12

CYBER LAW

*Karnika Seth**

I INTRODUCTION

THE FIELD of information technology (IT) and the law on IT are dynamic. Rapid advancements in information technology necessitate adapting the existing laws or creation of new laws to regulate the cyberspace. At the same time, it is necessary to allow such freedom as it is essential to harness its full potential for the benefit of mankind. IT law regulates not only actions in the cyber space but also interfaces with computers or internet or communication devices such as cell phones in the offline environment. IT has expanded its horizons in the last few decades. Its significance has broadened from a mere facilitator of information dissemination to a powerful means of communication, exchange of ideas through social media and social learning. An apt example of this in the year 2011 is the Anna Hazare campaign which became a highlight point on facebook wherein more than one lac followers joined the movement through facebook.[1] Censorship of Internet was a highly debated and discussed topic when Google and Facebook amongst others, were sued for allegedly hosting offensive content on their websites and a Delhi Court ordered twenty two websites to remove the objectionable content from its sites.[2] These service providers faced both civil and criminal cases in different matters for hosting offensive content which brought issues such as censorship, due diligence and filtering to the fore front.[3] This survey discusses the recent developments in cyberlaws, in particular, the recent decisions passed by the Indian courts to interpret and elucidate the extant cyberlaw.

---

* Advocate, Supreme Court of India.

1 Kapil Ohri, "How Powerful is Anna Hazare on Facebook and Twitter?," afaqs, Aug 18, 2011, http://www.afaqs.com/news/story.html?sid=31413.

2 Anna Edwards, "Clean up your Website': Indian Court Orders Facebook and Google to Remove 'Anti-religious' Content", http://www.dailymail.co.uk/news/article-2081078/Facebook-Google-ordered-remove-anti-religious-content.html# ixzz1keKMQcSm.

3 "Google, Facebook Fight Indian Criminal Case", read more at: http://www.ndtv.com/article/technology/google-facebook-fight-indian-criminal-case-167715&cp.

II PRINCIPLES TO DETERMINE JURISDICTION

A landmark case on determining jurisdiction in internet cases was decided by the Delhi High Court in *Casio India Co. Ltd* v. *Ashita, Tele Systems Pvt. Ltd.*[4] The suit related to an action of passing off in respect of a domain name of a website wherein the court dealt with passing-off action. The defendant had registered a domain name www.casioindia.com and marketed its product through the website. It was alleged by the plaintiff that the impugned domain name was identical and confusingly similar to the plaintiff's trademark 'Casio'. The plaintiff alleged that the defendant registered the impugned domain name for making illegal monetary gains and had no legitimate right to register the impugned domain name. The plaintiff being a wholly owned subsidiary of Casio (Japan), was the owner of the trademark 'Casio' in India used for electronic products. The plaintiff also had the registrations of similar domain names casioindia.net, casioindia.org, CasioIndiaCompany.com, CasioIndia.net as well as CasioIndia.info, CasioIndia.Biz and CasioIndia.Co amongst other domain names. The defendant no.1 had managed to get the registration of the aforementioned domain name during the time when it held a distributorship agreement with the plaintiff. On the issue of territorial jurisdiction, the defendant contended that since it carried on business in Mumbai and was resident of Mumbai no cause of action arose in Delhi and as such the Delhi High court had no jurisdiction to adjudicate the case. The court by relying on *Rediff Communications Ltd* v. *Cyberbooth*[5] and *Info Edge India Pvt. Ltd.* v. *Shailesh Gupta*[6] held that once the access to the impugned domain name website could be had from anywhere else, the fact that the residence of the defendant which was in Bombay would not limit the territorial jurisdiction only to Bombay. The very fact that the website of the defendant no.1 can be accessed from Delhi, was sufficient to the court to invoke the territorial jurisdiction of the High Court of Delhi.

This view on determining jurisdiction in cyberspace was overruled later by the Delhi High Court in *India Television Independent News Services Pvt. Ltd.* v. *India Broadcast Live LLC*.[7] In this case the court has assumed personal jurisdiction though the defendants have registered their domain name indiatvlive.com. The plaintiff company managed a Hindi news channel, India TV and claimed its right over the mark 'India TV' which it alleged to have used continuously since 01.12.2002. The plaintiff also claimed that 'India TV' is a well-known mark. The plaintiff was also the registered owner of the domain name www.IndiaTVnews.com since 18.11.03. The services of the channel were made available for live access on the said website. The defendants nos.1 & 2 registered a deceptively similar domain name indiatvlive.com. As the website contained the words "INDIA TV" in its domain name, the plaintiff alleged that defendant registered the impugned domain name to cash on the reputation of the plaintiff and there was no legitimate interest of defendant in registering the said domain name. The plaintiff prayed for relief of permanent

4 (2003) PTC 265 (Del).
5 AIR 2000 Bom 27.
6 2002 (24) PTC 355.
7 (2007) 35 PTC 177 (Del).

injunction restraining defendant from using the domain name and mandatory injunction against the registrar of the impugned domain name to transfer the same to the plaintiff. In this case the defendant no.1 contended that since neither of the defendants reside or work for gain in India as the promoters of defendant no.1 are permanent residents of the United States and the defendant no.1 is Delaware State Corporation formed under the laws of the United States the court did not have personal jurisdiction over the defendants. The court relied on *Cybersell Inc* v. *Cybersell Inc.*,[8] and noted that India did not have long arm statutes as in United States and in order to invoke personal jurisdiction over a non resident defendant, it had to be examined whether (i) the defendant's activities have a sufficient connection with the forum state (India), (ii) whether defendant purposefully avails himself of privilege of doing business in the forum state; (iii) whether the cause of action arises out of the defendant's activities within the forum and (iv) whether the exercise of jurisdiction would be reasonable. The high court observed that mere accessibility of website from a particular place is not sufficient for the Indian courts to assume personal jurisdiction over a foreign website owner or entity.

However, by adopting the principles discussed in the *Zippo* case,[9] the court took the view that wherever the website is interactive and not passive (or only information based), the jurisdiction can be assumed. The court held so:

> There must be something more to demonstrate that the defendant directed his activity towards the forum state.

The court noted that in *Cybersell* case the interactivity of the website was limited to receiving browser's name and expression of interest but not signing up for the services. This was not held to be sufficient for the exercise of jurisdiction. In *Compuserve's*[10] case, where defendant specifically targeted customers in the forum state, it was held to satisfy the *targeting test* to attract jurisdiction over non-resident defendant. The court further observed that the level of interactivity should be analysed, and limited interactivity would not be sufficient for a court to exercise jurisdiction. In the present case, the website "indiatvlive.com" of the defendant no.1 was not wholly of a 'passive' character. It had a specific section for subscription to its services and contained options for the countries whose residents could subscribe to the services and it targeted customers in India. Hence, the court concluded that services provided by the defendant no.1 could be subscribed to and availed of in Delhi (India), i.e., within the jurisdiction of the court. Thus, the court held that the defendants were carrying on activities within the jurisdiction of the court and has sufficient contacts with the jurisdiction of the court and the claim of the plaintiff has arisen as a consequence of the activities of defendant no.1 within the jurisdiction of the court. The court also relied on the 'effects test' and held that since the plaintiff channel was an Indian news channel intended for Indian audiences, any damage alleged to have been caused or alleged to be likely to arise to the

8 Case no. 96-17087 D.C. no. CV-96-0089-EHC.

9 *Zippo Mfg. Co.* v. *Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997).

10 *Cubby, Inc.* v. *Compuserve, Inc, U.S District Court, S.D. New York*, 776 F. Supp. 135, Oct. 29, 1991 case no. 90 Civ. 6571 (PKL).

goodwill, reputation etc. of the plaintiff would be in India. For the effects test, court relied on *Panavision International* case,[11] wherein the registration of the plaintiff's mark as a domain name by the defendant had the effect of injuring the plaintiff who was based in California and the California court was held to have jurisdiction. Thus, the court held that as the defendant was carrying on activities within its jurisdiction, it had sufficient contacts with the jurisdiction of the court and the court could assume personal jurisdiction over the defendant. In this case, thus personal jurisdiction was assumed, however, on a different reasoning than that of *Casio India*.

Based on the reasoning in *India TV case*, the High Court of Delhi in *Renaissance Hotel Holding Inc* v. *B. Vihaya Sai*[12] refused to assume jurisdiction in a trademark infringement case where a US based hospitality company lodged an action against an Indian hotel based at Bangalore seeking directions to restrain the defendant from using the trademark 'Sai Renaissance' on internet as a domain name. The court took the view that only because a booking could be made from Delhi, the jurisdiction of the court cannot be assumed.

However, *Zippo approach* has diminishing importance, as almost any website today can be said to be interactive with its users. In fact, the *target based approach* has assumed more importance and it is settled law of cyberspace that if a website targets customers from an area, the service provider ought to be answerable to courts of that area. This shift in approach is being adopted by Indian courts too. In *Banyan Tree Holding Pvt. Ltd.* v. *Murli Krishnan Reddy*,[13] the Delhi High Court relied on *India TV* case and held that in a passing off or infringement case the plaintiff is required to prove that the defendant has purposefully availed itself of the benefit of conducting business in forum state and engaged in specific targeting of customers in that area and mere hosting of interactive website without targeting will not attract personal jurisdiction. For the "effects" test to apply, the plaintiff is required to establish and show prima facie that the specific targeting of the forum state by the defendant resulted in an injury or harm to the Plaintiff within the forum state. This approach is correct interpretation of law on jurisdiction in cyber space, as a *Zippo* sliding scale approach has become obsolete since almost all websites are interactive today and interactivity alone, without targeting, can no longer be a justified criteria to invoke personal jurisdiction.

III JURISDICTION OF HIGH COURT IN 'IT' CASES

Section 61 of the IT Act, 2000 provides a bar against civil courts, as regards jurisdiction, to entertain any suit or proceedings in respect of any matter which adjudicating authority appointed under the Act or Cyber Appellate Tribunal is empowered under the Act to determine, and restrains granting any injunction by any court or authority in respect of any action taken or to be taken in pursuance of any power conferred by or under the Act.

---

11 *Panavision International LP* v. *Dennis Toeppen*, case No. 96-3284 DDP (JRX).United States District Court, C.D. California, decided on 19.09.1996.

12 137 (2009) DLT 265: 2009 (39) PTC 547 (Del).

13 (2008) 38 PTC 288 (Del).

In a case before Delhi High Court, the court considered whether in light of provisions of section 61 which bars the jurisdiction of civil courts, a suit filed by the plaintiff for injunction against infringement of copyright and confidential information in a civil court is maintainable when such acts involve unauthorized access and downloading of such matter using computers instead of approaching the adjudicating authority. The court relied on *Secretary of State* v. *Mask and Co*[14] wherein it was held that the exclusion of the jurisdiction of the civil courts 'must either be explicitly expressed or clearly implied'. The court also relied on decisions of the Supreme Court in *Roop Lal Sathi* v. *Nachhattar Singh Gill,*[15] and *Raptakos Brett and Co. Ltd.* v. *Ganesh Property*,[16] and held that where legal issues involve two Acts, only a part of the plaint that pertains to IT Act cannot be rejected on ground of lack of jurisdiction. The court held that although some of the causes pleaded in the suit may be barred, the court should not reject the plaint on that basis alone and that can be decided at the final stage considering the 'composite nature of the claims' in the pleadings. This reasoning in this decision seems justified as section 81 of the IT Act, 2000 expressly states that provisions of IT Act shall not restrict any person from exercising any right conferred under the Copyright Act, 1957 or Patent Act, 1970.

In another case *Olive e-Business* v. *Kirti Dhanawat*,[17] the High Court of Delhi allowed an interim ex-parte temporary injunction in a suit for permanent injunction filed to restrain an employee from unauthorisedly using/misappropriating trade secrets and confidential information of the employer company and against diversion of client queries using internet and computers. The court viewed that there were sufficient grounds to allow a relief ex-parte as not granting the relief would have caused irreparable damage to the company.

IV JURISDICTION OF THE CYBER APPELLATE TRIBUNAL IN IT CASES

Section 57 of the IT Act, 2000 provides that any person aggrieved by an order passed by the controller or adjudicating officer may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter. In *Avinash Agnihotry* v. *Controller of Certifying Authorities,*[18] filed before Cyber Appellate Tribunal, the Tribunal held that the jurisdiction of Cyber Appellate Tribunal is to hear appeals from the orders passed by the adjudicating authority or the Controller and without exhausting the remedy before the said authorities, a direct appeal is not maintainable before the Cyber Appellate Tribunal. This decision is important because it reinforces the true spirit of the law and the hierarchy of adjudication system as envisaged under the IT Act, 2000.

14 AIR 1940 PC 105.
15 1982 (3) SCC 487.
16 1998 (7) SCC 184.
17 CS (OS) 2393 (2001) dated 26-09-2011 passed by Delhi High Court.
18 Appeal no. 4/2009 before Cyber Appellate Tribunal, decided on 28.05.2010.

V CYBERSQUATTING AND TRADEMARK INFRINGEMENT/PASSING OFF CASES

Indian courts have consistently granted reliefs to plaintiffs in trademark infringement/passing off cases or cybersquatting cases wherein trademarks of plaintiff have been infringed by defendant's malafide registration with a view to sell the marks at an exorbitant price to the rightful owner.

One of the earliest cases of domain name passing off and infringement in Indian courts was the famous *Yahoo Inc* v. *Akash Arora.*[19] In this case, the US based Yahoo Inc lodged an action against the defendant based in India for registration of deceptively similar trademark 'yahooindia.com' and unauthorized use of 'Yahoo India' as its trademark. The defendant had copied the trade dress of the website and the HTML code of the plaintiff's webpages. The High Court of Delhi passed an injunction order to restrain the defendant from using Yahoo as a trademark or domain name and using the code which infringed the plaintiff's copyright in the literary work on its website. The court rejected the argument of the defendant that the provisions of the Indian Trade Mark Act would not be attracted to the use of the domain name or on the internet. The court further observed that the word 'Yahoo' had acquired distinctiveness and was indicative of the source of origin and association with the plaintiff. Though the mark was not registered in India, it had secured a trans-border reputation. The court held that it was a clear case of passing-off as the defendant domain name was deceptively similar as it was likely to confuse the general public as to an association with the plaintiff even though the defendant added the word 'India' in its domain name. Since the passage of this decision, many cases have been decided by Indian courts on domain name infringement issues.

In *Aqua Minerals Ltd* v. *Pramod Borse*[20] the defendant intentionally registered 'Bisleri' as its domain name which was identical to the plaintiff's registered trademark 'Bisleri'. The court observed that a domain name is more than an internet address and is entitled to equal protection as a trademark. The court further observed that with developments in technology, services rendered on internet are also being given equal protection so as to protect a service provider from passing off the service rendered by others as his service. Thus, the court granted an injunction order in favour of the plaintiff and ruled that the domain name deserves equal protection as a trademark, since a domain name has the same function as a brand name.

Similarly in *Satyam Infoway* v. *Sify Net Solutions,*[21] the appellants used 'Sify' as an essential element of its domain names www.sifymall.com, www.sifyrealestate.com, www.sify.net. The respondent started carrying on business of internet marketing under the domain names, www.siffynet and www.siffynet.com. The Supreme Court categorically held that the appellant's trademark rights were infringed and held the respondents guilty of passing-off. Therefore, the court granted

19 1999 IIAD Delhi 229.
20 AIR 2001 Del 463.
21 (2004) PTC (28) 566 (SC).

an injunction order restraining the respondent from using the impugned domain names.

In *Eicher Limited* v. *Web Link India*[22] the defendant illegally registered the domain name 'eichertractors.com' infringing the trademark of the plaintiff, 'EICHER'. The impugned domain name was already registered by the defendant in their own name without any license or permission and, therefore, it was contended by the plaintiff that it was registered in bad faith and with malafide motive to cash on the reputation of the plaintiff. The Delhi High Court observed that the said domain name 'eichertractors.com' was bound to create confusion in the minds of the users and held that a suit for passing-off was maintainable. Similar decision was delivered in the case of *Tata Sons Limited* v. *Fashion ID Ltd.*[23] wherein defendants were restrained from conducting any business using domain name tatainfotecheducation.com or the word TATA or any name comprising of the same and the impugned domain name was ordered to be transferred to the plaintiffs.

In *The Federal Bank Ltd* v. *Matt Hiller*[24] the plaintiff received information that the defendant is using a deceptively similar domain name 'www.federalbank.co.in' for advertising about websites relating to banks and other financial institutions. The plaintiff filed suit for permanent injunction against the defendant who was restrained from using the impugned domain name as the registration was made in bad faith and defendant had no legitimate interest in domain name.

In *Arun Jaitley* v. *Network Solutions Private Ltd.,*[25] the Delhi High Court ordered the defendant no.3, to permanently restrain from using, promoting, advertisement or retaining or parting with the domain name namely 'Arunjaitley.com' and restrained from adopting, using the mark, name in any of the extensions of the domain name on internet wherein the name 'ARUN JAITLEY' forms one of the feature. The defendant no. 3 and its entities were also directed to transfer the said domain name to the plaintiff with immediate effect. The governing body under the ICANN Rules was also directed to block and further transfer the said domain name to the plaintiff.

VI COPYRIGHT INFRINGEMENT

In cases involving copyright infringement on internet, the Indian courts have held that same principles that apply in offline world equally apply to the internet space. In a case before the Delhi High Court, *Gramophone Co. Of India Ltd.* v. *Super Cassette Industries Ltd.,*[26] the plaintiff filed a suit for permanent injunction to restrain defendants from issuing any sound recording which embodies the works (literary and musical works), in which the copyright is owned by the plaintiff. The plaintiff had also sought an injunction restraining the defendant from launching sound recordings which are remixed versions of the sound recordings, in which the plaintiff owns copyright that infringe the copyrights of the plaintiff. The plaintiff contended that it has not granted any right, permission or license to the defendant

22 2002 (25) PTC 322 (Del).
23 117 (2005) DLT 748.
24 MIPR 2007 (3) 380.
25 181 (2011) DLT 716.
26 2010 (49) PTC SY1 (Del).

to make version recordings of the works in which it has copyright. The court while disposing of the interim applications for grant of temporary injunction observed that when a version recording in compliance with section 52(1)(j) of Copyright Act has been made, it is as much a sound recording as any other sound recording would be of the original literary, dramatic or musical work which could have been made under a specific license from the author of such original works. The court further expressed that copyright protection applies with equal force on internet and held:

> The concept of the law does not change merely on account of the march of science and technology. The same principles continue to govern the field even after the advent of new technology. Numerous formats in which sound recordings are distributed have been evolved with the passage of time, such as audio magnetic tapes, compact disks and digital copies which are distributed electronically over the internet or through mobile telephones. In my view, the right of the owner of the copyright in the version recording to sell or give on hire or offer for sale or hire the version recording, and his right to communicate his version recording to the public is in no manner curtailed by reference to the format in which the version recording may be sold or hired or offered for sale or hire.

The court observed that there is no limitation contained in the Copyright Act which prohibits the exploitation of the version recordings by sale/hire of copies of the version recording, as a version recording through mobile telephones or through the internet.

Hence, on this reasoning, the court found there is nothing in the Copyright Act from which it might be inferred that the Parliament intended to limit the statutory license under section 52(1)(j) to any particular mode of distributing copies of the version recording. The court clarified that in any case, the making of copies of the version recording and its sale ought to comply with the requirements of section 52(1)(j) and rule 21 of the Copyright Rules.

VII CYBER CRIMES

Tampering of source code

In *Syed Asiffuddin* v. *The State of Andhra Pradesh*[27] Tata Indicom employees faced charges of hacking with computer source code under section 65 of the IT for manipulating the electronic 32 bit number (ESN) programmed in cellphones which were to be used only on Reliance Info Com Service Network. Under section 63 of the Copyright Act, any infringement of the copyright in a computer programme is punishable. Therefore, prima facie, if a person alters computer programme of another

27 2005 Cr; LJ 4314. 'Computer source code' or source code, or just source or code may be defined as a series of statements written in some human readable computer programming language constituting several text files but the source code may be printed in a book or recorded on a tape without a file system, and this source code is a piece of computer software. The same is used to produce object code. But a programme to be run by interpreter is not carried out on object code but on source code and then converted again.

person or another computer company, the same would be infringement of the copyright. The court held that such tampering of code amounts to tampering with the computer source code and will not be covered by fair dealing and other exceptions to copyright infringement under section 52 of the Copyright Act as it was not reverse engineered to perform the intended function it was supplied for and nor was it reverse engineered for a lawful purpose. Also, Tata Indicom are a competitor and not a lawful processor within the meaning of section 52 of the Copyright Act. As the phone was reverse engineered with the unlawful objective of unlocking the code so that it can be even used on Tata Indicom Network, it sufficed ingredients required under section 65 of the IT Act, 2000. Therefore, in the proceedings for quashing of the FIR, while the court quashed FIR with respect to sections 409, 420 and 120-B of IPC but declined to quash it under section 65 of the IT Act, 2000 and section 63 of the Copyright Act, 1957.

Hacking under section 66 of IT Act, 2000

Indian courts, in the recent past have dealt with past cases pertaining to hacking of computers under IT Act, 2000. In *Abhinav Gupta* v. *State of Haryana*[28] the petitioner was accused of hacking confidential information, confidential drawings and design plans of his former employer while he was in the employment. He had allegedly intentionally provided the confidential information to the competitor of his former employer. The High Court of Punjab and Haryana had to decide on the petition filed, under section 438 of the Cr PC by which the petitioner sought an order of anticipatory bail with respect to an FIR filed under section 66 of the IT Act, 2000 and sections 420 and 406 of the IPC. The court examined the definition of 'hacking' under section 66 of the IT Act, 2000 and found from screen shots filed by the defendants that the petitioner had transferred confidential information during his earlier employment to his personal e-mail address and later disclosed the same by forwarding it to the e-mail box of the competitor which he joined later. The court declined to accept the petitioner's plea that such material was forwarded to his personal mail id for discharge of his duties on the ground that he ought not to have in any case forwarded the same to the competitor company where he subsequently took the employment. The court, while considering the accused petitioner as a 'hacker' who extracted information for his own pecuniary benefits and for the benefit of his subsequent employer, declined to grant anticipatory bail to the petitioner.

Phishing

Phishing is a financial crime wherein a cyber criminal poses as a genuine party such as a bank and steals sensitive financial information from the victim to defraud him for making wrongful pecuniary gains. In *National Association of Software and Service Companies* v. *Ajay Sood* [29] the court explained the meaning of phishing as a cyber crime where the criminals use internet and computer to cheat gullible people by impersonating genuine entities such as a bank to steal personal sensitive information such as credit card numbers and misuse the same to make unlawful

28 2008 Cri LJ 4536.
29 119 (2005) DLT 596.

money. In this case, the court injucted the defendants 1 and 4, their servants and agents from circulating fraudulent emails purportedly originating from plaintiff or using any name/mark/address of the plaintiff amounting to tarnishment and passing off. In *Shri Umashankar Sivasubramaniam* v. *ICICI Bank,*[30] the petitioner has evoked section 43 read with section 46 of IT Act, 2000 and section 85 of IT Act. The petitioner filed a case for claiming compensation under section 43 of the IT Act, 2000 as he was made a victim of phishing attack from an email that appeared or seemed to have been sent by his bank requesting him to update his personal account data. When the bank contended that the petitioner was negligent, the adjudicating authority took the view that the bank did not adopt due diligence measures to make its banking system secure. It was observed thus:

> Respondent Bank namely ICICI has failed to establish that due diligence was exercised to prevent the contravention of the nature of unauthorized access as laid out in Section 43 of the Information Technology Act of 2000. The Respondent Bank has failed to put in place a foolproof Internet Banking system with adequate levels of authentication and validation which would have prevented the type of unauthorized access in the instant case that has led to a serous financial loss to the petitioner customer. The basic loophole in ensuring that a customer recognizes an email as from the bank was a glaring error on the respondent's part that would have prevented this incident. The degree of connivance or complicity may be debated upon but the neglect of the personnel of the Respondent Bank both immediately prior to and immediately after the loss in protecting the interests of the customer are clearly evident. Adequate checks and safeguards have not been planned together with the fact that the effort to investigate and track the perpetuator of the fraud who was a subject of its own procedures is being made a customer are seen to be poor. The Know Your Customer norms have been violated in letter and in spirit. The petitioner has been made to run around in search of justice and retribution following the incident without any support from the bank. The Respondent Bank is found guilty of the offences made out in Section 85 read with relevant clauses of Section 43 of the Information Technology Act of 2000.
>
> The petitioner was awarded a sum of Rs. 12,85,000/- as compensation.

Similar to the concept of phishing are the concepts of 'smishing' and 'vishing'. Smishing is use of sms on mobiles to make financial gains by cheating and impersonating a genuine service provider and vishing is use of voice recordings or phone calls to achieve the same objective. However, no cases have been reported to have been decided by Indian courts so far on these two emerging concepts of cyberspace.

30 Decision dated 12.04.2010 out of civil jurisdiction petition no. 2462 of 2008 (Office of the Adjudicating Officer and Judicature at Chennai).

VIII PUBLISHING OF OBSCENE MATERIALS ON INTERNET

Another important aspect of emerging cyber laws is whether there are any settled parameters to judge online obscenity in India. In *Ranjeet Udeshi's* Case,[31] the Supreme Court of India had laid down the test for judging offline obscenity in India. The court relied on the 'Miller Test' in the United States which established three step test of obscenity namely:

i) If the average person considers the work as a whole to be obscene on the basis of contemporary community standards;
ii) If the work is patently offensive and describes any sexual conduct defined by a state law;
iii) If the work in totality lacks serious literary, artistic, political or scientific value.

Relying on the Miller Test, the Supreme Court of India held that obscenity would appeal to the carnal side of human behaviour and shall not be protected by fundamental right to freedom of speech and expression. The work needs to be considered as a whole and judged while considering as to whether it is so gross that it is likely to deprave and corrupt the readers. In this case, the court took the view that section 292 of IPC prohibiting sale of obscene materials is constitutionally valid under article 19 (2) of the Constitution and held the book 'Lady Chatterley's Lover' written by D.H Lawrence as obscene.

Later in, *Chandrakant Kalyan Das* v. *State of Maharashtra,*[32] the court observed that the definition of 'obscenity' is not provided in section 292 of IPC or in any legislations prohibiting publishing or sale of obscene objects. The court further observed that the term 'obscenity' varies from jurisdiction to jurisdiction based on the cultural and moral standards of any society. The Supreme Court of India adopted the 'Most Vulnerable Person Test' given in the *Regina* v. *Hicklin*[33] wherein the court held that, the test for obscenity was applicable to separate portions of a work also apart from work as a whole.

However, this test was replaced by the Supreme Court in *Ajay Goswami* v. *Union of India,*[34] wherein the court held that selling and publishing of obscene material is not protected by freedom of speech and expression under article 19 of the Constitution of India. The court rightly observed that '*community based standard test'* is obsolete in the internet age which has converged the world into one global place. In the instant case, the court took a liberal view and described the '*responsible reader test'* to judge obscenity. It held that publication should be judged as a whole and the content needs to be examined with a *responsible reader standard*. The court held that a complete ban on publishing news items or pictures will deprive adults from reading entertainment content that is "permissible under the normal norms of decency in any society".

31 1965 1 SCR 65.
32 1970 AIR 1390.
33 1868 Vol 3 QB 360.
34 2007 1 SCC 143.

Obscene materials on the internet

Some interesting cases have been dealt by Indian courts pertaining to section 67 in the IT Act that provides punishment for publishing or transmitting obscene material in electronic form. The earliest case on section 67 is the *State of T.N* v. *Suhas Katti,*[35] wherein the court sentenced the accused to imprisonment for two years for publishing obscene messages against a divorcee woman in a yahoo message group. E-mails were also forwarded to the victim by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. The accused was held guilty under sections 469 and 509 of the IPC read with section 67 of the IT Act, 2000. The case also illustrates the efficient management of cyber forensic evidence which resulted in the conviction in a cyber crime.

In another case, *N. Saravanan & L. Prakash* v. *State,*[36] decided by the High Court of Madras, the accused was a doctor who allegedly photographed and video recorded intimate activities of his women patients. The intimate activities were posted on internet and the petitioner thus amassed several crores. The accused was subsequently prosecuted under section 67 of the IT Act, 2000. The petitioner filed bail application which was rejected by the court. By dismissing the present *habeas corpus* petition the court refused to quash the FIR and investigation.

In another landmark case, *Avnish Bajaj* v. *State,*[37] the Baazi.com website published a MMS clip which offered for sale a video clip, shot on a mobile phone, of two children of a Delhi school indulging in sexual act. The managing director of the company was arrested and he lodged an action in the court to annul criminal proceedings against him for making available for sale and causing to be published an obscene product within the meaning of section 292 of the IPC and section 67 of the IT Act, 2000. The petition also raised questions under section 482 of the Cr PC concerning question of criminal liability of directors for offences committed by the company under the IPC and the IT Act, 2000, especially when such company is not arraigned as an accused. The court held that the website had published an obscene material and prima facie case is made against the company under section 292 of the IPC and section 67 of the IT Act, 2000. In the charge sheet it was noted that the listing on the website itself contained obscene words indicating child pornography in the MMS clip. The court held that under the IPC, the director was not automatically liable criminally as per section 292 because it did not envisage an automatic liability of directors. However, the court firmly held that under section 85 of the IT Act, 2000, the director is personally liable since the section stipulates deemed criminal liability of directors where the offence is committed by a company. The court observed thus:[38]

> A prima facie case for the offence under Section 67 read with Section 85 IT Act is made out against the petitioner since the law as explained by the

35 Judgement delivered on 5.11.2004 by Additional Chief Metropolitan Magistrate, Egmore.

36 MANU/TN/8296/2006, decided on 16.03.2006 by the High Court of Madras.

37 150 (2008) DLT 769.

38 *Id*. at 800.

decisions of the Supreme Court recognizes the deemed criminal liability of the directors even where the company is not arrainged as an accused and particularly since it is possible that BIPL (EIPL) may be hereafter summoned to face trial. Consequently, while the case against the petitioner of the offences under sections 292 and 294 IPC is quashed, the prosecution of the petitioner for the offence under section 67 read with section 85 IT Act will continue.

IX LIABILITY OF INTERMEDIARIES FOR THIRD PARTY CONTENT

Liability of intermediaries on internet recently became the most debated topic when Google search engine and Facebook two social networking site, amongst others, were sued for allegedly hosting anti-religious and offensive content on their websites. The Delhi High Court ordered 22 websites to remove the objectionable content from its sites and asked Google and Facebook to develop a mechanism to keep a check on these websites.[39] Both civil and criminal cases were initiated against these service providers for hosting illegal content which brought issues such as censorship, due diligence and filtering to the fore front. Section 79 of the IT Act, 2000, was amended by the IT (Amendment) Act 2008 to clarify the liability of intermediaries in the IT Act, 2000 and broadened the definition of the term 'intermediary'.

Section 79 of the IT Act places a burden on the intermediary to remove any unlawful third party materials, on receiving actual knowledge of illegal contents on its websites. Those websites which do not regularly monitor or select contents of third party content, cannot be imputed with actual knowledge or intention unless actual notice is served on the intermediary by third party or brought to notice by a government agency. Recently, Ministry of Communication and Information Technology, Government of India issued the Information Technology (Intermediary) Guidelines Rules, 2011. These Rules provide due diligence requirements by intermediary, obligation to publish its terms of use, privacy policy and other obligations. It is important to note that according to rule 3(2), an intermediary is responsible to inform the users via terms of use, of prohibition on posting certain objectionable and illegal content, *inter alia*, not to upload, publish, display, update or share any information which is defamatory, obscene, invades the privacy, abets money laundering, is harmful to minors, infringes intellectual property, is grossly offensive or content that is virus infected or use 'spoofing', 'phishing' or content that threatens unity or security of India or provokes commission of any cognizable offence. As per rule 3 (4) of the said rules, an intermediary shall not knowingly host or publish such information and on receipt of an electronically signed complaint by an affected party, remove the same within 36 hrs from receipt of the complaint.[40] In case of non compliance by a user of its terms of use, privacy policy or rules, intermediary is entitled by rule 3(5) to terminate access or usage rights of a user to computer resource of intermediary and remove

39 *Supra* note 2.

40 Rule 3(4), Information Technology Guidelines Rule, 2011.

the non compliant information. Since the ambit of the said 'prohibitory clause' is fairly wide, a clarification on its correct interpretation is required from the Indian courts on the *meaning and scope of some of the terms* used therein so as to prevent ambiguity in the application of law.

X ADMISSIBILITY OF ELECTRONIC EVIDENCE

Indian courts have held electronic records to be admissible in evidence wherever a record is digitally signed there is a presumption of its authenticity under the Indian Evidence Act. Similarly, where a certificate by chief technology officer of a company is given under section 65B of the IT Act, 2000 electronic records are admissible in any legal proceedings without further proof or production of original as an evidence. Even if such certificate is not filed, print outs of e-mails or other records could be proved as secondary evidence under section 63 of the Evidence Act read with section 4 of the IT Act concerning legal recognition of electronic records.

In a case before the Supreme Court of India, *K.K Velusamy* v. *N.Palanisamy*,[41] the court held that a compact disc can be produced as a piece of evidence as per amended definition of 'evidence' in section 3 and 'electronic record' in section 2(t) of the IT Act, 2000 that includes a compact disc containing an electronic record of a conversation. The court held that it is similar to a photograph and can be received in evidence under section 8 of the Evidence Act, 1872. Earlier, *in R.M Malkani* v. *State of Maharastra,*[42] the Supreme Court held that electronically recorded conversation is admissible in evidence if the conversation is relevant to the matter in dispute, the voice is identified and the accuracy of the recorded conversation is proved by removing the possibility of deletion, alteration or manipulation.

In *Dharamvir* v. *CBI,*[43] the court considered a case where CD intercepted telephone conversations which were copied from hard disks and were produced as evidence in a legal proceeding. The court dealt with the question as to whether the said content can be considered as electronic record. The court observed that the recording of telephone calls and even hard disk shall constitute electronic record that can be led as evidence, as a hard disk may contain active information that can be analysed through forensic software.

On a similar reasoning in *CBI* v. *Abhishek Verma,*[44] the court took the view that every form of electronic record including data on CD, USB and floppy are admissible in evidence where they are submitted in accordance with section 65 (A) & (B) of the Evidence Act.

In *Shri P. Padhmanabh* v. *Syndicate Bank Ltd,*[45] the court dealt with a case where a nationalized bank had issued an ATM card which was allegedly used by the owner to draw money continuously for three days well exceeding the balance in his account. The court observed that the ATM machine was malfunctioning and

41 (2011) SCC 275.
42 AIR 1973 SC 157.
43 148 (2008) DLT 289.
44 (2009) SCC 300.
45 AIR 2008 Kant 42 : 2008 (1) Kar LJ 153.

there was irregularity in maintaining the books of account in the normal course of business. The court on the basis of this reasoning held that no presumption of authenticity about the entry of electronic records relied by the bank could be made in favour of the bank under section 65 (A) & (B) of the Indian Evidence Act.

In *State* v. *Mohammad Afzal,*[46] the court held that any challenges to accuracy of computer evidence on grounds of misuse or operational failure or tampering should be proved by the person challenging its reliability and only making allegations would not be sufficient. In this case, the prosecution produced the evidence of mobile number records of phone numbers found on a slip of paper at the parliament attack location and mobile phones which were confiscated from the accused. The prosecution was able to prove its electronic record files which were call records that were computer generated and the testimony of witnesses established that the calls pertained to the services provided by the concerned company. The court observed that there was no suggestion given to any of the witnesses that their computers were malfunctioning. Thus, the said call records were held to be admissible in evidence and proved through testimony of witnesses. By referring to section 65B of the Evidence Act the court also observed thus:

> The sub-section 4 makes admissible an electronic record when certified that the contents of a computer print out are generated by a computer satisfying the conditions of sub-section 4, the certificate being signed by the person described therein. Thus, Sub-section (4) provides for an alternative method to prove electronic record and not the only method to prove electronic record.

In *State* v. *Navjot Sandhu,*[47] the court held that in case the certificate containing details of section 4 of section 65 (B) of the Indian Evidence Act is not filed, the same can still be produced as secondary evidence under section 63 of the Evidence Act. The court observed thus:

> According to Section 63, secondary evidence means and includes, among other things, "copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies". Section 65 enables secondary evidence of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. It is not in dispute that the information contained in the call records is stored in huge servers which cannot be easily moved and produced in the Court. That is what the High Court has also observed at para 276. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service providing company can be led into evidence through a witness who can identify the signatures of the certifying officer or otherwise speak to the facts based on his personal knowledge. Irrespective of the compliance of the requirements of Section 65B which is a provision dealing with

46 2003 VII AD DEL 1.
47 2005 (11) SCC 600.

> admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely sections 63 & 65. It may be that the certificate containing the details in sub-section (4) of Section 65B is not filed in the instant case, but that does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely sections 63 & 65.

Thus, Indian courts have consistently recognized that electronic records are admissible as an evidence in legal proceedings and its authenticity could be proved through certificate of chief information officer under section 65B (4)of the Evidence Act or through oral testimony of witnesses.

Tax law and Internet cases

Unprecedented growth of e-commerce has brought many interesting cases before Indian courts and tax authorities in the respect of determining tax jurisdiction and application of tax law to sale or licensing of digital goods and e-businesses. In *Dy. C.I.T, Non-Resident Circle, New Delhi* v. *Metapath Software International Ltd.*,[48] the assessee was a UK based company providing software and hardware to telecom companies based in India. In this case, the hardware was supplied by the assessee to Indian customers directly from overseas. The title in the hardware was transferred and payment was made outside India. The assessee also did not market its products within India and assessee and Indian parties contracted on principal to principal basis. The court held that no permanent establishment could be deemed to be established in this case and the income arising out of the sale of hardware to the customers would not be taxable under Indian income tax laws. As regards software, by virtue of section 9(1) [vi] of the Income Tax Act, 1961 the consideration for a license for a software is taxable in India only where the license of software connotes transfer of all or any of the copyrights with respect to the software provided. In this case, the software did not entitle the customers to license, distribute or make copies thereof but were only allowed to use the software. Therefore, the term royalty was held not to cover such a case.

In *Lucent Technologies Hindustan Ltd* v. *Income Tax Officer,*[49] the assessee was a manufacturing seller of electronic switching systems required for the telecommunication industry and substantial part of its sales were made to the department of telecommunications (DOT), Government of India. It imported certain systems from its parent company in USA and did not deduct tax at source from the payments made. The assessee was served a notice of default under section 201(1) of the Income Tax Act, 1961 demanding interest for default. The assessee contended that no TDS was deducted since the sale of software and hardware 'are inextricably linked for its functioning'. It was also contended that the payments were made outside India and the supplier had no permanent establishment in India. The income tax appellate tribunal held that assessee's transactions with Lucent USA were a

48 2006 (9) SOT 305 NULL.
49 2005 (92) ITD 366 BLR.

purchase of integrated equipment comprising of both hardware and software both being functionally interdependent which forms the sale of a copyrighted article. The tribunal held that the assessee never required any ownership rights over the software as the assessee could not reproduce, reuse or sell the same to others. Therefore, the tribunal held that the payment was made for license for its use. In this case, both the income tax authority and commissioner of income tax (appeals) adopted the view that payment for hardware and software could be regarded as royalty. However, the Appellate Tribunal held an opposite view that payment made for import of software did not amount to royalty and no TDS was deductible for such payments. Further, the sale of integrated equipment comprised of hardware and software which were interdependent for its operations and the purchase of software was not a separate transaction. Vacating the orders passed by the income tax officer in the case, the tribunal held that the department is not justified in treating the impugned payments as royalty simpliciter and holding that the assessee is an assessee-in-default for failure to deduct tax at source.

In *Tata Consultancy Services* v. *State of Andhra Pradesh,*[50] the apex court examined whether the canned software that comprised of intangible intellectual property sold by the appellants can be deemed to be "goods" and as such assessable to sales tax under the Andhra Pradesh Sales Tax Act. The court observed that canned software containing information when stored in a physical medium gets transferred from an intangible to a tangible medium and is liable to be taxed on the interpretation of the term 'goods' under Andhra Pradesh General Sales Tax Act.

In *Commissioner of Income Tax* v. *Oracle Software Ltd.,*[51] the Supreme court took the view that a process that makes an article fit for use amounts to 'manufacture' and running a duplication activity on a duplicating music system to make a CD fit for use will thus amount to 'manufacture' under section 80IA(1) read with section 80IA(12)(b), of the Income Tax Act, 1961. The court relied on the apex court's judgment in *Gramophone Co. of India* v. *Collector of Customs, Calcutta*[52] and rejected the view that there is no manufacture if the original and copied content is from the same source. The court observed that the moment there is transformation into a new commodity which is commercially known as a distinct commodity and has its own character, utility and name, irrespective of number of processes it involves, manufacture takes place. The court clarified that the transformation of the goods into a new and different article should be such that in the commercial sense it will be known as another and a different product.

In yet another case, *Bharat Sanchar Ltd* v. *Union of India,*[53] the Supreme Court examined the question whether the mobile phone services could be classified as goods or services or both and whether sales tax /service tax or both will apply to this industrial sector. The apex court observed that goods can be intangible. The

50 AIR 2005 SC 371.

51 2010 320 ITR 546 (SC).

52 (1999) INSC 402, 25th Nov, 1999.

53 (2006) 286 ITR 273 (SC) (BCAJ): (2006) 3 SCC 1. In *Associated Cements Co. Ltd.*, 2001 (4) SCC 593 the court clarified that computer software will be considered as goods even though it is also copyrightable as intellectual property.

court observed that these may be either tangible or intangible property. In order to constitute 'goods', the court elucidated that basic features such as utility, marketability and transferability needs to be assessed and fulfilled in a given case. It was held:

> If the SIM Card is not sold by the assessee to the subscribers but is merely part of the services rendered by the service providers, then a SIM card cannot be charged separately to sales tax. It would depend ultimately upon the intention of the parties. If the parties intended that the SIM card would be a separate object of sale, it would be open to the Sales Tax Authorities to levy sales tax thereon.

The court further held that if the sale of a SIM card is only incidental to the service being provided and in order to facilitate the identification of the subscribers, their credit and other details, it would not be assessable to sales tax. On this reasoning, the Supreme Court criticized the high court in erroneously including the cost of the service in the value of the SIM card.

XI MISCELLANEOUS

Service of court notice through e-mail

In a recent case*, Central Electricity Regulatory Commission vs National Hydroelectric Power Corporation,*[54] the Supreme Court held that court notices should be also sent by e-mail apart from registered post, in order to avoid delays and piling up of arrears and such practice should be followed in all commercial litigation and where urgent relief is sought in the Supreme Court. The court held that the soft copy of the appeal or petition can be sent in a pdf format. This is a welcome judgment which will expedite service of court notices and serve interest of all parties.

Contracts formed through electronic means

In *Shakti Bhog Foods Ltd.* v. *Kola Shipping Ltd.*[55] and *Trimex International* v. *Vedanta Aluminum,*[56] the court elucidated the legal recognition of electronic contracts by holding that intention of the parties is the material consideration and the form of agreement is only secondary in contract formation .These principles are also reflected in section 10A of the IT Act, 2000 as inserted by IT (Amendment) Act, 2008 which expressly grants legal recognition to contracts formed through electronic means. The court in *Shakti bhog* case held that it is explicit from the provisions of section 7 of the Arbitration and Conciliation Act, 1996 that existence of the arbitration agreement can be inferred from a document signed by the parties or even by letters, telex, or other means of communication that reflects record of an arbitration agreement formed between the parties.

54 2010(10) SCC 280
55 2009 (2) SCC 134.
56 2010 (3) SCC 1.

XII CONCLUSION

This survey has attempted to capture important judgments delivered by the Indian courts on cyber laws. Clear principles to determine jurisdiction in internet law cases have been established by Indian courts by adopting 'targeting approach' as elucidated by the decision in the *Banyan Tree* case. Also, clear principles have been laid down by the courts in domain name dispute cases wherein courts have held that equal protection ought to be provided to trademarks of a service provider or vendor on the internet. Indian courts have upheld the admissibility of producing electronic evidence and recognized that even secondary evidence in respect of electronic evidence can be produced in a legal proceeding as per section 63 of the Evidence Act. Certain pertinent legal issues, such as liability of intermediaries and internet censorship, have been recently brought before Indian courts in 2011 for adjudication which clarified the due diligence requirements expected from intermediaries that operate in India. By and large, the development of cyber laws in India through court decision has been positive and progressive in the year 2011.