

ideologies, come to terms with the market forces, and accept a globalised free market economy.

Such a scenario in the world wherein there are dramatic changes in the information and communication technologies the business transactions are being made with the help of computers. Business community as well as individuals are increasingly using computers to create, transmit and store information in the electronic form instead of the traditional paper documents. Information stored in the electronic form is very cheap, easier to store and retrieve, speedier, and long lasting, unlike paper documents. Now, business people have realised the advantages of business transaction in the electronic form. Such a change of thinking of business people as well as the availability of the facilities in the form of computers and electronic commerce has made it essential to have an effective legal regime for governing the e-commerce and business transactions properly and effectively.

### **Need for Cyber Laws**

The utility of computers and the Internet is well understood and in fact embedded in the modern business and commerce as well as in the society in general. The advantages of the use of computers and internet are immense in the modern business and our society cannot smoothly function without computers and information technology (IT). But the use of internet and computers has brought along many unavoidable misuses of computer and the internet. This has been easily possible more so because, in the use of the computers, there is no territorial limit and can be used from any jurisdiction. This sort of freedom has helped many computer experts indulging in unlawful cyber criminal activities across the world. Hacking, bugging, cheating, pornography, embezzlement, fraud and so on have become very popular on the internet. In the 'Times City' (Times of India) it was reported that the cases of credit card fraud have shot up these days<sup>1</sup>. It was reported that, according to the Delhi Police, complaints of online credit card frauds have seen a sharp increase in the past two years. And since online transactions are one-sided, customers end up paying for frauds. Moreover, there is counterfeiting of plastic money. It may be that someone got hold of your card details and copied them onto a bogus card, and started spending your money<sup>2</sup>.

It is alarming to find that now a days even terrorists plot terror over the Internet. It is reported by the US officials that four Caribbean men who plotted to carry out attacks on fuel tanks and lines leading to the John F. Kennedy airport had conducted "precise and extensive" surveillance using photographs, video, and satellite images downloaded from the Google Earth. Such an act of plotting terror jolted the American national security establishment<sup>3</sup>.

1. 'Times City', *The Times of India*, New Delhi, July 30, 2007, p. 7.

2. *Ibid.*

3. *Times of India*, New Delhi, June 6, 2007, p. 15.

The above instances point the importance and need to have proper legislation to curb the menace of modern kinds of cyber crimes on the Internet. At present legal provisions recognise paper based records and documents, which bear signatures. But the e-commerce, eliminates to a great extent the need for paper based transactions, and therefore in order to facilitate and promote it, there is an imminent need for cyber laws.

The United Nations Commission on International Trade Law adopted the Model Law on Electronic Commerce in 1996. India is a signatory to this and has therefore to revise the laws accordingly. Keeping in view the urgent need to bring suitable changes in the existing laws to facilitate e-commerce and e-governance, the Information and Technology Bill, 1999 was introduced in the Parliament in India. Now India has the Information Technology (IT) Act, 2000, which has been enacted keeping in view the necessity of proper regulation of IT to have proper e-commerce and e-governance in India. It is to be seen that there are two principal hurdles which stand in the way of facilitating these two in India. First, the need for writing and secondly, signature. At present many legal provisions assume the existence of paper based records and documents and the need for these to bear signatures. In order to facilitate e-commerce and e-governance, the Information Technology Act, or the IT Act 2000 made changes in the Law of Evidence which is traditionally based upon paper-based records and oral testimony. The International Trade, through the medium of e-commerce, is growing rapidly in the past few years and therefore many countries have switched over from the traditional paper-based commerce to e-commerce. Therefore, the Act also provides for legal recognition of electronic records and electronic signatures. Such changes in laws will enable the conclusion of contracts and the creation of rights and obligations through the electronic medium. The new law also provides for the use and acceptance of electronic records and electronic signatures in government offices and its agencies. It is hoped that the Indian citizen's interaction with the governmental offices will be hassle free very soon. Consequently, the necessary changes in the laws in the Indian Penal Code (IPC) and The Indian Evidence Act 1872 have also been made.

### **Historical Perspective**

Let us now take a historical perspective of the issue at hand.

### **Impact of the Internet and Information Technology (IT) on Business and Society**

The Internet reflects the immense power in cyber space as the latest step in network development. The Internet was originally conceived and developed with the same spirit of collaboration and cooperation that it now fosters. This network of networks stands in stark contrast to the public telecommunication networks

that had slowly developed under central control and private telecommunication networks that served limited groups and users. The Internet has emerged as fundamentally decentralised and open. It offers a communication medium to people all over the globe, from all works of life, using all kinds of devices, uniform only in its enabling protocol<sup>4</sup>.

The Internet, because of its open architecture, digital format and unifying protocols, has emerged as the platform to support increased connectivity and interaction among networks. Computer and computer storage use digital formats, and the networks in which they operate are digital networks. This is an important distinction between present and past technologies, as well as the underlying reason for the seemingly sudden interoperability of formally distinct technologies. Since images, sound, text and video can all be digitised, boundaries between formerly distinct networks are fading and opportunities for interoperability are increasing<sup>5</sup>.

The technological developments occurring today offer a vision of the future marked by dramatic new capabilities in processing speed, transport and storage of data. The constraining influence of bandwidth is beginning to diminish as communication technologies continue to improve. With robust competition among telephone, cable and wireless companies, as well as improvements in transmission media-optical fiber, twisted-pair copper wire, coaxial cable and various wireless technologies, we can move data more efficiently across communications networks. We may reach the point where anything that can be digitised can be delivered efficiently to an ever-growing number of users and where the marginal cost of transport approaches zero.

The technological changes that are taking place in processing, data storage, to develop and communicate on the Internet are changing the relative costs of many systems. This in turn has the potential to change the products and services that are available. The most fitting example is the development of packet switching, fundamental to the development of the internet, which can be seen as substituting relatively cheap processing at the network's edge for relatively expensive circuit-switched transport<sup>6</sup>.

## The Character and Use of Internet Technologies

Industrial heterogeneity is likely to be the rule of the day. Information technologies and their applications are totally characterised by heterogeneity. People access the internet by using a wide variety of devices that range from high-performance workstations to handheld appliances. The competitive and

4. Ryder, Rodney D., *Guide to Cyber Laws*, 3rd ed., Wadhwa & Company, New Delhi, 2007, pp. 4–5.

5. *Ibid.*, p. 5

6. *Ibid.*, p. 31.

heterogeneous marketplace increases the importance of the role of standards. The unifying nature of the Transmission Control Protocol/Internet Protocol (TCP/IP) has been critical to Internet's success. Given the increasing importance of IT and telecommunications, the role of standards of technologies will become even crucial and contentious in the future<sup>7</sup>.

The Internet gives us all the opportunity to act as a global community, to advertise and operate across all frontiers, over borders, and beyond the control of any national government. The intense volume of information and the simplicity of its transfer causes some problems. Ownership of information is very hard to protect, the illicit reuse of copyright material is commonplace, the spreading of false and malicious information is also a daily occurrence. Therefore, the aim of cyber or cyber-related laws world-wide is to harmonise the existing laws and the ultimate aim of legislation world-wide should be to reduce the costs of world trade by issuing out inconsistencies and uncertainties resulting from differences in the municipal laws<sup>8</sup>.

Online services, through the Internet and other forms of electronic communication—both interactive and otherwise—are re-shaping the way the world handles information and does business. Lawyers themselves are both the guardians of integrity of business process and intensive users of information. And they have come to terms with these new methods of transmitting, storing and using information. Lawyers have to focus on the future to anticipate the problems, which IT can produce, and to develop answers which the business world will need, to ensure the safe evolution of new methods of doing business<sup>9</sup>.

We are living in a society in which existing legal frameworks are constantly challenged by the technological advancement. This creates a need to constantly update and adapt the way in which we organise ourselves in order to maintain the State's overall control of its domestic affairs and national interest<sup>10</sup>.

Nowadays we see the importance of information highways' which means merging of all sources of information into a single retrievable database. For instance, every home, office, news medium, library, data bank business, government agency and computer will be connected to every device, such as telephone, television, or personal computer. The advent of the Internet has thus, revolutionised the global market place. Products and services once offered only at the local store are now available to the consumers at every corner of the planet<sup>11</sup>.

Around the world, e-commerce is the subject of intense interest in many sectors: in government, business, service sector, amongst consumers and academics. E-commerce has expanded from the closed world of business-to-business transactions between non-parties to encompass a complex web of

7. *Ibid.*, p. 33.

8. *Ibid.*, p. 38.

9. *Ibid.*, p. 41.

10. *Ibid.*, p. 43.

11. *Ibid.*, p. 44.

## CHAPTER 6

# Protection of Intellectual Property Rights in Cyberspace in India

### The Cyberspace

Web-based technology through the Internet has increased our capacity to access it easily with rapid speed which is very useful for e-commerce and having quick electronic business transactions. Information stored in electronic form is cheaper, easy to store, retrieve, and speedier to communicate. The advantages of the Internet have naturally attracted many business people to conduct the business through e-commerce. The present millennium is going to witness a new internet culture which will be a driving force in the days ahead and is bound to change the way the modern business will function through cyberspace and the Internet. Internet originally was confined to military establishments. But Internet has due to its speed, interactivity and flexibility tremendous potential to disseminate information beyond the geographical boundaries. The Diverse activities which at present are possible over the internet might not have been even envisioned by its inventors. The rapid changes in the process have not yet ended and they are still evolving<sup>1</sup>. All the facets of business transactions with which we are accustomed in physical environment can be now executed over the internet. These transactions include among others online advertising, online ordering, publishing, banking, investment, auction and also professional services<sup>2</sup>. Internet has made it possible to replace traditional paper-based communications by paperless communication which does not know physical or geographical boundaries, and is possible in any part and from any part of the globe between the parties known or unknown to each other. The efficiency and speed brought by this technology has made it as matchless alternative in electronic commerce.

1. See Cole, Patrick E., et.al, "Business—The Internet Economy", *Time*, July, 20, 1998, p. 34.

2. See House of Commons Research Paper available at <http://www.parliament.uk>.

With its global reach, the Internet provides the intellectual property owners with a seemingly unlimited market for their works. However, the internet offers similarly expanded opportunities for those seeking to infringe the rights of others, while making the detection and elimination of such infringement extremely difficult. The challenge that the law has faced in the recent years is how to tackle the development of intellectual property on the internet while preventing its unauthorised exploitation. We find that the advantages of Internet have brought some legal issues which do not find solutions in the existing legal framework which was enacted to suit the needs of physical environment and tangible medium and not the cyberspace which is faceless and borderless. And the most important of the many legal issues raised by the internet is the protection of the copyright. Till recently, Internet, because of the lack of technology, was used sparingly to disseminate only one or two works over which the copyright could be claimed. However, Internet, which is a multimedia, has made it possible through a single medium not only to disseminate all works over which copyright can be claimed but also to create new works which deserve copyright protection but are not covered in the present Copyright Act, 1957.

Even before the advent of Internet, the copyright issues cropped up by the introduction of other technologies also. However, none has brought more pressing copyright concerns than digitalisation<sup>3</sup>. The flexibility of digital technology which makes possible text, sound and images to be transmitted and stored in easily manipulated bits and bytes has been credited with transforming information from simply a means of acquiring and managing other assets into a primary asset itself<sup>4</sup>.

Intellectual property owners have to make difficult decisions about how to allocate resources to identify and stop infringement. As Internet infringement involved generally in fan-organised websites devoted to popular culture, the intellectual property owners risk alienating their consumers by a possible public relations backlash by too aggressively protecting their intellectual property rights. Moreover, the intellectual property owners must be aware of new forms of possible intellectual property infringement that arise from the unique nature of internet technology. These include linking, framing, the use of metatags, spamming etc.

Intellectual property means knowledge or information in any form which has a commercial value and intellectual property rights can be defined as a mix of ideas, inventions and creations on which society provides the status of property. And the protection of the intellectual property right systems include a range of laws, institutions and arrangements. Until now the protection of law institutions

3. Gailey, Elizabeth Atwood, "Who Owns Digital Rights? Examining the Scope of Copyright Protection for Electronically Distributed Works", *Communications and the Law*, p. 3. Quoted in *Law of Copyright from Gutenberg's Invention to Internet*, by A.K. Koul and V.K. Ahuja, Faculty of Law, Delhi, 2001, at p. 183.

4. Branscomb, Who Owns Information? From Privacy to Public Access, p. 1 (1994), Quoted in *Ibid* at p. 183.

and arrangements were based on essentially national legislations. However, recently international regimes for the protection of intellectual property have been brought under the umbrella of World Intellectual Property Organisation (WIPO) on the one hand and the World Trade Organisation (WTO) on the other hand. These international regimes, for the protection of intellectual property, attempt to strike a balance between the interest of the intellectual property owner and its interests of the intellectual property users by ensuring the owners of intellectual property adequate return on their investment in knowledge and increasing social benefits from unrestricted access to knowledge to the intellectual property users. This aspect can be clearly pointed out by the agreement on TRIPs in the WTO. The TRIPs agreement imposes minimum standards on patents, copyright, trademarks and the trade secrets. And these standards which are applicable to all WTO members are based almost entirely on intellectual property legislation in the industrialized countries particularly the US.

### The Relevance of Domain Names in Intellectual Property Rights

In the new e-commerce economy it is important that before doing any sort of business activity a company must be easily traceable on the Internet. This means that the company must have an address in the cyberspace. This requires the company must have registration under a particular domain name and a website of its own. The Domain Name System (DNS) has made it possible for the registration of a company which enables a company to conduct online transactions and make it easily traceable by the customers, suppliers and other users. As it is difficult to remember all-numeric addresses which each computer, public server has its own unique all-numeric IP addresses and therefore domain name has a major role to play in the development of the DNS and the emergence of domain names as important corporate assets. The growth of e-business organisations or companies have to cater to new markets for which the Internet is to play an important role. As a consequence, it is important for a company to secure an appropriate domain name. For this, the domain name and the protection of the company's right to use it are the aspects which every organisation or company has to face. The domain names serve a number of useful purposes and will rapidly grow to form the fulcrum of a company's visibility and marketing operations. Once there is domain name of the company it will soon be remembered only through its web address rather than its geographical or telephonic addresses and numbers. The representation of the company's both name and address on the Internet can serve as a typical trademark function of showing a company's recognition and goodwill in the market place. Therefore, domain name is relevant as the consumers often see them as performing in e-commerce, the same role as trade marks and trade names have played in the traditional modes of business.

Various types of domain name disputes have come for consideration before the courts all over the world. One of the most serious kinds of disputes has been about 'Cybersquatting' which involves the use of a domain name by a person with neither registration nor any inherent rights to the name.

### Deception by Squatting in Cyberspace

The consumers when looking to find the name of the brand on the Internet, the easiest way for them is to type a domain name of the brand or the company. Generally, in India, a domain name has at least two key parts. The second level domain describes like .Com or .Gov and third level domain contains familiar name that describes product, service or topic that the website addresses. The popularity of Internet in advertising, recruiting and for market place for products and services by the companies on the Internet have the interest and desire to have domain names which are easy to remember and they relate to the product trade names or trademarks such as www.rediff.com. Such kind of identification is essential for any business in order to conduct commerce on the Internet and also advertise and educate the public about the company's product. It helps the consumers realise that they are communicating with the intended source of goods and they are confident of purchasing the genuine goods and are getting from known and reliable source. Internet serves with anonymity and has increased the importance of identity by brand name on the Internet. Trademarks and domain names being similar, have been exploited by some people who register trademarks of others as domain names and sell those domain names back to the trademark owners or third parties at a high profit. This is known as 'cybersquatting' which means some person sitting on the property of another person. Such a trend of cybersquatting has led the courts to consider the relationship between trademarks and domain names in *Intermatic Inc. v. Toeppen*<sup>5</sup>, wherein a US court found that the offer to sell a domain name in the US was 'use in commerce' and therefore it amounts to a trademark's use. And the court held that such an offer to sell a domain name to the owner of an identical or similar trademark was a trademark infringement. The practice of cyber squatting is abusive whereby one entity registers a domain name that includes the name or trademark of another. This practice shows the importance of the role played by domain names in establishing online identity. This practice usually is famous in order to either block the legitimate user registering its most sought after domain name or hoping to sell the names for profit in the market.

The practice of cybersquatting has resulted in litigation in various cases. In *Marks & Spencer Plc v. one in a Million*<sup>6</sup> case in the UK, the court granted an injunction to prevent cybersquatting on domain names involving well known brands like *Marks and Spencer*. In India, UK, Italy, Germany and the US and

5. 947 Fed. Supp. 1227 (N.D.III. 1996).

6. 1998 FSR 265.

many other countries the authorities concerned with the domain names have ruled that the act of registering a domain name similar to or identical with a famous trademark is an act of unfair competition whereby the domain name registrant takes unfair advantages of the goodwill and fame of the trademark by increasing traffic to the domain or to seize a potential assets of the trademark owner in the hope that the trademark owner will pay the registrant to relinquish the domain name. In cases relating to the infringement of domain name which have been decided in favour of the trademark owners we find that the domain registrant has acted without the intention to make use of the domain name as intended by the domain registration system. The absence of such intention is called *bad faith*. This is generally done for the profits of potential sale of the domain name to the trademark owner.

In this connection the most significant case decided by the Delhi High Court is *Yahoo! Inc. v. Akash Arora & Anr*<sup>7</sup>. In this case the Internet search engine Yahoo! Inc. sued an Internet pirate who had not only copied the domain name *Yahooindia.com* but had also used Yahooindia as a trademark on its website and was offering directory services with information specific to India. And was passing itself off as an extension of Yahoo! Inc. In this case the Delhi High Court granted an injunction restraining him from using Yahoo either as a part of his domain name or as a trademark or from copying any of the contents of the plaintiff's website and thereby infringing Yahoo's copyrights. The court further held that trademark law applies with equal force on the Internet as it does in the physical world<sup>8</sup>. But it may be noted that the principles of trademark law apply on the Internet with a different and with stricter standards. In *tanishq.com*, *Nasscom.org* and *tatasons.com* cases also, the courts have followed the same approach as in the case of Yahoo! Inc<sup>9</sup>.

Eventhough the courts have laid down the principles for violating the infringement of domain name or trademark on the cyberspace, there are still some difficulties in implementing such violations. One of the difficulties is of detecting the wrong or of serving the notice to the defendants. Secondly, there is the risk of the domain name being transferred if you give the cease and desist notice. Thirdly, even if you get an injunction, there is a possibility that the defendant would get registration of alpha-numeric variations as was found in the Tata cases. Such situations make the enforcement an expensive affair.

In this connection it may be pointed out that the Internet Corporation of Assigned Names and Numbers (ICANN) has adopted a policy called Uniform Domain Name Dispute Resolution Policy (UDRP) which offers an expedited administrative proceedings for trademark holders to contest 'abusive registrations of domain names' which provides cancellation, suspension or transfer of a domain name by the registrar. The advantages of the ICANN's dispute system

## Some Leading Cases Involving Complaints from India before WIPO

A number of cases have been filed before the World Intellectual Property Organisation (WIPO) where the complainants have been well known Indian corporate houses or media companies. In most of the cases the Indian complaints involving domain names before WIPO have been decided in the favour of the complainants. We may cite two important cases relevant for this purpose.

In *Tata Sons Ltd. v. The Advanced Information Technology Association*<sup>13</sup>, it was decided by the WIPO Administrative Panel, Instructing Network Solutions Inc. to transfer the impugned domain name *tata.org* to the complainant Tata Sons Ltd. The administrative panel relied on the decisions that had been earlier given in favour of Tata Sons Ltd. by the Indian courts providing protection to the Tata trademark from abusive registrations. In this case the panel held that the respondent had not even activated its website was itself indicative of bad faith.

Similarly in *tridenthotels.com* case the complainant was Oberoi Hotels which owned the trademarks 'Trident' and 'Trident Hotels' in India. In this case the panel held that the use of the word 'Trident' in combination with the word hotels has a certain distinctive character as it indicates a chain hotels such as the complainants group. The domain name *tridenthotels.com* signifies that the domain name was intended to be used for a chain of hotels. It was held by the administrative panel that this was indicative of the bad faith on the part of the respondent.

## Protection of Copyright on Cyberspace

The new technology which is multi-functional IT or the Internet poses number of challenges for laws to protect copyrights. Copyright being an intellectual property gives rights to the authors in literary, artistic, dramatic and musical works. As in other intellectual property rights available under the copyright are essentially negative in nature, similarly these are basically the rights to stop others from doing certain things as for example, right to stop piracy, counterfeit, copying or imitations. The copyright even enables the holder to stop even the third parties who might independently reach the same idea from exploiting them without the permission of the copyright owner. It means that the copyright holder has a right to control the activities of others. Therefore, copyright is rightly called as 'bundle of rights' such as right to reproduce work in copies, right to make an adaptation of the copyrighted work, right to perform or display the work in public etc. However, it may be pointed out that copyright does not exist in an idea but is available only when it is in some form or expression. Therefore, no person can have a copyright merely on having idea of story which is only in his

7. 1999 PTC 201.

8. *Ibid.*

9. *Ibid.*

13. Cited from [www.arbiter.wipo.int](http://www.arbiter.wipo.int).

mind. But once a person has written it he will have the copyright on the story which he expressed.

In India 'copyright' means the exclusive right subject to the provisions of the law to do or authorise the doing of act in respect of work or any substantial part of work.

- (a) In the case of literary, dramatic or musical work not being a computer programme to reproduce the work in any material form including the storing of it in any medium by electronic means, to issue copies, to perform the work in the public, to make any cinematograph film, or sound recording, to make any translation or to make any adaptation<sup>14</sup>.
- (b) In the case of computer programme to—
  - (i) do any of the acts specified in clause(a); and
  - (ii) sell or give on commercial rental or offer for sale or for commercial rental any copy of the computer programme.

Provided that such commercial rental does not apply in respect of computer programmes where the programme itself is not the essential object of the rental<sup>15</sup>.

In relation to computer programmes 'literary work' includes computer programmes, tables and compilations including computer databases<sup>16</sup> and an 'author' means in relation to a literary work or dramatic work the author of the work, in relation to a musical work, the composer, and in relation to any literary, dramatic, musical or artistic work which is computer generated, the person who cause, the work to be created<sup>17</sup>.

The above relevant provisions relating to the Copyright Law in India clearly suggest the interpretation that the copyright in computer software would subsist in case the computer software produced entity only if the computer produced entity is 'original' and a copyright subsists only in an original literary work. The copyright Act is not concerned with the originality of ideas but is concerned with the expression of thought, and in the case of a literary work with the expressions of thought in print or writing what is required is that the work must not be copied from another work but must originate from the author. The requirement for the purpose of a copyright is that the work originated from the author though the materials on which it is based might have been used by others earlier also. If labour, skill, judgement and learning with the materials which gives the product may not be either novel, or ingenious, it would be the claimant's original work because it is originated by him, emanated from him and not copied. Copyright subsists in a computer programme provided sufficient effort or skill has been done to give it a new and original character. However, a computer programme which only produces the multiplication tables or the alphabet cannot claim a copyright protection as the skill or effort used is very little<sup>18</sup>.

14. Section 14, The Copyright Act, 1957.

15. Section 14(b), *Ibid.*

16. Section 2(o), *Ibid.*

17. Section 2(d), *Ibid.*

18. Section 13, *Ibid.*

In India, the definition of computer includes any electronic or similar device having information processing capabilities<sup>19</sup>. And, a computer programme means a set of instructions expressed in words, codes, schemes or in any other form, including a machine, readable medium, capable of causing a computer to perform a particular task or achieve a particular result<sup>20</sup>.

"Communication to the Public" means making any work available for being seen or heard or otherwise enjoyed by the public directly or by any means of display or diffusion other than by issuing copies of such work regardless of whether any member of the public actually sees, hears or otherwise enjoys the work so made available.

*Explanation:* For the purposes of this Clause, communication through satellite or cable or any other means of simultaneous communication to more than one household or place of residence including residential rooms of any hotel or hostel shall be deemed to be communication to the public<sup>21</sup>.

The Indian law about copyright is based on Article 10 of the TRIPs Agreement which deals with computer programmes and stipulates that computer programmes shall be treated as literary works under Berne Convention.

There are various kinds of software based on their availability on the Internet and can be classified as follows:

- Commercial software
- Freeware
- Shareware
- Copy lifting software

Though there are different kinds of software as mentioned above, the law relating to protection of copyright doesn't make any distinction among any of these software's. Under the law in India all kinds of software have been given similar protection for the purposes of copyright.

Computer software that is sold for a price is called commercial software. It may be pointed out that it is only with respect to commercial software a large scale computer piracy is done. This aspect of piracy of commercial software is the basic concern of the copyright law. In the case of computer freeware, the software is fully available on the Internet free of cost. And therefore, the user of such software has not to pay anything to the author and if the user wishes he may appreciate the work of the author and acknowledge the benefit he derived from the use of the author's work. A shareware is a software that is distributed openly and widely for users to try before they buy that programme. Whereas in copy lifting, the user can use the software for as long as he likes freely. And he is even allowed to change, alter or add to the code and also pass the original work with modifications with or without a fee, which is prohibited in shareware software and freeware.

19. Section 2(ffb), *Ibid.*

20. Section 2(fcc), *Ibid.*

21. Section 2(ff), *Ibid.*

It may be explained that the software is created or developed by the owner or author either online or offline. Then the owner/author of the software uploads the content on the internet which in turn is transmitted from one website to another website with great speed. From a website, a user can have access to the software through the search engine. The user may download the software from the website and may use it online or offline. Therefore, a Software on the Internet—

- can be created online or offline;
- is made available online; and,
- can be used by the internet user online or offline. The law of copyright is relevant at all the levels of transactions on the Internet. The law confers the exclusive right on the owner/author with respect to the computer software created by him. However, the infringements of his copyright can take place during the transmission of message or with respect to how the software is used.

### Rights of Software Copyright Owners

We have briefly pointed out the rights of the copyright owner as provided for under Section 14 of the Copyright Act, 1957. Here we will explain to understand the copyrights particularly of the software copyright owners.

- First the author of the software has the right to reproduce and make any number of copies of his work as he likes.
- Secondly the software copyright owner may display his software on the Internet which would amount to display to the public which right is provided under Section 14(d) of the Copyright Act and if a defendant by making available copyrighted product online will be liable, for violation of the right of public display and distribution of the copyrighted work in violation of author's copyright<sup>22</sup>.
- The owner of the copyright software enjoys an exclusive right to distribute copies of the work to the public by sale or by transfer of ownership or by rental. This right to distribute in India flows from Section 14 of the Copyright Act, 1957, which provides the right to publication. The software author's right of commercial rental to the public is recognised by TRIPS Agreement in Article 11 and Article 14(4) and by Article 7 of the WIPO Copyright Treaty.
- Similarly, the owner of the software copyright has the right to adaptation of his work by updating, changing and modifying his software copyright. No other person than the owner of the copyright software has the right to modify or change his work whether a new work is created or not.

22. *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp 1552.

### Infringement of Copyright on Cyberspace

Under the law, copyright in a work shall be deemed to be infringed—

- (a) when any person, without a license granted by the owner of the copyright or the Registrar of Copyrights under this Act, or in contravention of the conditions of a license so granted or of any condition imposed by a competent authority under this Act—
  - (i) does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright;
  - (ii) permits for profit any place to be used for the communication of the work to the public where such communication constitutes an infringement of copyright in the work, unless he was not aware and had no reasonable ground for believing that such communication to the public would be an infringement of copyright; or
- (b) when any person—
  - (i) makes for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire; or
  - (ii) distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright; or
  - (iii) by way of trade exhibits in public; or
  - (iv) Imports into India<sup>29</sup> ...

There is no definition of infringement provided under the Copyright Act 1957. However, Section 2(m) gives the meaning to the words 'infringing copy', is in relation to—

- literary, dramatic, musical or artistic work, a reproduction thereof otherwise than in the form of a cinematographic film;
- a cinematographic film, a copy of the film made on any medium by any means;
- a sound recording, any other recording embodying the same sound recording, made by any means;
- a programme of performance in which such a broadcast, reproduction right or a performer's right subsists under the provisions of this Act, the sound recording or a cinematographic film of such programme or performance.

If such a reproduced copy of sound recording is made or imported in contravention of the provisions of this Act.

For the purpose of infringement by the defendant: first, there must be sufficient objective similarity between defendant's infringing work and the copyrighted work or a substantial part thereof. And secondly, the copyrighted work must be the source from which the infringing work is derived. In

29. Section 51, The Copyright Act, 1957.

*Jarrold. v. Houston*<sup>30</sup>, it was held by the Court that the intention to commit fraud on the part of the defendant for the purpose of saving labour was an important consideration in arriving at the conclusion of occurrence of any infringement. In other words in order to prove infringement an *animus furandi* on the part of the defendant is quite relevant to determine infringement of the copyrighted work.

In India in the case of *R.G. Anand v. Delux Films*<sup>31</sup>, the Supreme Court relied on the 'doctrine of dominant impact' and the court held that if the viewer after seeing the films gets total impression that the film is by and large a copy of the original play, violation of copyright may be said to have been proved<sup>32</sup>. After careful examination of various authorities the court in the above mentioned case laid down the following test to determine infringement of a copyrighted work:

- (1) There can be no copyright in an idea, subject-matter, themes, plots or historical or legendary facts and violation of the copyright if access is confined to the form, manner and arrangement, and expression of the idea by the author of the copyrighted work.
- (2) The Court should determine whether or not the similarities are on fundamental or substantial aspects of the mode of expression adopted in the copyrighted work. If the defendant's work is nothing but a literal imitation of the copyrighted work with some variation here and there it would amount to violation of the copyright. In other words in order to have action against the infringed copy, the copying must be a substantial and material one which at once leads to the conclusion that the defendant is guilty of an act of piracy.
- (3) One of the surest and the safest test to determine whether or not there has been a violation of copyright is to see if the reader, spectator or the viewer, after having read or seen both the works is clearly of the opinion and gets an unmistakable impression that the subsequent work appears to be copy of the original<sup>33</sup>.

## Cyberspace, the Internet, Websites and the Nature of the Copyright

On the Internet, the digital nature perspective of intellectual property law is the most important characteristic as compared to the traditional 'analog' methods of recording of works of intellectual property-on paper, film, or on magnetic tape whereas digitisation converts all words, images, sounds, graphics and films into binary numbers, either ones or zeroes. These digitally stored works, as bits grouped in bytes disassociated from their physical form are then transferred over

the networks to be finally reconstructed into recognisable art by a reference to their binary values. This means that for the intellectual property system we do not transfer fixed expression of works as we would buy a book or license of a video but the digital representation of those works. Such a change needs different set-up of laws in order to protect copyrights on the Internet<sup>34</sup>. The copyright on the website the underlying source code or computer programme is protectable as a literary work<sup>35</sup>. In *Two Pesos v Taco Cabana*<sup>36</sup> case, a US court held that the layout of the web page or rather the 'look and feel' of the website, if distinctive, is amenable to protection as a trade, dress. In this case it was held that the decor of a restaurant could be protected as trade-dress.

A website creator must ensure that he owns the copyrights in all the aspects involved in the creation of website for its functioning. In law it is presumed that anything created by an employee during the course of employment belongs to the employer. However, it is better that one must stipulate in an employment contract that the copyright in all materials including software programmes, website designs created or developed by the employee would vest in the employer. In the case of consultant of the software programmers unless the contracts between the website owner and the consultant vest the copyrights in any materials so created in the owner the said copyright would vest with the consultant or the software programmer.

While downloading from the Internet the defendant makes the permanent copies of the copyrighted work on the hard disc of the computer and this amounts to a reproduction of the copyrighted work. For the users who want to download a file or software programme it is important to read instructions and the copyright notices attached with the files. The author may permit the user to download but may not permit distribution for posting on the internet through some other website. For the owner of a website to have effective control over his material on the website, it is important that he expressly prohibits any downloading of such materials, because in downloading the materials from the website there is always a threat of it being used for various commercial purposes like transmitting and sale of such material to other users.

## Linking, Hyper-Linking and Framing

The Internet or the web was initially created for the purposes of enabling hypertext capabilities allowing one side to link or hyperlink and access another sight. In this way, the users could make sense of the great mass of data contained on the Internet. As linking or hyper linking was used for education or research purposes and it was both accepted and encouraged when Internet was a research

30. (1857) 3 K & J 1708.

31. AIR 1978 S.C. 1613.

32. *Ibid.*, pp. 1631–32.

33. *Ibid.*, p. 1627.

34. Ryder, Rodney D., *Guide to Cyber Laws*, 3rd ed., 2007, p. 262.

35. Section 2(fc), The Copyright Act, 1957.

36. 505 US 763 (1992).

network. However, on the commercial Internet the sight owners have contended that before employing a link, the website must seek permission from the website to which it wants to link. Some of the website owners have challenged the practice of linking without first seeking permission. In *Ticketmaster Corp. v. Microsoft Corp.*<sup>37</sup> case, Ticketmaster sued Microsoft for linking to its sight without permission. Ticketmaster objected to Microsoft's practice of linking, deep within its site rather than to the home page and claimed *inter alia* that Microsoft unfairly diverted advertising dollars that otherwise would have gone to Ticketmaster. The impetus for the suit was probably primarily economic. But linking deep within the site, Microsoft bypassed Ticketmaster's home page which contains advertising. As a result, no 'hit' to the home page was recorded, potentially decreasing Ticketmaster's revenue. Also Ticketmaster had setup contractual arrangement with other firms in which those companies had agreed to pay to link to the Ticketmaster site. Free linking by Microsoft could devalue those relationships.

On the website, framing is a relatively recent phenomenon as compared to linking. A framing site, by virtue of certain commands in its HTML code, links to another site, displaying that site within window or frame. The frame itself is comprised of content from the framing site. In comparison to generic hyper linking, in the case of framing, the user remains at the framing site and views content from both sites. The address that the user's browser displays may continue to be that of the framing site. The user may be unaware that the content in the frame comes from another site. The difference between linking and framing may make trademark liability more likely for sites that frame rather than merely hyperlink. Sites are increasingly challenging those who frame them. Probably the most widely publicized challenge was that brought by a group of plaintiffs led by the Washington Post against Total News Inc. The plaintiffs in this case objected to the Total News site's framing of their content. The Total News would surround the content of the plaintiffs' sites with ads that Total News itself had sold. In this case the plaintiffs argued that the Total News had infringed their copyrights and trademarks, diluted their trademarks and engaged in unfair competitions.

It appears that the copyright law is unlikely to be applied in the act of framing although it may be a close question. It can be argued that none of the exclusive copyrights rights is implicated by the frame, as it is simply a method of display. The frame though, might implicate the copyright owner's exclusive right to prepare derivative works. Even if the framing site were considered a derivative work of the framed site, the creator of the framing site may still not be liable for copyright infringement. The user actually does the framing and the user's conduct is likely to be protected under the copyright doctrine of fair use. As in the case of linking, if the user is not a direct infringer, then the site that provides the ability to frame cannot be a contributory infringer. Hyper

linking and framing are just two of the Internet practices, which plaintiffs are challenging. Neither is clearly illegal under existing legal doctrine, nor is it clear that either should be. The uncertainty of the current public law of copyright and trademark may lead parties to seek redress under the law of tort. Further parties may also attempt to order their relationships using the law of contract to set the terms of access and use of a site. And therefore if hyperlinking and framing are able to survive the implication of law under the intellectual property statutes the parties may be able to claim the damages under the law of tort and contract.

### Remedies for Infringement of Copyright on Cyberspace

Under the Copyright Act, 1957, for the infringement of the copyrighted works without a license granted by the owner of the copyright or the Registrar we find that there are three types of remedies available to the owner of the Copyrighted work viz., (i) Civil remedies (ii) Administrative remedies (iii) Criminal remedies under the law.

The civil remedies under the law may be classified further in two categories (a) preventive civil remedies, and (b) compensatory remedies:

Under the Copyright Act, 1957 preventive civil remedies may include interlocutory injunction and the final injunction in the suite for infringement of copyright. Injunction is the most important remedy against the infringement of copyright under the law. Injunction means a judicial process by which one who is threatening to invade or has invaded the legal or equitable rights of another is restrained from commencing or continuing such act, or is commanded to restore matters to the position in which they stood previous to the action<sup>38</sup>. Injunction may be interlocutory granted before trial of a suite or permanently granted after the trial.

The owner of a copyright prefers speedy and effective relief to prevent further infringements of his copyright and consequent damage to his business and therefore the owner does not want to wait for some years until full trial is completed. And therefore, the law provides an interim relief to the plaintiff owner of the copyright by way of interim injunction. In this way the owner of the copyright has tremendous advantage because the defendant is stopped dead in his tracks, though the interim injunction is the discretion of the trial court which is judicial order under the law and not arbitrary, vague and fanciful. Such interim injunction is granted to plaintiff where there is likelihood of success on the merits of the case and is irreparable harm will be caused to the plaintiff if interim injunction is not granted. And if the plaintiff succeeds at the trial of the case by establishing infringement of his copyright then he will be entitled to a permanent injunction to restrain the defendant from future infringements. Such injunction will be operated only during the unexpired term of the copyright.

37. CV 97-3055 RAP (filed 4/28/97).

38. Khosla, G.D., *Know your Copyright*, p. 52 in P. Narayanan, *Copyright Law* (Eastern Law House, Calcutta, 1986) at p. 219.

Where there is possibility of the defendant destroying or disposing of the incriminating material the court may also make an order for the inspection of the premises of the defendant. This allows the plaintiff's advocate to take possession of infringing copies, documents and other materials relating to the copyrighted work.

Moreover, a compensatory remedy is also available to the plaintiff which includes damages, account of profit and delivery of infringing copies. Damages are granted to a owner of the copyright for the loss or damage caused to him by the infringement of copyright. However, the plaintiff is only entitled to claim the profits on account of infringement made by defendant or the plaintiff may claim damages for infringement of copyright. The copyright owner is entitled to opt either for damages or for account of profit.

Second, the type of remedy available to the plaintiff under the Copyright Act, 1957 provide for an effective and speedy administrative remedy to the copyright owner under Section 53 of the Act. Section 53(1) of the act provides the registrar of copyright to make an order prohibiting the importation into India such copies on the application of the owner of copyright in any work or his authorized agent after making such enquiry as the registrar deems fit. The remedy under the Section 53 of the Act is quasi-judicial in nature and an appeal can be made to the Copyright Board against the order of the registrar<sup>39</sup>. Sections 63 to 70 of the Copyright Act provide for the offences relating to copyrights. In Section 63, is given the infringement of copyright in a work or any other right conferred by the Act except the resale share right in original copies as provided under Section 53A which is punishable with imprisonment for a term, which shall not be less than six months but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakhs rupees. But the Court has discretion to reduce the minimum term of imprisonment and the minimum fine for adequate and special reasons which have to be recorded in the judgement. Moreover, for the second and subsequent convictions, the minimum term of imprisonment is enhanced to one year and the minimum fine to one lakh rupees which may be relaxed for adequate and special reasons to be recorded in the judgement. But there is no change in the maximum punishment.

### The Liabilities of an Internet Services Provider (ISP) in Cyberspace

The liabilities of ISPs may arise in a variety of legal areas, such as criminal law, Torts law, Trade secret law, Copyright law, Trademark law, Unfair Competition law and the like. Many countries have tried to define the liability of ISPs in

39. Section 72, The Copyright Act, 1957.

disseminating third party content<sup>40</sup>. The function of service providers is to host content, such as web pages of subscriber, over which the service provider exercises no control. And it is impossible practically to monitor or screen the activities of users of network services. Therefore, service providers need legal protection similar to that as given under the law to common carriers, such as telephone companies, for infringements committed by their consumers. Such a view is consistent with the Agreed Statements Concerning the WIPO Copyright Treaty which states that the mere provision of physical facilities for enabling or making a communication does not by itself amount to a communication. As it is impossible to monitor the activities of users of network services, for example, educational institutions, libraries and museums and service providers, they should have no legal obligations to monitor what is transmitted, or seek facts or circumstances indicating illegal activity. The Copyright Forum's recommendation in this regard is based on Article 15(1) of the European Union's Directive on Electronic Commerce. The European Union's approach is preferred over that of the US which is viewed as being too complex<sup>41</sup>.

### Cyberspace and the Protection of Patents in India

The law of patents is very relevant for the information technology industry as it is in other industries. The owner of a patent is granted certain exclusive rights to a particular invention. The rights of patent owner include the right to make, the right to use, and the right to sell the invention and also the obvious extensions connected with the rights of inventions. One of the objects of the patent granted to the owner is to enable the inventor to make better profits from his efforts. The patent serves to protect the inventor from the unhealthy competition from the copycats. In the computer technology which is fast-paced, being the first to develop and to patent an invention which satisfies the demand in a market can provide significant leverage over competitors. The patent owners can also have an agreement to let others make use of the patented invention. This is generally done by means of a license agreement which specifies what the licensee may do with the invention in exchange for a royalty paid to the licensor patent holder. Patents and other licenses are very common in the computer industry and in fact have influenced the major facets of personal computer market. We can see the effects of Indian Business Machines (IBM's) decision to license the operating system for its personal computer from a company which has become famous like Microsoft.

40. The term 'third party' is used to distinguish third parties from primary actors and victims (second party).

41. *Society of Composers, Authors and Music Publishers of Canada v. Association of Internet Service Providers*, June 30, 2004. The decision is available online at: <<http://www.lexum.umontreal.ca/csc-scc/en/rec/index.html>>

The term 'patent' refers to a grant of some privilege, property or authority made by the government or the sovereign of the country to one or more individuals. The instrument by which such a grant is made by the government is known as patent. A patent is a form of intellectual property rights in, among other things, a new and useful device, design or process. In India, under the law, a patent is a—

- right granted by the government;
- to exclude others;
- from engaging in activities such as making, using, importing, offering to sell or selling an invention.

In India, the law relating to patents came on the Statute Book as The Patents Act, 1970. Patent, under the Act, is granted by the Controller to the inventor for a period of twenty years. It is exclusive right to make use, exercise and vend his invention. The Patents (Amendment Act) 2005, defines: 'patent means a patent for any invention granted under this Act'<sup>42</sup>. The Patent's Act grants to the inventor substantive rights and secures to him the valuable monetary right which he can enforce for his own advantage either by using it himself or conveying the privileges to others. He receives something tangible, something which has present existing value, which protects him from some competition, and is the source of gain and profit.

After the expiry of the period for which exclusive right is granted to the inventor, invention can be put to use by any person other than one to whom a patent had been granted. The person to whom a patent is granted is called patentee.

### Patent as a Form of Intellectual Property

An invention is the creation of intellect applied to capital and labour, to produce something new and useful. Such creation becomes the exclusive property of the inventor on the grant of patent. The patentee's exclusive proprietary right over the invention is an intellectual property right. The owner's of the 'patent', that is, the patentee is entitled to deal with his such property in the same manner as owner of any movable property deals with his property. This means that the patentee can sell the whole or part of his property (patent). He can also grant license to other(s). Such sale and license of assignment of patented property naturally has to be for valuable consideration, acceptable mutually.

In *Bishwanath Prasad Radhey Shyam v. Hindustan Metal Industries*<sup>43</sup>, the Supreme Court has held that "the object of patent law is to encourage scientific research, new technology and industrial progress. Grant of exclusive privilege

IT Act. However, even this Section is bailable because it is punishable only up to a term of imprisonment of three years only.

Under Section 66C of the IT (Amendment) Act, 2008 any person who fraudulently or dishonestly makes use of the electronic signature, password for any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Under this Section the offender requires *mens rea*, because the offence can be committed by fraudulently or dishonestly making use of electronic signature, password or unique identification feature. The offence in the section is cognizable because the offence can be committed by fraudulently or dishonestly making use of electronic signature, password or unique identification feature. The offence in the section is cognizable as well as bailable under section 77B of the IT Act.

Under Section 66D of the IT (Amendment) Act, 2008 any person who by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine which may extend to one lakh rupees.

Even this Section for cheating by personation by using computer resource can be committed by the offender when he in fact cheats by personating. And therefore, the offence under the section requires *mens rea* on the part of the offender. This Section is also made cognizable as well as bailable under Section 77B of the IT Act. Previously cheating by personation was defined under Section 416 of the IPC and was punishable under Section 419 of the IPC.

### Violation of the Right of Privacy on Cyberspace/Internet

Privacy cannot be defined in an absolute fashion because it connotes different meanings and perceptions for different people. It is a kind of right of an individual or group to keep their lives out of public view in order to keep secret their personal affair. It is a kind of a claim by individuals, groups or institutions to determine for themselves as to how, to what extent and when information about their lives and affairs may be communicated to others. Being a subjective type of right which is dependant on individuals, regions, and society in different countries in this world, makes the realization and acceptance of the scope of privacy difficult for protection a complicated affair. In fact the right of privacy of people is more to employ restraint or obligation. The right of privacy may be expressed as the 'right to be let alone'<sup>43</sup>.

The right to privacy as a human right has been recognized in Art. 8 of the European Convention on Human Rights 1950 which reads as follows:

42. Section 2(m), The Patent's Act, 1970.

43. (1979)2 SCC 511.

33. Warren and Brandeis, "The Right to Privacy", *Harvard Law Review*, IV (5), (1890).

**Article 8.**

(1) Every one has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

In legal parlance privacy has been known to include a number of varied rights like to make decision for yourself, the right to travel anonymously, the right to be left alone and the right to control the dissemination of information about yourself. The concept of privacy has been applied in so many arenas of contemporary life including privacy of health care, to credit reports and privacy from search and seizure that it has come to be known as the word like 'freedom' and 'rights', 'privacy' connotes multiple meanings in multiple discourses<sup>34</sup>. In the modern era when means of communication and communication networks in cyberspace and Internet have undergone radical changes and the violation or threat to privacy is considered as a weapon to ensure confidentiality of individual's human affairs.

In the UK the right to privacy was initially recognised in *Prince Albert v. Strange*<sup>35</sup>. This right to privacy has been extended to private communication between husband and wife in the UK<sup>36</sup>. The English law started to recognise the right to privacy. Any infringement of such privacy right should give a cause of action or as an injunction as the case may require.

In India the right to privacy was for the first time emphasised by the minority judgement delivered by Justice Subba Rao in *Kharak Singh v. State of UP*<sup>37</sup>, where he said that the right to personal liberty takes in not only a right to be free from restrictions placed on movement, but also free from encroachments on the private life of a person. However, it is only in *Gobind v. State of Madhya Pradesh*<sup>38</sup>, the Supreme Court has recognised the right to privacy as a fundamental right, but it is not absolute. So far there is no statutory law on the protection of privacy in India, but privacy has been included within the meaning of Article 21 of the Constitution of India. Though in a limited and narrow sense the right to privacy is protected by the IPC yet the different facets of this right have no comprehensive protection as such except resorting to relief under the law of torts.

34. Gormely, Ken, A Brief History of Privacy, One Hundred Years of Privacy, 1992, *Wisconsin Law Review*, 1335 (1992).

35. (1849) H & TW 1.

36. *Argyll v. Argyll* (1967)1 ch. 302.

37. AIR 1963 SC 1295 (1306).

38. AIR 1975 SC 1378.

*Rajagopal v. State of T.N.*<sup>39</sup>, is concerned with the publication of the autobiography of a condemned prisoner which contained *inter alia* the materials as to show close nexus between the prisoner and several IAS, IPS and other officers, some of whom were his partners in several crimes. The Supreme Court laid down the following broad principles regarding the right to privacy:

- (1) the right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Art. 21. It is a 'right to be let alone'. A citizens has a right to safe-guard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters. None can publish anything concerning the above matters without his consent...
- (2) The aforesaid rule is subject to the exception that any publication concerning the aforesaid aspects becomes objectionable if such publication is based upon public records including courts records. Once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media and others ... .

The Supreme Court of India in *People's Union for Civil Liberties v. Union of India*<sup>40</sup>, has held that telephone-tapping is a serious invasion of an individual's privacy. With the growth of highly sophisticated communication technology, the right to hold telephone conversation, in the privacy of one's home or office, without interference, is increasingly susceptible to abuse. Telephone-tapping would infract Article 21 unless it is as permitted under the procedure established by law.

### Punishment for Violation of Privacy, Breach of Confidentiality and Privacy under the IT Act

In the IT (Amendment) Act, 2008, a new provision under the IT Act has been introduced for the purpose of punishment for violation of privacy. Under Section 66E, whoever intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under the circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

The above Section punishes intentionally or knowingly capturing, publishing or transmitting the image of a private area without the consent of that person which violates the privacy of that person is punishable with imprisonment up to three years or with fine up to two lakh rupees or with both imprisonment and fine. The Section requires *mens rea* on the part of the offender in the form of either intention or knowledge of violating privacy of a person. The offence is also cognizable as well as bailable under Section 77B of the IT Act.

39. AIR 1995 SC 264: (1994)6 SCC 632.

40. (1997)1 SCC. 301.

The above offence defined provides for meaning to various situations under the explanation which are as follows:

- (a) 'transmit' means to electronically send a visual image with the intent that it be viewed by a person or persons;
- (b) 'capture', with respect to an image, means to videotape, photograph, film or record by any means;
- (c) 'private area' means the naked or undergarments clad genitals, public area, buttocks or female breast;
- (d) 'publishes' means reproduction in the printed or electronic form and making it available for public;
- (e) 'under circumstances violating privacy' means circumstances in which a person can have a reasonable expectation that—
  - (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
  - (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

On cyberspace, with the use of Internet, we provide information to others in many ways. Even though the information we provide to one person or company on the Internet may not make sense unless it is combined with information we provide to another person or company. Some of the methods by which we provide information to others are as follows:

- When we sign with an Internet Service Providers (ISP). The ISP provides mechanism for connecting the computer to the Internet. Each computer connected to the Internet has a unique address known as the IP address.
- When we correspond through e-mail we are giving information to the recipient. By e-mail we might also be giving information to our employer, the government, our e-mail provider and to anyone that the recipient of e-mail passes our message to.
- By browsing through Internet we are also relying personal information to websites.
- When we use search engines on Internet the search engines also have the availability to track our searches.
- The instant messaging/chatting/video conferencing in all these methods can be archived, stored and recorded on our computer as easily as e-mails, which can also affect privacy.
- Blogging where people post a video or photograph online also can affect privacy.
- Even online banking requires a lot of sensitive information over the internet, which may affect privacy.

- Sometimes many websites use web bugs to tracks as to who is viewing there pages. The web bug can confirm when the message or web page and record the IP address of the viewer.
- Sometimes direct marketing online newspapers and other businesses have friendly boxes asking for if the websites can save our account information for future transactions.
- Even spyware are software that secretly gather the information through our Internet connection without our knowledge.
- Lastly, phishing and pharming that deceive us into revealing our personal information.

Under Section 72 of the IT Act, except as otherwise provided in this Act or in other law for time being in force, if any person in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured excess 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.

Under the above Section, breach of confidentiality and privacy when a person discloses such electronic records to other persons who are not authorised to get such information about documents and records, is punishable with imprisonment up to two years or with a fine which may extend to one lakh rupees, or with both. As the offence under Section 72 of the IT Act is punishable for maximum imprisonment of only two years, therefore, the offence under this section is non-cognizable under section 77B of this Act. Moreover, the offence is bailable under section 77B. As the offence can be committed by disclosure to any other person without the consent of that person who is authorised to give such consent, it appears that the offence under this section requires positive disclosure on the part of the offender in order to commit the offence under this Section.

The above Section 72 relating to confidentiality and privacy must be understood along with the reasonable restrictions provided under Article 19(2) viz; reasonable restrictions on the right of freedom of speech and expression in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

With the amendment of the IT (Amendment) Act, 2008, a new Section 72A has been introduced where by any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any person, shall be punished with imprisonment for a

term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

The above offence under Section 72A of the IT Act is in a way an aggravated form of the offence provided under Section 72 of the Act. The above Section 72A requires *mens rea* for the commission of the offence either with the intention or knowledge of the offender. The punishment which may extend to three years imprisonment makes the offence cognizable though it is a bailable offence under Section 77B of the Act.

In *A. Shankar S/o. K. Achimuthu v. The State*<sup>41</sup>, the respondent D.S.P. of the CBCID Cyber Crime Cell had registered a case under Section 5 of the Official Secrets Act, Sections 43 and 66 of the IT Act and Sections 378, 379 and some other Sections of the IPC on the basis of a complaint lodged by Principal Secretary to Government Home Department. It is alleged by the prosecution that on given dates at the room of Legal Advisor's of Directorate of Vigilance and Anti-Corruption, Chennai the petitioner being a Special Assistant of Confidential Section in Directorate of Vigilance and Anti-Corruption office, with intent to cause damage to the office of the Directorate of Vigilance and Anti-Corruption, without the permission of the owner of the computer that is, having taken advantage of the absence of Legal Advisor, unauthorisedly accessed into the computer system of Legal Advisor through his pen drive and also downloaded the audio file and caused publication of the same in the *Deccan Chronicle* and also telecast the same day on 'Makkal TV' and 'Jaya TV'. Thus the petitioner, by accessing the computer system and information without the permission of the owners/authorised users copied caused publication and thereby diminished the value of information, utility and affected it injuriously. On the basis of the above facts the Tamil Nadu Government had appointed a Commission of inquiry. The Commission of inquiry had found that the petitioner was responsible for the access and the leak of the telephone conversation and it recommended to register a criminal case against the petitioner.

Under Section 197 of the Criminal Procedure Code, sanction is required for prosecution of a public servant accused of any offence alleged to have been committed by him while acting or purporting to act in the discharge of his official duty. And no court shall take cognizance of such offence except with the previous sanction. It is submitted by the petitioner that out of the three charges viz; under Sections 66, 70 and 72 of the IT Act, 2000, the government had given sanction only for the offences under Sections 66 and 70 of the act and in respect of Section 72 no sanction has been accorded and hence sanction of prosecution itself is defective one and therefore, the whole investigation or whole proceeding against the petitioner have absolutely been vitiated.

In this case the High Court on quashing the prosecution before the trial court under Section 482 of the Criminal Procedure Code, 1973 held that the inherent power cannot be invoked to quash the charge on the ground of question

41. MANU/TN/3055/2010.

of facts relating to non-granting of sanction under Section 72 of the IT Act, 2000. The court held that it is of the firm view that the question of sanction of prosecution can be taken during the conduct of trial and therefore the proceeding that is, the charge sheet at this stage cannot be quashed on the ground of want of sanction in respect of Section 72 of the IT Act, 2000.

## Terrorism on Cyberspace/Internet

In modern times terrorism as a means and method to cause fear and undue violence against individuals, groups or countries has posed a very menacing effect and as a big challenge in this world. The causes of terrorism in this world are numerous including religious, geographical and against particular countries by one country against the other countries. While terrorism is a complicated, complex and a very challenging task, and is condemned by most of the people is almost all the countries in this world yet there is no unanimity among the people about the methods to regulate the phenomenon of terrorism in this world. Historically, many ways, means and methods have been used by people to terrorise one group of individuals or countries or to terrorise the other group of individuals or countries.

The modern age being an era of high levels of technology where in computers, computers systems, the cyberspace and Internet have become immensely popular. And even the terrorists also use Internet and cyberspace frequently in order to achieve their terrorist objectives. The possibility of speedy, anonymous, to size, accurate and timely information with the help of Internet and cyberspace gives competitive advantage to the terrorist and terrorists groups. The expression 'cyber terrorism' in fact is a combination of the words cyberspace and terrorism, which means unlawful attacks and threats of attacks, against computer, networks and the information stored in the computer systems to intimidate or coerce the governments or its people for political, social or religious objectives. In order to be properly called cyber terrorism attacks should be such to result into violence against persons, property or society, resulting in extreme harm and generate high fear among the people. The beginning of cyber terrorism can be traced right from early 1990s when the increase in the growth of Internet and cyberspace was visible in this world. Now a days the terrorists on the cyberspace has more financial backing, higher technical opportunities and even huge military backing and potential.

Cyber terrorism has special features to make a distinction between a cyber terror attack and the activities of a hacker. The cyber terrorist attack is pre-defined and the victims are generally specific targets and the cyber terrorist's attacks objective is to destroy or damage specific targets like political, civil, economic, energy and military infrastructure. And the object is to cause fear in order to achieve their political, religious or economic goals. They persuade people to believe that the victims are vulnerable and their machinery negligent.