was an intention to deceive.

For trademarks which are considered to be well known, infringing use may occur where the use occurs in relation to products or services which are not the same as or similar to the products or services in relation to which the owner's mark is registered. A growing area of law relating to the enforcement of trademark rights is secondary liability, which allows for the imputation of liability to one who has not acted directly to infringe a trademark but whose legal responsibility may arise under the doctrines of either contributory or vicarious liability.

Protection of Goodwill:

Many countries protect unregistered well-known marks in accordance with their international obligations under the Paris Convention for the Protection of Industrial Property and the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement). Consequently, not only big companies but also SMEs may have a good chance of establishing enough goodwill with customers so that their marks may be recognized as well-known marks and acquire protection without registration. It is, nevertheless, advisable to seek registration, taking into account that many countries provide for an extended protection of registered well-known marks against dilution (Art. 16.3 TRIPS), i.e., the reputation of the mark being weakened by the unauthorized use of that mark by others.

You should be aware of the fact that a number of trademark laws merely implement obligations under Article 16.3.http://en.wikipedia.org/wiki/Traaemark - cite_note-Paris_Convention_1967-40 of the j TRIPS Agreement and protect well-known registered trademarks only under the following conditions: 1- that the goods and services for which the other mark is used or is seeking protection are not identical with or similar to the goods for which the well-known mark acquired its reputation 2- that the use of the other mark would indicate a connection between these goods and the owner of the well-known mark, and 3 - that his interests are likely to be damaged by such use.

Infringement of Trademark:

Trademark infringement is a violation of the exclusive rights attaching to a trademark

without the authorization of the trademark owner or any licensees (provided that such authorization was within the scope of the license). Infringement may occur when one party, the "infringer", uses a trademark which is identical or confusingly similar to a trademark owned j by another party, in relation to products or services which are identical or similar to the products or services which the registration covers. An owner of a trademark may commence civil legal proceedings against a party which infringes its registered trademark. In the US, the Trademark Counterfeiting Act of 1984 criminalized the intentional trade in counterfeit goods and services.

The ACTA trade agreement, signed in May 2011 by the United States, Japan, Switzerland, and the EU, requires that its parties add criminal penalties, including incarceration and fines, for copyright and trademark infringement, and obligated the parties to active police for infringement.

In many countries (but not in countries like the United States, which recognizes common law trademark rights), any trade mark is not registered cannot be "infringed" as such, and the trademark owner cannot bring infringement proceedings. Instead; the owner may be able to commence proceedings under the common law for passing off or misrepresentation, or under legislation which prohibits unfair business . practices. In some jurisdictions, infringement of trade dress may also be actionable.

Where the respective marks or products or services are not identical, similarity will generally be assessed by reference to whether there is a likelihood of confusion that consumers will believe the products or services originated from the trademark owner.

Likelihood of confusion is not necessarily measured by actual consumer confusion, though normally one of the elements, but by a series of criteria Courts have established.

Passing off Trademarks:

Passing off is a common law tort which can be used to enforce unregistered trademark rights. The tort of passing off protects the goodwill of a trader from a misrepresentation that causes damage to goodwill.

The law of passing off prevents one person from misrepresenting his/her goods or services as being the goods and services of the claimant, and also prevents one person from holding out his or her goods or services as having, some association or connection with the plaintiff when this is not true.

A cause of action for passing off is a form of intellecttial property enforcement against the unauthorised use of a mark which is considered to be similar to another party's registered or unregistered trademarks, particularly where an action for trademark infringement based on a registered trade mark is unlikely to be successful (due to the differences between the registered trademark and the unregistered mark). Passing off is a form of common law, whereas statutory law such as the United Kingdom Trade

Marks Act 1994 provides for enforcement of registered trademarks through infringement proceedings.

Passing off and the law of registered trademarks deal with overlapping factual situations, but deal with them in different ways. Passing off does not confer monopoly rights to any names, marks, get-up or other indicia. It does not recognize them as property in its own right.

Instead, the law of passing off is designed to prevent misrepresentation in the course of trade to the public, for example, that there is some sort of association between. the business of defendant and that of the claimant. Another example of passing off is where the defendant does something so that the public is misled into thinking the activity is associated with the claimant, and as a result the claimant suffers some damage, under the law of passing off it may be possible for the claimant to initiate action against the defendant.

3.6 DEFENCES OF TRADEMARKS:

How can I defend myself against a claim of Trademark Infringement?

Their are four distinct defences include claim of infringement:

- **Doctrine of Laches**
- **Estoppel**
- **Unclean Hands**
- **Fair Use/Collateral Use**

• **Doctrine of Laches:** Stating that the other party neglected to assert a right or claim which, taken together with lapse of time and other circumstances causing prejudice to you, operates as bar in court of equity.
• **Estoppel:** "The doctrine of estoppel has three essential elements - a position of authority assumed by the defendant; submission to and reliance upoh that assumption by the plaintiff; and injury suffered by the plaintiff as an immediate consequence of such submission and reliance."

• **Unclean Hands:** Invoked by a court only when a plaintiff otherwise entitled to relief has acted so improperly with respect to the controversy that the public interest in punishing the plaintiff outweighs the need to prevent defendant's illegal conduct.

• **Fair Use/ Collateral Use:** Fair use allows fair comment that incidentally involves use of the mark for a purpose other than that normally made of a trademark. Most often occurs in advertising cases (so long as there are no untrue claims) and parody cases (but it is not fair use when a claimed parody is used to promote competitive goods or services).

Collateral use allows the use of goods that bear a preexisting mark. Basically, when a

party uses a trademarked item as a component of a more complex product, the doctrine of collateral use allows the party to so identify the component by its trademarked name without .fear of being liable for infringement. This is only true to the extent the party does not deceive the public into thinking that the product, as sold, is actually marketed by the trademark owner.

3.7 OBJECTIVES OF DESIGN:

Design objective (DO):

In communications systems, a desired performance characteristic for , communications circuits and equipment that is based on engineering analyses, but (a) is not considered feasible to mandate in a standard, or (b) has not been tested. DOs are used because applicable systems standards are not in existence.

Examples of reasons for designating a performance characteristic as a DO rather than as a standard are (a) it may be bordering on an advancement in the state of the art, (b) the requirement may not have been fully confirmed by measurement or experience with • operating circuits, and (c) it may not have been demonstrated that the requirement can be met considering other constraints, such as cost and size.

A DO is sometimes established in a standard for developmental consideration always make the proper development. A DO may also specify a performance characteristic that may be used in the preparation of specifications for development or procurement of new equipment or systems.

Rights of Design:

The term “Design Right” refers to the specific.There are specific differences between Design Right and Registered Designs.

Registered Designs give you exclusive rights in a design, in the UK, for up to 25 years. You can stop people making, offering, putting on the market, importing, exporting, using or stocking for those purposes, a product to which your design is applied. You can protect two-dimensional designs or surface patterns as well as shape and configuration with a Registered Design.

By comparison, Design Right gives you automatic protection for the internal or external shape or configuration 9f an original design, i.e. its three- dimensional shape. Design Right allows you to stop anyone from copying the shape or configuration of the article, but does not give you protection for any of the 2-dimensional aspects, for example surface patterns. Protection is limited to the United Kingdom (UK), and lasts either 10 years after the first marketing of articles that use the design, or 15 years after creation of the design - whichever is earlier. For the last 5 years of that period the design is subject to a Licence of Right. This means that anyone is entitled to a licence to make and sell products copying the design.

If you are the owner of a design right subsisting in a design, you have the exclusive right to reproduce the design for commercial reasons by making articles to the design or by making a design document recording the design for the purpose of enabling articles to be made. If anyone else carries out these activities without your permission, they may infringe the design right.

However, it is more difficult to prove infringement of an unregistered Design Right as you must be able to prove it was copied, or that the potential for copying existed.

Infringement proceedings must be brought before the Courts, however somq disputes concerning the subsistence of design right can be referred to us.

Design Infringement:

A design registration provides protection for aspects of the appearance of an article, such as its shape, configuration, pattern or ornamentation. Unlike patents, a design registration does not protect purely functional aspects of an article unless they also contribute to its appearance. As most manufactured articles involve an element of designer choice, design protection is generally available.

Design infringement generally. A design registration is infringed by the unauthorised manufacture or importation for sale (or ' commercial use) or the unauthorised sale or hire (or offering to sell or hire) of articles incorporating or embodying the registered design in New Zealand. Legal action can only be taken against an infringer once the Certificate of Registration has issued. Court proceedings are initiated in the High Court. Appeals are possible to the Court of Appeal. The case is heard and decided by a Judge alone, with no jury involvement.

The question of infringement is a question for which the eye must be the judge. Courts may apply either a side-by-side test and/or an imperfect recollection test, and will also consider actual usage of the design in question. The degree of novelty of the registered design in light of the prior art (i.e. any material in the public domain as at the application date of the registered design) must also be considered. In one case it was said: “If there is substantial novelty or originality small variations in the article alleged to infringe will be unlikely to save the defendant. On the other hand if the features of novelty or originality are but little removed from prior art small differences may avoid an infringement.”

Defences of Design Infringement:

This note briefly looks at the four main defences to unregistered design (UDR) infringement:

(1) Challenge for validity: The defendant can challenge the validity of the UDR, for example by arguing that the design is commonplace.

(a) A party to a dispute as to subsistence, term or first owner of an UDR can

refer the matter to the Comptroller- General of Patents, Designs and Trade Marks whose decision is binding on the parties (s246(l)).

(b) The rules for bringing such proceedings are set out in the Design Right (Proceedings before Comptroller) Rules 1989.

(2) Innocent Infringement:

It is a partial defence for the defendant to show that he did not know (and had no reason to believe) that:

(a) (for primary infringement) UDR subsisted in the design - in which case the defendant is not liable for damages; or

(b) (for secondary infringement) the article was an infringing article - in which case the defendant is liable only for damages not exceeding a reasonable royalty.

(3) Compulsory licence:

In the last five years of the UDR term any person may licence an UDR (and thus avoid any infringements),

(a) Should the owner and licensee not be able to agree to the terms of the licence then the terms will be settled by the Comptroller-General of Patents, Designs and Trade Marks (s237(2)), in the downtime before the decision is made the licensee may use the UDR;

(b) The licensee can expect to pay a royalty for the licence which will vary depending on the facts of the situation.

(4) Use by the Crown a government department may use a design for supplying articles for defence and health-service purposes if it pays compensation to the owner in an agreed amount (or if no agreement is reached then as determined by a court)

UNIT 4

4.1 COMPUTER SOFTWARE AND INTELLECTUAL:

Congress has provided for both private and public enforcement of the antitrust laws. Anticompetitive conduct may be challenged by the Antitrust Division of the Department of Justice, the Federal Trade Commission, state attorneys general, and private parties who have been injured by the antitrust violation and have standing to sue.

When the federal government sues, their are wide range of injunctive relief, one of them is positive relief, in "positive" relief requiring the restructuring of a company or the implementation of certain practices, as well as recover its own damages as a purchaser. In addition, the Department of Justice is uniquely empowered to seek substantial criminal fines against both corporations and individuals and prison sentences against individuals. In more limited circumstances, the federal government may seek civil fines or equitable monetary remedies, including the disgorgement of ill-gotten gains and restitution. State attorneys general can sue in a parents patriae capacity on behalf of injured citizens of their states. They also can recover for state entities where they have been ; directly injured. Private parties injured by various J reasons including alleged antitrust violation can sue to recover three times their actual damages, plus costs I j and attorneys' fees, and for equitable relief similar to what the government can obtain. Private antitrust enforcement has been more vigorous in the United States than anywhere else in the world. The private antitrust enforcement include two factors.

(1) the availability of treble damages plus costs and attorneys' fees, and
(2) the U.S. class action mechanism, which allows plaintiffs to sue on behalf of both themselves and similarly situated, absent plaintiffs.

An aggressive and capable antitrust plaintiffs include so many class actions following on to government criminal prosecutions and in situations where individual plaintiffs might not have the ability or incentive to sue. Congress, state legislatures, and the courts have developed rules governing who can recover for injuries that are "passed on" to various levels of consumers, the availability of attorneys' fees and prejudgment interest on damages, and how liability is allocated among alleged participants in an antitrust conspiracy.

Over the years, observers that there is lots of talking on public and private enforcement framework in locate compensation of victims. With respect to private civil actions, for example, the availability of trouble damages has been both loaded as the key to an effective enforcement system and blamed for burdening business with litigation of questionable merit. Some observers contend that trouble damages are insufficient to deter and compensate at optimal levels and should be increased to some higher multiplier; others take the opposite view. With respect to government civil

and criminal enforcement, observers similarly have suggested both that the government has too great an enforcement arsenal at its disposal and that it has too little.

Because of the interrelated nature of the rules and procedures governing private and public enforcement, The commission decided to clear both public and private enforcement. The recommendations include:

(A) the availability of trouble damages and the rules relating to prejudgment interest and attorneys' fees, as well as the liability of each defendant for the full harm caused by all participants in an antitrust conspiracy (known as "joint and several liability");
(B) which party should recover antitrust damages
(C) new authorization should be provided by the department or the Federal Trade Commission to obtain civil fines for substantive, non-criminal antitrust violations or to seek monetary equitable remedies on an expanded basis; and
(D) Any changes to the current criminal antitrust enforcement are needed or not.

4.2 CLAUSES OF LICENSING:

Preamble:

The preamble is the introduction to your licence. The preamble means purpose of the agreement, i.e., for one party to license the content of the other party. Typically, a preamble defines information about both the parties include sign the agreement, the names of the parties, their addresses, the name or a brief description of the content always be licensed, who owns the content, and who wants to license the content, it is important to make out date of agreement; alternatively, this may be set out at the end of the agreement above the signature lines.

Content Covered by the Agreement:

The clause include agreement called as "Subject", "Subject Matter" or "Product Definition."

When we create agreement it is always be clear dependent on the content. Is the content a single photograph or a set of photographs by a specific photographer on a certain topic? Or is your museum licensing the electronic version of a print publication to which you subscribe, or an electronic-only periodical? Is the content an online subscription to a journal, database, Or encyclopedia? You may need to define whether such content includes full text articles, abstracts, table of contents, indices, and new or special online products, sections or services that are available online.

Rights for "Re-Use":

There are lots of rights for media that museums have recently started to consider when licensing the content of others. For many of these' uses, it is possible that the licensor will only allow a limited excerpt in the general licence and that use of larger

portions or whole works will require an additional separate licence likely for an additional fee. These include:

- Use of licensed content transfer in an e-book published by the museum.
- Use of content transferred to an iPod for access by museum visitors.
- Use of content for creating different information.
- Use of content for virtual exhibits (by both physical and virtual museums).
- Use of content on social networking sites including MySpace, YouTube, flickr, blogs and wiki's.

Fair Dealing:

In Canada, licence agreements may limit rights that otherwise would apply under the application of the Canadian copyright law and principle of fair dealing. If an agreement does not discuss fair dealing or expressly acknowledge it, then it will apply. However, The agreement contains lots of rules for fair dealing. Note that even if fair dealing is restricted, it will only be restricted in terms of the licensee, and not vis-a-vis any third party as the agreement is only valid between the parties who sign it. This is a controversial issue. Some licences that specifically refer to Fair Dealing allow it under the licence in a manner that is consistent with the Fair Dealing provision in the Canadian Copyright Act.

Usage or Authorized Uses:

Licence agreements generally specify the purpose of the use of the content for licensing and sub-licensing. Their are lots of part to be referred such as "Authorized Uses", "Conditions of Use" or "Purpose". Usage may include the following:

- Personal.
- Non-commercial.
- Non-profit.
- Scholarly.
- Research.
- Scientific.
- Educational.
- Collaborative'works.
- Review or comment.
- Private use or research.
- Electronic reserves.
- Use of excerpts in e-books.
- Class packages, training courses, course management systems.
- Internal research in the course of employment, business or profession.

The use of licensing as a marketing and brand extension tool maximum upto 30 years. When well- executed, a strong licensing relationship brings benefits to all parties to

the deal - property owners and their agents, licensees and their affiliates, retailers and, ultimately, consumers, Each parties goals and aims added lots of important values to end product

To get the strongest outcome, each participant in the licensing process has certain responsibilities to fulfil. Every agreement between the licensing parties is unique in its specifics, so even these responsibilities vary to some extent.

4.3 BENEFITS OF LICENSING:

Licensors:

There are many reasons for an intellectual property (IP) owner to grant a license. The most obvious one is to generate revenue from the guarantee and royalty payments. But licensing also can serve a number of other purposes. In some cases, those "other" reasons to license might actually be more important to the licensor than revenue alone:

(1) Marketing support for the core business: For a television show, film, children's book or sports brand, the retail display and proliferation of licensed products doesn't only generate product sales, but it also promotes the core property.

Apply different way to promote the film itself. A sports fan wears a shirt with the logo of their favourite team may be expressing their enthusiasm about the team, but they are also subtly promoting the sport, the league and the team to anyone who passes her by on the street.

The same goes for a beer brand. Seeing a store display of glassware carrying a well-known beer logo reinforces the brand image, supporting the brand's overall marketing efforts.

(2) Extending a corporate brand into new categories, areas of a supermarket, or into new distribution channels: Licensing represents a way to move a brand into new businesses without making a major investment in new manufacturing processes, machinery or facilities. In a well-run licensing program, the property owner maintains control over the brand image and how it's portrayed (via the approvals process and other contractual strictures), eventually reaping the benefit in additional revenue (royalties), as well as exposure in new channels or supermarket aisles. Examples might include:

- A well-known brand of construction tools licensed into such areas as work gloves or work boots.
- A better brand always looking with better skin.
- A popular restaurant chain licensing a frozen food manufacturer to market a line of food manufacturer to market a line of appetisers under its brand.

- A well-known fashion label licensing its name into such natural extensions as leather accessories, shoes, fragrances or home textiles.

(3) Trying out potential new businesses or geographical markets with relatively small upfront risk:

By licensing its brand to a thirdparty manufacturer, a property owner can try new businesses, or move itself into new countries with a smaller upfront investment than by building and staffing its own operations.

(4) Maintaining control over an original creation:

Licensing represents a way for artists and designers to profit from their creative efforts, while maintaining control over how they are used. For brand owners (particularly those doing business internationally), licensing and registering the internationally), licensing and registering the

brands in multiple markets is a way to protect the brand from being used by others without permission.

Licenses are given to use property correctly there are lots of responsibilities on licensor to create successful program They include:

- A timely and efficient approval process, so that products can move their way along the development chain in a timely way.
- Giving guidance (often in the form of a printed or digital style guide) about how the brand, character, logo or other IP can be portrayed within the product, on packaging, or in advertising and promotional materials.
- Assisting in marketing activities and, in many cases, helping to sell the brand to retailers.

An IP owner also has to be aware of the risks involved in licensing. The brand owner has to be careful that a potential licensee can:

- Creation and delivery of product with high performance of quality standard.
- Service the retailer adequately.
- Prove that their goals for the brand align with those of the brand owner..
- Serve as a true partner in a relationship that, when well-executed, is a win-win proposition • Serve as a true partner in a relationship that, those of the brand owner..
- Serve as a true partner in a relationship that, when well-executed, is a win-win proposition for all involved.

4.4 LICENSEES:

Licensees lease the rights to a certain property for incorporation into their merchandise, but usually do not share ownership in it. Nevertheless, licensing provides a number of important functions to them.

(1) Gaining the consumer awareness and marketing benefit of a Well-known brand, character, logo,design:

The most obvious benefit to a manufacturer or service provider that licenses a brand, character, design or other piece of intellectual property is the marketing power it brings to the product. It can take hundreds of thousands of pounds to build a brand from scratch, and licensing represents a way for a manufacturer to take advantage of all the brand building and image building that has gone on before. A child in a toy store doesn't seek "an action * figure." He's generally looking for a particular character he's found of. Faced with a choice among several cleaning implements, shopper might be drawn by one that bears the brand of a well-known cleaning fluid, rather than a more generic label. In making the decision about whether or not to take on a license, a more generic label. In making the decision about whether or not to take on a license, a manufacturer often weighs the potential royalty payments against the cost of building a brand on its own.

(2) Moving into new distribution channels: Taking on a license might help a manufacturer whose brand has been marketed in, for example, discount retail chains to market a more upscale, high quality line in shops or department stores that wouldn't carry the lower end products.

(3) Reducing in-house costs: A manufacturer who licenses artwork or designs to be applied to household items or clothing has less reliance on in-house art staff that would otherwise need to be maintained.

(4) Enhancing authenticity and credibility: The publisher of a car-racing videogame might license a host of well-known automotive brands and car models to lend legitimacy and authenticity to the game. Similarly, a maker of automotive parts or accessories will license the car brand to establish in the consumer's mind that its products will work seamlessly with the cars of the parent brand. In taking on a license, a licensee takes on a financial obligation, and also an obligation to adhere to agreements in such areas as submitting products for all necessary approvals, creating a product to agreed-upon standards and marketing the product. The risks that the licensee faces in a licensing program are fewer in number than those of the licensor, but potentially greater in magnitude, their are lots of risks including royalties guarantees. Even if the products do make it to the market, there is no certainty at all that they will do well, no matter what property a manufacturer chooses.

UNIT 5

5.1 INTRODUCTION:

Internet use as global system worldwide through internet we can connect lots of devices the main used for this connectivity is TCP/IP. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW), the infrastructure to. support email, and peer-to-peer networks. Most traditional communications media including telephone, music, film, and television are being reshaped or redefined by the Internet, giving birth to new services such as voice over Internet Protocol (VoIP) and Internet Protocol television (IPTV). Newspaper, book and other print publishing are adapting to website technology, or are reshaped into blogging and web feeds. The Internet has enabled and accelerated new forms of human interactions through instant messaging, Internet forums, and social networking. Online shopping has boomed both for major retail outlets and small artisans and traders. Now humans can communicate anywhere by using internet services at anytime. Business-to-business and financial services on the Internet affect supply chains across entire industries. The Internet has no centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own policies. Only the overreaching definitions of the two principal name spaces in the Internet, the Internet Protocol address space and the Domain Name System, are directed by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN). Internet protocols used for addressing your devices while domain name system recognized which type of addressing you used as information of lots sites. The technical underpinning and standardization of the core protocols (IPv4 and IPv6) is an activity of the Internet Engineering Task Force (IETF), a nonprofit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise.

5.2 SCOPE OF CYBER LAWS:

The rapid development of information technology posed certain challenges for the law that are not confined to a particular category of law but arises in diverse areas of law, such as criminal law, intellectual property law, contract and tort. Of late, owing to the rapid development of the internet and the World Wide Web, various unprecedented problems have emerged.

These problems concern the issues of free speech, intellectual property, safety, equity, privacy, ecommerce and jurisdiction and are governed by the Cyber Law. The branch of law which regulates the technological aspects of information or information processing is called Cyber Law. The scope of different problem includes:

(a) dealing with the computer hackers or those who introduce viruses;
(b) categorization of 'contract for the acquisition of software' on similar footing with contract which dealing with goods;
(c) dealing with the phenomenon of mass consumer purchases from other jurisdictions under ecommerce;
(d) existence of copyright in a computer programme and question of patent protection;
(e) question of destruction of copyright due to the wide spread dissemination of text on networks;
(f) regulation of 'cyber squatting' and trafficking in domain names under law;
(g) the question of regulation of the content of material on the internet and freedom of information and expression; and
(h) the protection of the privacy of the individual amid the increasing capacity for storing, gathering, and collating information.

5.3 SCOPE OF CYBER JURISPRUDENCE:

Jurisprudence studies the concepts of law and the effect of social norms and regulations on the development of law. There are two types of jurisprudence:

(1) The philosophy of law, or legal theory
(2) Case Law Legal theory does not study the characteristics of law in a particular country (e.g. India or Canada) but studies law in general i.e. those attributes common to all legal systems. There are lots of questions arise with legal theory:

(1) What is law and legal system?
(2) What is the connection between law and power?
(3) What is the connection between law and justice or morality?
(4) What is difference between law and power?
(5) What is the difference between justice and j morality?
(6) Does every society have a legal system?
(7) How should we understand concepts like legal I rights and legal obligations or duties?
(8) What is the proper function of law?
(9) What sort of acts should be subject to punishment, and what sort of punishments should be permitted?
(10) What is mean by justice?
(11) What rights do we have?
(12) Is there a duty to obey the law?
(13) What value does the rule of law have?

Case law is the law that is established through the decisions of the courts and other officials. Case law assumes even greater significance when the wordings of a particular law are ambiguous. The interpretation of the Courts helps clarify the real objectives and meaning of such laws. This chapter first discusses the meaning of cyber law and

the need for the separate discipline of cyber law. The primary source of cyber law in India is the Information Technology Act, 2000 (IT Act) which came into force on 17 October 2000. The main goal of act to provide restriction on use of electronic commerce and electronic records with the government.

The IT Act also penalizes various cyber crimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs. 1 crore). An Executive Order dated 12 September 2002 contained instructions relating provisions of the Act with regard to protected systems and application for the issue of a Digital Signature Certificate. Minor errors in the Act were rectified by the Information Technology (Removal of Difficulties) Order, 2002 which was passed on 19 September 2002. The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques. Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to the Government bodies. On the same day, the Information Technology (Certifying Authorities) Rules, 2000 also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006 Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July 2001. Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National of Difficulties) Order, 2002 which was passed on 19 September 2002. The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques. Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to the Government bodies. On the same day, the Information Technology (Certifying Authorities) Rules, 2000 also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA. I'hese rules were amended in 2003, 2004 and 2006 Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on

9th July 2001. Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National.

Repository of Digital Certificates. These were issued on 16th December 2002. The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 also came into force on 17th October 2000. These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers. The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT. Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT. On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers. The appointment of adjudicating officers to decide the fate of multi-crore cyber crime cases in India was the result of the public interest litigation filed by students of Asian School of Cyber Laws (ASCL).

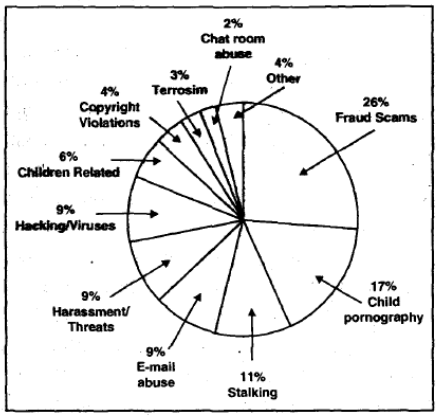

Fig. 5.1

5.4 DIGITAL SIGNATURE:

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signature contains important documents with high rate of security. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in transit. Digital signature highly used for software distribution and financial transaction, and in other cases where it is important to detect forgery or tampering. Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data

that carries the intent of a signature but not all electronic signatures use digital signatures. In some countries, including the United States* India, and members of the European Union, electronic signatures have legal significance. Digital signatures eniploy a type of asymmetric cryptography. For messages sent through a noesecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equiivafent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol. A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. Private keys are not published between sender and receiver while public can be shared sender and receiver.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly it should be correctly calculated and infeasible to generate a valid signature for a party without knowing that party's private key. There are several reasons to sign such a hash (or message digest) instead of the whole document.

- **For efficiency**: The signature will be much shorter and thus save time since hashing is generally much faster than signing in practice.
- **For compatibility**: Messages are typically bit strings, but some signature schemes operate on other domains (such as, in the case of RSA, numbers modulo a composite number JV). A hash function can be used to convert an arbitrary input into the proper format. Hash function is proper way to store the information.
- **For integrity:** Without the hash function, the text "to be signed" may have to be split (separated) in blocks small enough for the signature scheme to act on them directly. However, the receiver of the signed blocks is not able to recognize

if all the blocks are present and in the appropriate order. The receiver is always know the importance of the block that present in appropriate order.

5.5 USE OF DIGITAL SIGNATURE:

Authentication: Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user **Integrity**: In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. When receiver receives the message the decrypt that message.

5.6 DIGITAL CONTRACTS:

An electronic contract is an agreement created and "signed" in electronic form - that means always send the contract through email.in other words, no piaper or other hard copies are used. For example, you write a contract on your computer and email it to a business associate, and the business associate emails it back with an electronic signature indicating acceptance. An e-contract can also be in the form of a "Click to Agree" contract, commonly used with downloaded software: The user clicks an "I Agree" button on a page containing the terms of the software license before the transaction can be completed.

5.7 CERTIFYING AUTHORITY:

An organization which issues public key certificates.

- Must be widely known and trusted.
- Must have well defined methods of assuring the identity of the parties to whom it issues certificates.
-

Must confirm the attribution of a public key to an identified physical person by means of a public key certificate. Always maintains online access to the public key certificates issued. Public-Key

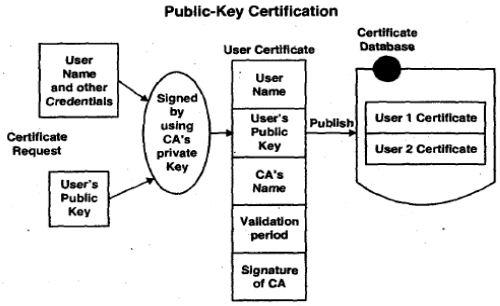

Fig. 5.2

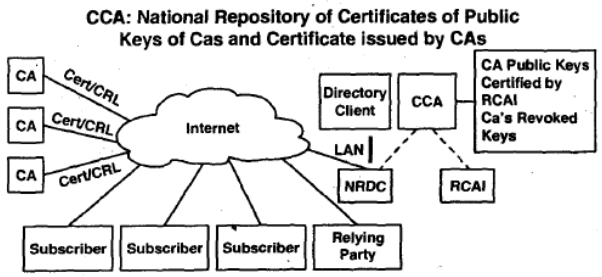

Fig. 5.3

5.8 COPYRIGHTS OF DIGITAL MEDIA:

The Digital Media Copyright Act, otherwise known as the Digital Millennium Copyright Act or simply the DMCA, is a Federal copyright law that was meant to curb Internet piracy of digital media. The bill passed in the U.S. Senate by unanimous decision on October 12, 1998 and was signed into law by President Bill Clinton seventeen days later. Since that time, the DMCA has been implemented in many notable court cases and heavily criticized by society. It is essentially the law that made it illegal to download copyrighted digital media such as music, movies, and software, and is what the RIAA and MPAA have used to combat piracy in the courts. So exactly what is the Digital Media Copyright Act and what's all the commotion about? Well, the DMCA is still a heated topic today because of its use in the fight against online piracy and its effects on Internet users. This article serves to educate those on what is in the DMCA and how it affects the everyday Internet user.

So What Is the Digital Media Copyright Act?

The DMCA is comprised of five titles and implements two treaties signed at the World Intellectual Property Organization (WIPO) Geneva conference in 1996. The five titles present in 1970 are:

- Title I: WIPO Copyright and Performances and Phonograms Treaties Implementation Act
- Title II: Online Copyright Infringement Liability Limitation Act

- Title III: Computer Maintenance Competition Assurance Act
- Title IV: Miscellaneous Provisions A
- Title V: Vessel Hull Design Protection Act Now that's a lot of legal wordiness and doesn't really explain the key points of this document. Allow me to translate this for you. I will list the important points made in this law doctrine and cite examples of how they have influenced activity on the Web.

5.9 PRIVACY AND FREEDOM ISSUE IN CYBERWORLD:

The Internet and other communication technologies have created unprecedented opportunities to share information, opening up paths for pro-democracy groups, activists, journalists and individuals around the world to organize, and hold their governments accountable. But new technological tools are vulnerable to exploitation by governments aiming to crush dissent and deny human rights. All governments struggle to balance a need to deal with serious issues such as security, hate speech, and child safety for their citizens but in repressive societies, these concerns often serve as convenient pretext to engage in censorship or surveillance of the Internet that violates the rights and privacy of users and threatens the free flow of information.

- The Global Network Initiative (GNI): We helped launch and continue to support this multistakeholder initiative to protect and advance freedom of expression and privacy in the ICT sector.
- The "Netizen" project: Maintaining free access to the Internet or communications tools is essential to the work of journalists, activists and bloggers around the world who use them to organize. Working with these netizens gives us a window into how to maintain that space.
- U.S. government advocacy: We promote policies with the U.S. administration and Congress that support these strategies. Read more about Congressional action in this area, and join our email list to see how you can help!

5.10 E-GOVERNANCE OF CYBER CRIME AND CYBER LAWS:

Governing Laws: There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology "INFORMATION TECHNOLOGY ACT, 2000" [ITA-2000] was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes. The above Act was further amended in the form of IT Amendment Act, 2008 [ITAA-2008]. The ITA-2000 defines 'Computer' means any electronic magnetic, optical or other high-speed data 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. The word 'computer' and 'computer system' defined as interpreted to mean any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities and therefore any high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition.

Scope and applicability:

The scope is the main part of computer system and cyber laws. The scope and applicability of ITA-2000 was increased by its amendment in 2008. The word 'communication devices' inserted having an inclusive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc like what was later being marketed as iPad or other similar devices on WiFi and cellular models. Though ITA- 2000 defined 'digital signature', however said definition was incapable to cater needs of hour and therefore the term 'Electronic signature' was introduced and defined in the. ITAA -2008 as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone.

The new amendment has replaced Section 43 with Section 66. The Word "hacking" used in Section 66 of earlier Act has been removed and named as "data theft" in this section and has further been widened in the form of Sections 66A to 66F. The hacking contain both type that is legal as well as illegal. The section covers the offences such as the sending of offensive messages through communication service, misleading the recipient of the origin of such messages,

dishonestly receiving stolen computers or other communication device, stealing electronic signature or identity such as using another persons' password or electronic signature, cheating by personation through computer resource or a communication device, publicly publishing the information about any person's .location without prior permission or consent, cyber terrorism, the acts of access to a commuter resource without authorization, such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus like Trojan etc. The offences covered under section 66 are cognizable and non-bailable. Whereas, the consequence of Section 43 of earlier Act were Civil in nature having its remedy in the form of damages and compensation only, but under Section 66 of the Amendment Act, if such act is done with criminal intention, then it will attract criminal liability having remedy in imprisonment or fine or both.

Adjudication:

Adjudication powers and procedures have been dealt in Sections 46 and thereafter. As per the Act, the Central Government may appoint any officer not below the rank of a director to the Government of India or a state Government as the adjudicator. The I.T. Secretary in any state is normally the nominated Adjudicator for all civil offences arising out of data thefts and resultant losses in the particular state. Very few applications were received during first 10 years of existence of the ITA, that too in the major metros only. However, the trend of receiving complaint under ITA is rapidly growing. The first adjudication obtained under this provision was in Chennai, Tamil Nadu, in a case involving ICICI Bank in which the bank was told to compensate the applicant with the amount wrongfully debited in Internet Banking, along with cost and damages. There is an appellate procedure under this process and the composition of Cyber Appellate Tribunal at the national level, has also been described in the Act. Every adjudicating officer has the powers of a civil court and the Cyber Appellate Tribunal has the powers vested in civil court under the Code of Civil \ Procedure.

UNIT 6

Information/ Technology Act, 2000

MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department)

New Delhi, the 9th June, 2000/Jyaistha 19, 1922 (Saka)

The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:

In traditional method all the information storage involve paper based method but with this act all information storage involve electronic data interchange and electronic communication, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books

Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th . January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law; AND WHEREAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, this is the best alternative to paper based information; AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records. BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:

6.1 INFORMATION TECHNOLOGY ACT 2000- 1 (Sec. 1 to 13):

(1) Short title, extent and commencement:

(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification, appoint and For different provisions it may appoint' different dates and any reference in any such provision to the commencement of this Act shall be Constructed as a reference to the commencement of that provision.

(4) Nothing in this Act shall apply to:

(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881);
(b) a power- of- attorney as defined in section 1A of the Powers- of- Attorney Act, 1882;
(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;
(d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 (39 of 1925) including any other testamentary disposition by whatever name called;
(e) any contract for the sale or conveyance of immovable property or any interest in such property;
(f) All the class of documents are notified by the central government.

(2) Definitions:

(1) In this Act, unless the context otherwise requires:

(a) "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
(c) "adjudicating officer" means an adjudicating officer appointed under subsection (1) of section 46;
(d) "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;
(e) "appropriate Government" means respect all the matter of documents.

(i) enumerated in List II of the Seventh Schedule to the Constitution;
(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

(f) "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;

(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

(i) "computer" means any electronic magnetic, optical or other high- speed data 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;

(j) "computer network" means the interconnection of one or more computers through:

(i) the use of satellite, microwave, terrestrial line or other communication media; and terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) "computer resource" means computer, computer system, computer network, data, computer data base or software;

(l) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programme, electronic instructions, input data .and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

(o) (o)Data contain all the information of knowledge facts which are in formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally m the memory of the computer;

(p) Digital signature include electronic data transaction;

(q) "Digital Signature Certificate" means a Digital Signature Certificateissued under sub-section (4) of section 35;

(r) "electronic form" with reference to information means any information generated, sent, received. or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means the Official Gazette published in the electronic form;

(t) "electronic record" contain all tne data that is images videos and songs etc, received or sent in an electronic form or micro film or computer generated micro fiche;

(u) "function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(v) "information" includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

(w) "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

(x) "key pair", in an asymmetric crypto system, means private key is mathematically related with public key while private key is generated with the digital signature;

(y) "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be, Regulations made by the President under article 240, Bills enacted as President' s Act under sub- clause (a) f clause (1) of article 357 of the Constitution and includes rules, regulations, bye- laws and orders issued or made there under;

(z) "licence" means a licence granted to a Certifying Authority under section 24;

(aa) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(bb) "prescribed" means prescribed by rules made under this Act;

(cc) (cc)"private key" means the key of a key pair used to create a digital signature;

(dd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ee) (ee)"secure system" means computer hardware, software, and procedure that-

(a) are reasonably secure from unauthorised access and misuse;
(b) provide a reasonable level of reliability and correct operation;
(c) are reasonably suited to performing the intended functions; and
(d) adhere to generally accepted security procedures;

(ff) All the Security procedure are provided by the central government;

(gg) "subscriber" means a person who is related with the digital signature.

(hh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether- 126 IPR and Cyber Laws (BSc IT)Information Technology Act, 2000 127

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

(3) Authentication of electronic records:

1. Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.
2. When cryptosystem as well as hash function is transfer from one electronic record to another electronic record they may be effected Explanation.- For the purposes of this subsection," hash function" means, an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible:

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
(b) that two electronic records can produce the same hash result using the algorithm.

3. Any person by the use of a public key of the subscriber can verify the electronic record.
4. The private key and the public key are unique to the subscriber and constitute a functioning key pair. **CHAP ELECTRONIC GOVERNANCE CHAPTER III ELECTRONIC GOVERNANCE.**

(4) Legal recognition of electronic records:

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is:

(a) rendered or made available in an electronic form; and
(b) accessible so as to usable for a subsequent reference.

(5) Legal recognition of digital signatures:

Every data should be authenticated by fixing one person 128 IPR and Cyber Laws (BSc IT)with digital signature with it, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government. Explanation.- For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" Shall be construed accordingly.

(6) Use of electronic records and digital signatures in Government and its agencies:

1. Where any law provides for:

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;
(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in Information Technology Act, 2000 129force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

2. The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe: the manner and format in which such electronic records shall be filed, created or issued; the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

(7) Retention of electronic records:

1. Where any law provides that documents are retained for some time of period, then, that requirement shall be deemed to have been satisfied if such documents records or information are retained in the electronic form, if:

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be 130 IPR and Cyber Laws (BSc IT)demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

2. Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

(8) Publication of rule, regulation, etc., in Electronic Gazette:

Where any law provides that any rule, regulation, order, bye- law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye- law, notification or any other matter is published in the Official Gazette or Electronic Gazette: Provided that where any rule, regulation, order, bye- law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to date of the Gazette which was first published in any form.

(9) Sections 6, 7, and 8 not to confer right to insist document should be accepted in electronic form:

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government. or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any

document in the form of electronic records or effect any monetary transaction in the electronic form.

(10) Power to make rules by Central Government in respect of digital signature:

The Central Government may, for the purposes of this Act, by rules, prescribe:

(a) the type of digital signature;
(b) the manner and format in which the digital signature shall be affixed;
(c) the manner or procedure which facilitates identification of the person affixing the digital signature;
(d) all procedures and control processes to ensure adequate integrity, security and confidentiality of electronic records or payments; and
(e) any other matter which is necessary to give legal effect to digital signatures.

(11) Attribution of electronic records:

An electronic record shall be attributed to the originator:

(a) if it was sent by the originator himself;
(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
(c) by an information system programmed by or on behalf of the originator to operate automatically.

(12) Acknowledgement of receipt:

1. Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by-

(a) any communication by the addressee, automated or otherwise; or
(b) Any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

2. Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.
3. Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and

specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

(13) Time and place of despatch and receipt of electronic record:

1. Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

2. Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:-

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,

(i) receipt occurs at the time when the electronic record enters the designated resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

3. Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched 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 lace of business.

4. The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under subsection (3).

5. For the purposes of this section,

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) “usual place of residence”, in relation to a body corporate, means the place where it is registered.

6.2 INFORMATION TECHNOLOGY ACT 2000- 2 (Sec. 14 to 42):

(14) Secure electronic record:

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic * i record from such point of time to the time of verification.

(15) Secure digital signature:

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was:

(e) unique to the subscriber affixing it;

(f) capable of identifying such subscriber;

(g) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

(16) Security procedure: The central Government prescribes security procedure with commercial circumstances prevailing at the time when the procedure was used, mckiding-

(h) the nature of the transaction; the level of sophistication of the parties with reference to their technological capacity;

(i) the volume of similar transactions engaged in by other parties;

(j) the availability of alternatives offered to but rejected by any party;

(k) the cost of alternative procedures; and

(l) The procedures in general use for similar types of transactions or communications.

(17) Appointment of Controller and other officers:

1. The Central Government may, by notification in the Official Gazette, appoint a Controller of Information Technology Act, 2000 137Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

2. The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

3. The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

4. The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

5. The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

6. There shall be a seal of the Office of the Controller.

(18) Functions of Controller:

The Controller may perform all or any of the following functions, viz.:

(m) exercising supervision over the activities of the Certifying Authorities;
(n) certifying public keys of the Certifying Authorities;
(o) laying down the standards to be maintained by the Certifying Authorities;
(p) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
(q) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
(r) All the document should be written printed and visually formulate and also make advertisement that may be distributed or used in respect of a Digital Signature Certificate and the public key;
(s) specifying the form and content of a Digital Signature Certificate and the key;
(t) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
(u) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
(v) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
(w) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
(x) resolving any conflict of interests between the Certifying Authorities and the subscribers;
(y) laying down the duties of the Certifying Authorities;

(z) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

(19) Recognition of foreign Certifying Authorities:

1. Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
2. Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
3. The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under subsection (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

(20) Controller to act as repository:

(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall:

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;
(b) observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.
(c) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

(21) Licence to issue Digital Signature Certificates:

1. Subject to the provisions of sub-section (2), any person may make an application, to theController, for a licence to issue Digital Signature Certificates.
2. No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital signature Certificates as may be prescribed by the Central Government.

3. A licence granted under this section shall-

(a) be valid for such period as may be prescribed by the Central Government;
(b) not be transferable or heritable;
(c) be subject to such terms and conditions as may be specified by the regulations.

(22) Application for licence:

1. Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.
2. Every application for issue of a licence shall be accompanied by:

(a) a certification practice statement;
(b) a statement including the procedures with respect to identification of the applicant;
(c) Central government make the fees aa twenty five thousand not more that;
(d) such other documents, as may be prescribed by the Central Government.

(23) Renewal of licence:

An application for renewal of a licence shall be:

(a) in such form;
(b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

(24) Procedure for grant or rejection of licence:

The Controller may, on receipt of an application under sub-section.

1. of section 21, after considering the documents accompanying the application and such other factors, as he deems fit,: grant the licence or reject the' application: Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

(25) Suspension of licence:

1. The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,-

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;
(b) failed to comply with the terms and conditions subject to which the licence was granted;
(c) failed to maintain the standards specified under clause (b) of sub-section (2) of section 20;
(d) contravened any provisions of this Act, rule, regulation or order made there under, revoke the licence: Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

2. The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by order suspend such licence pending the completion of any inquiry ordered by him: Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

3. No Certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during such suspension.

(26) Notice of suspension or revocation of licence:

1. Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data base maintained by him.

2. Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories: Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock: Provided further that the Controller may, if he considers necessary, publicise the contents of data base in such electronic or other media, as he may consider appropriate.

(27) Power to delegate:

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

(28) Power to investigate contraventions:

(a) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of theprovisions of this Act, rules or regulations made thereunder.

(b) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income- tax authorities under Chapter XIII of the Incometax Act, 1961 (43 of 1961) and shall exercise such powers, subject to such limitations laid down under that Act.

(29) Access to computers and data:

1. Without prejudice to the provisions of subsection (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Ac, rules or regulations made there under has been committed, have access to any computer system, any apparatus; data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

2. For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

(30) Certifying Authority to follow certain procedures:

Every Certifying Authority shall:

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;
(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and
(d) observe such other standards as may be specified by regulations.

(31) Certifying Authority to ensure compliance of the Act, etc.:
Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made there under.

(32) Display of licence:

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

(33) Surrender of licence:

1. Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

2. Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

(34) Disclosure:

1. Every Certifying Authority shall disclose in the manner specified by regulations:

   (a) its Digital Signature Certificate which contains the public key to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
   (b) any certification practice statement relevant thereto;
   (c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and
   (d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority' s ability to perform its services.

2. Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a digital signature which is granted by the central government, then, the Certifying Authority shall:

   (a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or
   (b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation. **CHAP DIGITAL SIGNATURE CERTIFICATES CHAPTER VII DIGITAL SIGNATURE CERTIFICATES**

(35) Certifying Authority to issue Digital Signature Certificate:

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.
(2) Every such application shall be accompanied by such fee not exceeding twenty- five thousand rupees as may be prescribed by the Central Government, to be paid to the

Certifying Authority: Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under subsection (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for' reasons to be recorded in writing, reject the application: Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that:

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;
(b) the applicant holds a private key, which is capable of creating a digital signature
(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant: Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

(36) Representations upon issuance of Digital Signature Certificate:

A Certifying Authority while issuing a Digital Signature Certificate shall certify that:

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder
(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it
(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate
(d) the subscriber' s public key and private key constitute a functioning key pair
(e) the information contained in the Digital Signature Certificate is accurate; and
(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

(37) Suspension of Digital Signature Certificate:

1. Subject to the provisions of sub-section
2. the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate
   (a) on receipt of a request to that effect from:

(b) All the subscriber are listed in digital signature if the subscriber not present then any other person should be appoint to manage that information;
(c) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.
(d) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

3. On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

(38) Revocation of Digital Signature Certificate:

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it:

(a) where the subscriber or any other person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital signature authorized by any time by the central government, if it is of opinion that:

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority' s private key or security system was compromised in a manner materially affecting the Digital Signature Certificate' s reliability;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound- up or otherwise ceased to exist.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

(39) Notice of suspension or revocation:

(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories. CHAP DUTIES OF SUBSCRIBERS CHAPTER VIII ' DUTIES OF SUBSCRIBERS.

(40) Generating key pair:

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber,then, the subscribe shall generate the key pair by applying the security procedure.

(41) Acceptance of Digital Signature Certificate:

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber are certifies all the information contained Signature Certificate that:

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

(42) Control of private key:

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

6.3 INFORMATION TECHNOLOGY ACT 2000- 3 (Sec. 43 to 45):

(43) Penalty for damage to computer, computer system, etc.:

If any person without permission of the owner or any other person who is incharge 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 data 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 authorised 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 thereunder;

(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” contain different computer instruction that are used to communicate with computer

(j) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(k) by any means to usurp the normal operation of the computer, computer system, or computer network;

(i) “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 in a formalised manner or have been produced by a computer,

computer system or computer network and are intended for use in a computer, computer system or computer network;

(ii) “Computer virus is always harmful to computer data that destroy ,damages and * degrades the performance of computer or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iii) “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:

(a)furnish any document, return or report to the Controller or 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;

(b) 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;

(e) 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 suchcontravention or a penalty not exceeding twentyfive thousand rupees. Sec. 65 to 78:

(65) Tampering with 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 up to three years, or with fine which may extend up to two lakh rupees, or with other. Explanation.- For the purposes of this section, ”computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

(66) Hacking with computer system:

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes is value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

(67) Publishing of information which is obscene in electronic form: Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend t 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 extends to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

(68) Power of Controller to give directions:

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities with the provisions of this Act, rules or any regulations made thereunder, as specified in the order if those are necessary to ensure compliance.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

(69) Directions of Controller to a subscriber to extend facilities to decrypt information:

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information. (3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

(70) Protected system:

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised 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 1 able to fine.

(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 Digital 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.

(72) Penalty for breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers confeired under this Act, rules or regulations made there under, 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.

(**73) Penalty for publishing Digital Signature Certificate false in certain particulars:**

(1) No person shall publish a Digital 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 digital signature created prior to such suspension or revocation.

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

(74) Publication for fraudulent purpose: Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose 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.

(**75) Act to apply for offence or contravention committed outside India:**

(1) Subject to the provisions of sub-section (2)the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

(76) Confiscation: Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation: Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court' may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

(77) Penalties or confiscation not to interfere with other punishments: No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

(78) Power to investigate offences: Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

CHAP NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES CHAPTER XII NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

6.4 INFORMATION TECHNOLOGY ACT 2000- 4 [Sec. 46 to 64):

(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 thereunder 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 for 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 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. Where more than one adjudicating officers 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 subsection (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; m the amount of loss caused to arty person as a result of the default;

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

(c) the repetitive nature of the default.

(48) Establishment of Cyber Appellate Tribunal :

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations 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.

(49) Composition of Cyber Appellate Tribunal: A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

(50) Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal: A person shall not be qualified for appointment asthe Presiding Officer of a Cyber Appellate Tribunal unless he: (a) is, or has been, or is qualified to be, a Judge of a High Court; or (b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

(51) Term of office: The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty- five years, whichever is earlier.

(52) Salary, allowances and other terms and conditions of service of Presiding Officer: The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed: Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

(53) Filling up of vacancies: If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the

provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

(54) Resignation and removal:

(1) The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office: Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the 4 charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

(55) Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings:

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and n act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

(56) Staff of the Cyber Appellate Tribunal:

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

(57) Appeal to Cyber Appellate Tribunal:

(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an ' adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty- five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty- five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

(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 (5 of 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 (5 of 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 it 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 (45 of 1860) and the Cyber Appellate shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

(59) Right to legal representation:

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

(60) Limitation:

The provisions of the Limitation Act, 1963 (36 of 1963), shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

(61) Civil court not to have jurisdiction:

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

(62) Appeal to High Court:

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order: Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

(63) Compounding of contraventions:

(1) Any contravention under this Chapter may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify: Provided that such sum shall t ^not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so . compounded.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded. Explanation: For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention

(3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

(64) Recovery of penalty:

A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid. CHAP OFFENCES CHAPTER XI OFFENCES

6.5 INFORMATION TECHNOLOGY ACT 20005 (Sec. 79 to 90):

(79) Network service providers not to be liable in certain cases:

or the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Act, rules or regulations made thereunder for any third party Explanation - For the purposes of this section:

(a) “network service provider” means an intermediary;

(b) “third party information” means any information dealt with by a network service provider in his capacity as an intermediary;

(80) Power of police officer and other officers to enter, search, etc.:

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised; by the Central Government in this behalf may enter any public place and search and arrest without warrant any person fotind therein who is reasonably suspected or having committed or of eaiaamuting or of being about to commit any offence under this Act. Explanation.- For the purposes of this sub-section, the expression "public place” includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under subsection (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer- in charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

(81) Act to have overriding effect:

The provisions of this Act shall ' have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

(82) Controller, Deputy Collector and Assistant Controllers to be public servants:

The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deertied t be public servants within the meaning of section 21 of the Indian Penal Code (45 of 1860).

(83) Power to give directions:

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

(84) Protection of action taken in good faith:

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Presiding Officer, adjudicating officer and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.

(81) Act to have overriding effect:

The provisions of this Act shall ' have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

(82) Controller, Deputy Collector and Assistant Controllers to be public servants:

The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deertied t be public servants within the meaning of section 21 of the Indian Penal Code (45 of 1860).

(83) Power to give directions:

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

(84) Protection of action taken in good faith:

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Presiding Officer, adjudicating officer and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.

(85) Offences by companies:

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of and was responsible to, tile company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this subsection shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention,

(2) Notwithstanding anything contained in subsection

(1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly. Explanation.- For the purposes of this section

,(i) “company” means any body corporate and includes a firm or other association of individuals; and (ii) “director”, in relation to a firm, means a partner in the firm.

(86) Removal of difficulties:

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty: Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

(87) Power of Central Government to make rules:

(1) The Central Government may, by notification in the Official Gazette and in the Electronic Gazette make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the - generality of the foregoing power, such rules may provide for all or any of the following matters, namely:

(a) the manner in which any information or matter may be authenticated by means of digital signature under section 5;

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

(c) the manner and format in which electronic records shall be filed, or issued and the method of payment under sub-section (2) of section 6;

(d)the matters relating to the type of digital signature, manner and format in which it may be affixed under section 10;

(e) the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16; w the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers under section 17;

(g) other standards to be observed by the Controller under clause (b) of sub-section (2) of section 20;

(h) the requirements which an applicant must fulfil under sub-section (2) of section 21;

(i) the period of validity of licence granted under clause (a) of sub-section (3) of section 21;

(j) the form in which an application for licence may be made under sub-section (1) of section 22;

(k) the amount of fees payable under clause (c) of sub-section (2) of section 22;

(1) such other documents which shall .accompany an application for licence under clause (d) of sub-section (2) of section 22;

(m)the form and the fee for renewal of a licence and the fee payable thereof under section 23;

(n) the form in which application for issue of a Digital Signature Certificate may be made under sub-section (1) of section 35;

(o) the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;

(P) the manner in which the adjudicating officer shall hold inquiry under subsection (1) of section 46; .

(q) the qualification and experience which the adjudicating officer shall possess under sub-section (3) of section 46;

(r) the salary, allowances and the other terms and conditions of service of the Presiding Officer under section 52;

(s) the procedure for investigation of misbehaviour or incapacity of the Presiding Officer under sub-section (3) of section 54;

(t) the salary and allowances and other conditions of service of other officers and employees under sub-section (3) of section 56;

(u) the form in which appeal may be filed and the fee thereof under sub-section (3) of section 57;

(v) any other power of a civil court required to be prescribed under clause (g) of subsection (2) of section 58; and

(w) any other matter which is required to be, or may be, prescribed. (3) Every notification made by the Central Government under clause (f) of sub-section (4) of section 1 and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or the rule or both Houses agree that the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any success modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

(88) Constitution of Advisory Committee:

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee. (2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non- official members representing the interests principally affected or having special knowledge of the subject- matter as the Central Government may deem fit. (3) The Cyber Regulations Advisory Committee shall advise

(a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the Controller in framing the regulations under this Act. (4) There shall be paid to the non- official members of such Committee such travelling and other allowances as the Central Government may fix.

(89) Power of Controller to make regulations:

The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations cons stent with this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:

(a) the particulars relating to maintenance of data- base containing the disclosure record of every Certifying Authority under clause (m) of section 18;

(b) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under subsection (1) of section 19;

(c) the terms and conditions subject to which a licence may be granted under clause (c) of sub-section (3) of section 21;

(d) other standards to be observed by a Certifying Authority under clause (d) of section 30;

(e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;

(f) the particulars of statement which shall accompany an application under subsection (3) of section 35;

(g) the manner in which the subscriber shall communicate the compromise of private key to the Certifying Authority under subsection (2) of section 42.

(3) Eveiy regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in sesskm, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation, regulation should not be made, the regulation shall thereafter have

(90) Power of State Government to make rules:

The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act. (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:

6.5 INFORMATION TECHNOLOGY ACT 2000- 6 (Sec. 91 to 94):

(91) Amendment of Act 45 of 1860: The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

(92) Amendment of Act 1 of 1872: The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

(93) Amendment of Act 18 of 1891: The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

(94) Amendment of Act 2 of 1934: The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act.

6.6 THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008:

The Government of India has brought major amendments to ITA-2000 in form of the Information Technology Amendment Act, 2008. ITAA 2008 (Information Technology Amendment Act 2008) as the new version of Information Technology Act 2000 is often referred has provided additional focus on Information Security. It has added several new sections on offences including Cyber Terrorism and Information Technology Act, 2000 191 Data Protection. A set of Rules relating to Sensitive Personal Information and Reasonable Security Practices (mentioned in section 43A of the ITAA, 2008) was released in April 2011.

Criticisms:

The amendment was passed in an eventful Parliamentary session on 23rd of December 2008 with no discussion in the House. Some of the cyber law observers have criticized the amendments on the ground of lack of legal and procedural safeguards to prevent violation of civil liberties of Indians. There have also been appreciation about the amendments from many observers because it addresses the issue of Cyber Security. Section 69 empowers the Central Government/State Government/ its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence. They can also secure assistance from computer personnel in decrypting data (see mandatory decryption), under penalty of imprisonment.