LIABILITY OF ONLINE INTERMEDIARIES: EMERGING TRENDS

*Talat Fatima**

I Introduction

ONLINE INTERMEDIARIES are unconscious actors in the internet transaction and they have no preexisting legal relationship with other actors.[1] Derisory discourses in legal circles for the arraignment of these important virtual players in the offline world are gaining momentum. Though some sort of commonality in the forerunners of these online intermediaries, namely, the telephone and postal carriers is discernible; their liability frameworks are remarkably different as the automated transmission marks the dividing line between the online communication transmitters and landline carriers of yesteryears.

The virtual world of cyberspace is abounded with all the echelons of human society, be it artists, statesmen, organizations, businesses, individuals or so to say criminals. Without the agency of human hand the virtual world will not exist. Thus, though the criminal act may be committed in an utmost intangible environ its perpetrators are but from the real world. The liability factor in the internet arena is exacerbated by the anonymity and intangibility which have become the hallmarks of the crimes being committed in the internet age. It is seen that the ISPs have taken multifold roles like that of access providers, network providers and hosts and with it the liability falls into different components depending on the particular role the internet service provider (ISP) was involved in respect of the disputed act. Though the online intermediaries operate through software which works automatically, giving no controlling power to them, yet they are the preferred targets of the aggrieved claimant.[2] The effect of uncensored online content is so

*Lecturer & Head, Department of Law, Government PG College, Dholpur Rajasthan.

1. Chris Reed, *Internet Law* 89 (2005).

2. *Ibid*. There are three reasons why an online intermediary might be the target of third parties: *firstly*, the originator of the offending information content has insufficient assets to pay substantial damages; *secondly*, the originator of the offending content may be in a foreign jurisdiction; *thirdly*, action against the originator may not be very effective as he may move to a different server and action against the intermediary will result in blockage of the offending content.

immense that it can even incite one to commit an offence, for instance in the UK in the wake of the brutal murder of Jane Longhurst in 2003 viewing of obscenity played an important role in the commission of crime[3] as it was revealed that the killer, Graham Courts was a regular viewer of images of necrophilia and asphyxial sex and hence a reform to control online obscenity was suggested in the *Home Office Consultation Paper*[4] which proposes to establish a *possession offence***.** The reform rests on the view that it is no longer possible, due to technological developments, to control the supply of such images.[5] This also imposes greater responsibility on online intermediaries especially ISPs to prevent access to the pornographic content. But the *Consultation* contains little discussion of how intermediaries, such as ISPs could help limit the dissemination of such material.[6] As the intermediaries are the preferred targets they look for ways which will help them out of a possible legal entangle hence they resort to certain tactics like *disclaimers*[7] and *boundary markers*[8] to prevent liability mainly in the areas of liability arising out of contract or tort. ISPs help e-commerce by enabling internet users to disseminate information at low cost and to do so anonymously. The question of liability of such intermediaries

3. *R.* v. *Courts* [2005] EWCA Crim. 52.

4. *Consultation: On the Possession of Extreme Pornographic Material*. (Scottish Executive and Home office, 2005).

5. *Id*.at 23.

6. Jacob Rowbottom, "Obscenity Laws and the Internet: Targeting the Supply and Demand" *The Criminal Law Review* 105(2006).

7. Disclaiming or restricting liability for internet content usually takes the form of preventing a liability-inducing situation arising or disclaiming or restricting liability that may exist. *Disclaimers* are usually used to forego responsibility to a particular advice or information given on the internet should it cause any type of harm. As a *disclaimer* goes with the content on the Net it is always a part of the information provided and even though a *disclaimer* is there, if the overall effect of the information attaches responsibility on the owner then the disclaimer is of no use in saving the owner. The meaning of the *disclaimer* is also relevant to law provisions, which are governing the entire situation. However, a *disclaimer* is legally not acceptable in criminal matters particularly matter related with causing death and other bodily harm.

8. In the world wide web the boundaries between documents are blurred and the true site owner may often be lost when the user hops from one site to another without even knowing that the proprietors have changed. This usually happens in the online shopping malls. The site owner may also be only an introducer to third party suppliers and often it becomes hard to know as to who is the actual party with whom the user is interacting. In such cases the site owner often warns the user through a notice or buffer page that the site owner holds no responsibility for whatever is done by the third party. This again is helpful in avoiding some kind of tortuous liability.

arises when there is dissemination of illegal content and such liability is twofold - civil and criminal.[9] Quite recently this area of law has undergone a considerable change whereas effort is on to simplify the liability but at the same time to burden the online intermediaries with obligation to scan and filter the illegal content. Though their liability is multidimensional extending to the civil, tortuous and criminal entrenchment, the present paper sheds light mainly on the tortuous and criminal area addressing mainly the defamation liability where the largest number of cases have been reported and where landmark judicial pronouncements have evolved the corpus of law considerably in this area, examining at the same time India's stand on the most noisy discussion online.

II Online intermediaries: Building blocks of internet

The online intermediaries form the biggest chunk of liability - susceptible class.[10] The internet is an amalgamation of human and non-human agencies that are all equally important for its survival. The automation and uncertain mechanism often renders its human face namely, the myriad numbers of intermediaries liable for the activities online. The internet owes its existence to the infrastructure providers[11] who are its main survival plank. Intermediaries,[12] in the internet context are organizations whose services are used to facilitate

9. Ernst-Jan Louwers, Corien E. J. Prens; *International Computer Law* 22-65 (2004).

10. *Ibid*. The E-Commerce Directive divides the ISPs acting as an intermediary into three categories: where they are passive and act as mere *conduits*; then where the intermediary is concerned with *caching;* and lastly where the role is limited to mere *hosting*. In all these cases awareness of illegal content on the part of the intermediary negates immunity.

11. It consists mainly of the underlying *physical structure* of wires, switches and other communications paths which carry information between hosts. These are controlled and managed by telecommunication companies and as they are merely concerned with the operation of *physical* equipments hence they have little legal significance. The other is the *facilitating infrastructure* of the internet, which consists
of the transmission, routing and directory services which allow the transmission of TCP/IP packets to their destination. These services are provided across the physical infrastructure by intermediary service providers. *Supra* note 1at 27.

12. The online intermediaries play two roles in the internet arena. Firstly, they provide fundamental communication services like access, information storage etc. Secondly additional service consists of providing identification and search

a transaction between communicating parties.[13] These intermediaries are several in number and consist of transmission hosts,[14] resource hosts[15] including website host,[16] newsgroup host,[17] FTP site host,[18] DNS hosts,[19] communication services including ISPs,[20] directory services[21] and transaction facilitation services including domain name

13. *Ibid.*

14. In internet, communication is successful if the packets are passed from host to host until they reach their destination. A host, which receives and transmits a packet is called transmission host. As they transmit packets, the transmission hosts copy them before resending them hence liability for the information content has received legal attention.

15. A user, who wishes to make information resources such as web pages, will need services of resources hosts. A resource host provides space on its disk storage for the user's resources and then runs software such as a web server, which handles requests from other users for access to those resources.

16. It is the most visible type of host as its domain name appears in Uniform Resource Locator (URL).

17. It is a discussion forum in which internet users can read and post messages and replies to postings from other users. A newsgroup is simply a database, containing user postings, which are posted for some weeks, and then they are moved to the archives. Newsgroup can be private but the most visible and widely disseminated newsgroups form part of Usenet.

18. An FTP is a collection of information resources which are accessed by downloading them to the user's disk storage though modern browser software can sometimes be used to display the requested file rather than saving it to disk for later viewing. The uploading of resources to the site can be general (or anonymous) or through passwords. FTPs are on the same footing as websites so far legal issues are concerned. *Supra* note 1 at 31.

19. The domain name system host is an important part of the infrastructure of the internet. The domain names systems hosts are registered under words which are indicative of either the country of origin or of the relevant department. DNS hosts maintain database, which match domain names to IP address. Though fundamental in the working of the internet, the DNS host is of little legal significance yet its allocation has raised some legal questions.

20. An ISP is a host which is connected full time to other hosts and which provides access and other services to its subscribers. Subscribers connect to the ISP through dial-up connection and leased lines. Some ISPs provide unrestricted access to all internet resources while others may restrict access to some selected resources, e.g., family friendly services etc. ISPs provide mainly access and ancillary services such as mailbox and website space while some of them offer a range of additional resources to subscribers only in addition to providing them with access to the wider Internet- AOL (www.aol.com). *Supra* note 1 at 32.

21. If a user knows the URL of a resource he can obtain access to it. Without the URL the resource is hidden from the user. Directory services are such services which help the user to overcome this problem. *Id*. at 33.

allocation,[22] identity services[23] and payment.[24]

III Levels of liability

This obviously calls for making the ISPs liable for separate roles, separately. Knowledge or control over the information distributed by the ISPs is the key factor in determining the liability of ISPs and computer systems operators. Even in the pre-internet age levels of liability were different in case of publishers, distributors, common carriers[25] etc. A hairline difference does exist among the various activities in which ISPs are involved. Thus, an ISP may perform the functions of an access provider, software distributor, host, cache or content provider.[26] As content is disseminated in a borderless world,[27] basically the contours of liability of these online intermediaries including the ISPs are in connection with the content which is transmitted, copied or possessed by them and which often offend the rights of individuals which either arise out of a contractual bond or are simply some sort of tort or criminal offence like defamation, copyright infringement, child pornography, false advertisement, fraudulent misrepresentation, breach of confidentiality and privacy, and so on. A paradigm shift is seen in this direction whereas the Electronic Commerce Directive[28] (hereinafter called the directive) establishes a single set of threshold requirements for the liability of certain online intermediaries in respect of a broad range of wrongs. The relevant intermediaries are "conduits" (which equate broadly to network and access providers), "hosts" (storage) and "caches" (those who create temporary caches of

22. Domain names are allocated by domain name registries, either at the country level (e.g. .uk) or at the global level (.com, .org etc.) *id.* at 36.

23. There is no necessary connection between a user's chosen online identity and his physical world identity. But identity of parties is vital in commercial transactions hence certification authorities have evolved who take evidence of a user's physical world identity and by electronic means certify that identity to the concerned parties. These identification services have received substantial legislative attention.

24. E-commerce transactions require payment systems online. Cheaper and more secure payment mechanisms are the demand of time hence more intermediaries are being evolved to serve the purpose.

25. Sharon K Black, *The Communication Law in the Internet Age* 419 (2002).

26. Graham JH Smith & Bird & Bird, *Internet Law and Regulation* 2 (2002).

27. Margaret J. Radin, John A. Rothchild, Gregory M. Silverman, *Internet Commerce: The Emerging Legal Framework* 1020 (2002).

28. *Liability of Intermediary Service Providers:* European Union Directive (08-02-2000) also called E-Commerce Directive. The directive though not exhaustive on the point is yet a welcome exercise. The directive was to be implemented before 17-

material to make for more efficient operation of the network).[29] The categorized liabilities of the online intermediaries are studied under the following heads which are contained in the directive.

Mere conduits

The liability of conduits is given in article 12 of the directive.[30] The telecommunications provider shall come within the above provision so far its transmission services are concerned. The hosting activities of the same company shall fall under a different provision. Clause 2 of the article further explains the activities of a conduit:

> The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

Thus, a conduit can still take advantage of article 12 even though the transmission includes automatic storage of information. There is also provision for saving the legal systems of member states. If an intermediary falls outside the scope of the directive, courts will still examine the tortuous or criminal liability of the provider with reference to the national law of the concerned state. Article 11(3) reads thus:

> This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Thus, exposure to an injunction would be assessed by reference to the relevant legal system.

---

29. *Supra* note 26 at 204.

30. Art. 12 reads thus: "1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; and

(c) does not select or modify the information contained in the transmission."

Hosting

The hosting[31] liability is given in article 14:

> 1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
>
> (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity of information is apparent; or
>
> (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
>
> 2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
>
> 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

The wording of the provision is such that it tends to provide both civil and criminal immunity. Unlike conduits or caching intermediaries, the reservation of infringement termination rights against hosts extends to procedures governing the removal or disabling of access to information.[32]

Caching

Article 13 contains caching liability, which follows the similar approach as for conduits.

Article 13 reads as such:

> 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall

31. Hosting is a service which consists of the storage of information for third parties. The directive declares that the host provider shall not be liable if he was unaware of the illegal activity.

32. *Supra* note 26 at 208.

ensure that the service provider is not liable for *the automatic, intermediate and temporary storage of that information,* performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

(a) the provider does not modify the information;

(b) the provider complies with conditions on access to the information;

(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;

(d) the provider does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Caching means the temporary storage of information for technical reasons intended to achieve a higher speed of communication networks and faster access of such information.[33] Updating of information in clause 1(c) is useful in matters where the information is about facts relating to stock prices which often could be seriously misleading if not updated. The reference to technology in clause 1(d) covers the situation where the websites rely on usage data to justify advertising rates. If a user "hits" a cache instead of the source site, then the site may not capture the hit and will underestimate the usage.[34]

Limitation of intermediaries' liability

The EU Directive on Electronic Commerce,[35] in a harmonized manner, provide for situations in which the intermediaries covered by the directive cannot be held liable for certain acts. These limitations on the liability of intermediaries are to ensure basic services, which safeguard the continued free flow of information in the network, and to allow the internet and e-commerce to develop. The limitations on liability cover both civil and criminal liability, for all types of illegal

33. *Supra* note 9.
34. *Supra* note 26 at 209.
35. *Supra* note 28.

activities initiated by third parties. However, the directive does not affect the liability of the person who is at the source of the content and cases which are not covered by the limitations defined in the directive. Besides the matters dealt with by articles 12 to 14 some member states[36] provide for limitations on the liability of providers of hyperlinks and search engines. This is aiming to create incentives for investment and innovation and enhance the development of e-commerce by providing additional legal clarity for service providers.[37] In addition to this, article 15 prevents member states from imposing on internet intermediaries, with respect to activities covered by articles 12 to 14, a general obligation to monitor the information which they transmit or store or a general obligation to actively seek out facts or circumstances indicating illegal activities. But it does not prevent public authorities in the member states from imposing a monitoring obligation in a specific and clearly defined individual case.

In United States, the Digital Millennium Copyright Act, 1998[38] absolves the online service providers from liability for copyright infringement for: storing, linking, transmitting, routing, or caching infringing material. Under DMCA the service providers can limit their liability though the conditions of each limitation differ. Title II of the DMCA adds a new section - section 512 - to the Copyright Act to create new limitations on liability for copyright infringement by online service providers. The limitations are based on the following categories of conduct by a service provider: (i) transitory communications;[39] (ii) system caching;[40] (iii) storage of information on systems or networks

36. For example Spain, Austria etc.

37. First Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) dt. 21.11.2003 at 13.

38. DMCA implements two World Intellectual Property Organization (WIPO) treaties: (i) the WIPO Copyright Treaty, 1996 and (ii) the WIPO Performances and Phonograms Treaty, 1996. Title II of the Act -Online Copyright Infringement Liability Limitation Act - creates limitations on the liability of online service providers for copyright infringement when engaging in certain types of activities.

39. It limits the liability of service providers in circumstances where the provider merely acts as a data conduit, transmitting digital information from one point on a network to another at someone else's request. This limitation covers acts of transmission, routing, or providing connections for the information, as well as the intermediate and transient copies that are made automatically in the operation of a network (s. 512(a)).

40. S. 512(b) limits the liability of service providers for the practice of retaining copies, for a limited time, of material that has been made available online

at direction of users;[41] and (iv) information location tools.[42] Section 512 also contains a provision to ensure that service providers are not placed in the position of choosing between limitations on liability on the one hand and preserving the privacy of their subscribers, on the other.[43] Each limitation entails a complete bar on monetary damages and restricts the availability of injunctive relief in various respects.[44] A service provider may not be liable for monetary damages for copyright infringement caused by third parties as long as the service provider (i) does not know about the infringement, (ii) does not participate in the infringement and (iii) acts in good faith.

IV Defamation: Biggest liability online

The online intermediaries are often equated on the basis of functional similarity to telephone operators and postal agencies as they too, like these carriers are no more than "messengers" and carry the message, statement and information from originating point to the recipient point, from the author of such material to the end user. They are the agents of information which is in the process of transition. Apart from being a carrier the role of the intervening messenger may also take the form of a "publisher" who disseminates the content to the world at large. The question then arises as to who is to be held liable for such a harmful content? The originator or the carrier or the publisher? (as the case may be). The landline carriers had limited means and they were mainly in the form of telephone operators, postal agents or publishers but even then it was often seen that they were instrumental in harming the reputation of a person or causing him some mental loss. At such a time two views existed regarding the liability of such carriers or publishers.[45] The English law created the tort of libel as at that time new print technology called for a change in law so as to specify the liability arising out of such a change. Such a change called for a greater liability of such intermediaries as compared to the creator of such a message or content. In *Playboy Enterprises* v. *Frena*[46] the

41. S. 512(c) limits the liability of service providers for infringing material on websites (or other information repositories) hosted on their systems. It applies to storage at the direction of a user.

42. It relates to hyperlinks, online directories, search engines and the like. It limits liability for the acts of referring or linking users to a site that contains infringing material by using such information location tools (s. 512(d)).

43. U.S. Copyright Office Summary on the Digital Millennium Copyright Act of 1998 at 9.

44. S. 512(j).

45. Rodney D. Ryder, *Guide to Cyber Laws* 554 (2001).

46. 839. F.Supp.at 1552. (M.D. Fla. 1993).

district court held the defendant liable for infringing the distributing rights of Playboy, the content originator, and held that "Intent to infringe is not needed to find copyright infringement" and thus subjected the intermediaries to no-fault liability. The same thought was echoed in 1995 when the *White Paper* released by the Clinton Administration[47] refused to absolve the intermediaries from no-fault liability and held that "they are still in a better position to prevent or stop infringement than the copyright owner. Between these two relatively innocent parties, the best policy is to hold the service provider liable". This expanded prospect of liability raised major anxieties for the ISPs as it also showed the signs of hampering the growth of commerce and information technology. Thus, the imposition of liability on ISPs for third-party defamation and other speech torts provoked a strong congressional response in the form of section 509 of the Communications Decency Act, 1996.[48] The first amendment upholding the freedom of speech and expression leaned towards the service providers, curtailed their liability and favored free flow of information. Title II of the Digital Millennium Copyright Act[49] brought safe harbors for the service providers as it granted conditional immunity to them but at the same time imposed continuing obligation on them to limit the availability of infringing material.[50] Thus, legal position of the service providers remained unstable for long though judicial pronouncements analyzed the problem oft and on. As the EU Electronic Commerce Directive has a restricted application and as liability of online intermediaries takes the maximum toll and labor of most of the case law on the internet *infringement*, their liability is fixed in a number of other legislations some of which are pre-internet but their application is extended to these areas. The English courts have developed the law through various decisions and have minutely analyzed the role of the online intermediaries. Most of the cases coming to courts are regarding the liability of these intermediaries in respect of tort of defamation. An easy analogy is drawn between the online service providers and an inter exchange carrier in a long-distance telephone conversation. Thus, the backbone provider must be entitled to the same immunity from liability based on

47. *Intellectual Property and the National Information Infrastructure*, The Report of the Working Group on Intellectual Property Rights (Sep 1995).

48. 47 USC. s. 230. Another provision of the said Act imposed penalties for making indecent material available to minors. (Indecent material is protected by the First Amendment, obscene material is not) *Supra* note 27 at 1020.

49. 17 USC s. 512

50. *Supra* note 48.

communications that traverse its facilities as is enjoyed by telecommunications common carriers.[51]

Defamation: Boundaries of liability

Liability of service providers regarding defamation falls into two categories: liability as distributors and liability as publishers. As the contours of liability differ in each case they are discussed separately. Defamation is regarded as a tort as well as a crime in most of the legal systems of the world. The personal prestige of a person is jealously guarded by law. Like any other criminal activity, the wrong of *defamation* also received a boost in the internet age as the electrons became the powerful medium of proliferation of information whether healthy or incriminating.

Liability of online intermediaries for defamatory material- as a distributor:

Judiciary could identify the role of the online intermediaries in defamatory matters and fix the liability accordingly. In *Cubby, Inc.* v. *CompuServe Inc.*,[52] which is a landmark judgment on the point, the court, regarding CompuServe as an online intermediary, reached the conclusion that it was a distributor of the Rumorville publication which they carried as part of their journalism forum and were, therefore, not liable for the defamatory statement against the plaintiff which appeared in Rumorville.The outcome was based on the first amendment provisions which absolved the distributor for the defamatory contents if he had no knowledge of it. Though it was decided in *Cianci* v. *New Times Publishing Co.*[53] that ordinarily "one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it," yet in a number of other decisions[54] it was also held that vendors, book stores, and libraries, however, are not liable if they

51. Under common law, a common carrier required to transmit certain content is generally immune from defamation liability based on that content even if it knows of the defamation. *Restatement (*Second) *of Torts.* 612(2) (1965). Likewise, broadcasters are immune from defamation liability for equal-time material that federal state requires them to carry. [*See, Farmers Educational & Cooperative Union* v. *WDAY,* Inc., 360 US 525 (1959)] As quoted in *Internet Commerce—The Emerging Legal Framework.* 1020 (2002), *supra* note 27.

52. 776. F Supp. 135(S.D.N.Y. 1991).

53. 639 F. 2d 54, 61 (2d Cir. 1980).

54. *Lerman* v. *Chuckleberry Publishing, Inc*., 521 F. Supp. 228,235 (S.D.N.Y. 1981): accord *Macaluso* v. *Mondadori Publishing Co*., [527 F. Supp. 1017, 1019 (E.D.N.Y. 1981)].

neither know nor have reason to know of the defamatory content. In *Smith* v. *California*[55] the court had struck down an ordinance that imposed liability on a bookseller for possession of an obscene book, regardless of whether the bookseller had knowledge of the book's contents or not. The court regarded this provision as trying to achieve the impossible because a bookseller is not expected (nor capable of) reading each and every book in his shop. When CompuServe carries the publication as part of a forum that is managed by a different company, it has absolutely no editorial control over the contents. This is analogous to the librarian of a public library or a bookseller who has nothing to do with the editorial job of the books in his possession. A computerized database is thus the functional equivalent of a librarian or a newsvendor and hence to put a greater liability on an online news distributor as CompuServe is nothing but hampering the free flow of information which is against the letter and spirit of the first amendment. Plaintiff failing to establish that CompuServe had knowledge, or had reason to know (as required by the first amendment) that Rumorville statement had some defamatory element, allowed the court to rightly reach the conclusion that CompuServe was a distributor without knowledge of the contents and was hence not liable. It is thus obvious that as CompuServe neither installed any such electronic gadget of scrutiny nor made arrangements of censorship his job is restricted to that of a distributor *sans* editorial powers and so far the law provisions go he is not under obligation to pre-censorship of contents. He is thus rightly absolved from liability.

Liability of online intermediaries regarding defamatory statement-as a publisher:

Here the publisher who is scrutinizing and censoring the material to be published is liable under law in case such material is harming someone's reputation. A judicial pronouncement of the internet age *Stratton Oakmont* v. *Prodigy Services Co.*[56] takes into consideration the role of technology in the matter of censorship. Plaintiff's Stratton Oakmont Inc., a securities investment banking firm brought an action of defamation against Prodigy, the owner and operator of the computer network on which the defamatory statements appeared. Prodigy had around two million subscribers who communicate with each other on his bulletin board "Money Talk" on which the said statement appeared. On the bulletin board, the largest in United States, members can post statements regarding stocks, investments and other financial matters.

55. 361 US 147, 152-53 (1959).
56. 23 Media I. Rep. 1794 (N.Y. Sup.Ct. 1995).

Prodigy contracts with bulletin board leaders who participate in board discussions and also take promotional efforts to encourage usage and increase users. The entire matter revolved around one question and that is whether, Prodigy, involved in above activities is a publisher? It was shown in the course of the proceedings that Prodigy himself held out that he did exercise editorial power over its contents and this surely draws the distinction between CompuServe and Prodigy. Prodigy exercised this control through its automatic software screening program, and the guidelines which board leaders were made to follow. By actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and "bad taste"[57] they assumed the role of a publisher. Thus, here the precautionary measures, both technical and manual taken by the defendants, to give to its subscribers healthy and pure information entrenched him in the liability for defamation when such content offended against the plaintiff's reputation while all such restrictions even spoke against the freedom of expression. Perhaps this was one big reason when soon after *Prodigy* verdict the Congress came up with a covering piece of legislation vide 47 USC section 230 (c)(1)[58] which provided immunity to the ISPs and states; "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The wordings clearly indicate that the aim of the legislation is to remove the hurdle in the way of free flow of information by imposition of censorship etc. by the service providers and also to allow the service providers to work in an atmosphere without being apprehensive about the consequent liabilities which may arise from an incriminating content transmitted by an originator. The provision contains the word 'publisher' so as to avoid any controversy in future regarding the role of service providers in such situations.

V India's stand

As India too burgeons as an information super power, the internet-related issues become important and more so when freedom of speech and expression is preserved as a fundamental constitutional right.[59] Defamation in India is regarded both as a tort and a crime. Though no case related to the internet defamation has so far arisen the possibility

57. *Supra* note 27 at 1029.

58. Added by Communication Decency Act, 1996, s. 509, Pub. L. No. 104-104, 110 Stat. 137, 137-39 (1996)].

59. Art. 19(1) (a): Right to freedom of Speech and expression. Part III. *Constitution of India*.

however is always there. What exactly happens when a person's reputation is harmed by the content during the course of transmission on the internet? What will happen when during such course the online intermediaries are involved? What is the law applicable in such cases? Can the online intermediaries take the protection of section 79 of the IT Act? All this and more needs to be discussed.

Scope of section 79: Section 79[60] clearly exempts the online intermediaries from liability under the IT Act itself and does not mention ISPs liability under other Acts whether civil or criminal. Taking the wordings of the section literally liability under "this Act" shall mean extending immunity from civil liability for acts falling under any of the sub-sections of section 43 of chapter IX dealing with "Penalties and Adjudication" and from criminal liability falling under chapter XI dealing with "Offences". A scrutiny of section 43 and offences under chapter XI reveal that barring a few, most of the contraventions and offences listed therein are individual acts and the online intermediaries (ISPs) have little or no role to play in the commission of the crime, futile to talk of their liabilities under it. The most appropriate section, under which an online intermediary may seek protection of section 79, is section 67, dealing with publishing of information which is obscene in electronic form. From this one may infer that section 79 aims at giving limited immunity to the intermediaries only under the IT Act and not from liabilities arising under other statutes. That seemingly was not the intention

of the legislature as the scope of section 79 will be very narrow and the spirit with which it was enacted, namely protection of the service providers and encouraging free flow of information would be crushed.

Thus, keeping in mind that the intention of the legislature is to provide immunity to online intermediaries through section 79 it may be extended by the defence to the offence of defamation and to other offences entailing criminal liability. This position is further cleared by inclusion of section 67 in the IT Act where publishing of information

60. The relevant portion reads thus: **79. Network Service Providers not to be liable in certain cases-** For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation. —for the purposes of this section,

(a) "Network service provider" means an intermediary;

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

67 read with section 79 grants immunity to the service provider where the obscene material is published, transmitted or caused to be published in the electronic form through the agency of the service provider. The section also does away with the distinction between various roles which are played by the ISPs like the mere access provider, the content provider, hosts, caches etc. and in sub-section (a) only uses the general term 'intermediary' to explain the meaning of the term "network service provider'. This lacuna will place greater liability on the intermediaries, often for a liability which is not meant for him as such but for some other intermediary. Like, for example, often these intermediaries are acting as mere *conduits* which are often equated with distributors of the real world[61] and his liability is thus nullified in the absence of fault. Where the ISP is in the role of a *conduit* holding him liable under section 79 IT Act is unfair. Again an online intermediary may also act as a host where it stores the information of the recipient of the service and in such a case he is not to be held liable if it is stored at the request of the recipient provided the host is unaware of the illegality and if aware he acted expeditiously to remove it.[62]

Suppose A, an Indian online intermediary, receives for its bulletin board an article written by X in which some defamatory statements are made against Z. Here, A puts up the article on its bulletin board and Z sues him for defamation. What is the law which will help Z and hold A liable? Since it is a case of defamation, section 499 of the Indian Penal Code, 1860 would be invoked. The section does away with the distinction between a libel and slander. Since the defamatory matter appears on the internet, A will seek protection under section 79 of the IT Act claiming exemption. Here supposedly A draws an analogy between *publishing* information, which is obscene in electronic form, and *publishing* information which contains defamatory statement. Legally speaking A will be allowed to draw the analogy regarding the word *publishing* which is appearing in section 499 IPC and which is already giving immunity to A (as an online intermediary) when it appears in the context of section 67. There appears to be no legal hardship in such analogy as defamation like obscenity, is an offence which is breach of one's privacy and is also an anti-social offence and thus these two offences can be read *ejusdem generis*. In matter of internet defamation thus A can conveniently take the defence of section 79 where the incriminating matter is; "any third party information or data." The question then comes whether A was aware of the contents of the

61. *Stratton Oakmont, Inc.* v. *Prodigy Services Co.*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

62. E U. Electronic Commerce Directive, *supra* note 28.

matter?

Analysis: In the above matter first A's position will be examined under section 499[63] of the Indian Penal Code. The section requires, making or publishing imputation, such imputation must be made by words, either spoken or written or intended to be read, or by signs, or by visible representation. The key words in A's case are "making or publishing" and is to be seen whether A, as an online intermediary here, is to be held liable for it. As the matter is originated by X will A be also liable for "making" it? Here if it is proved that A had no knowledge of the contents of X's statement then he is not said to "make" the statement. But as A had put it up on the bulletin board what will be his position? Will he be regarded as the publisher of the material? As regarding the real life publishing act, a presumption under section 7, Press and Registration of Books Act, 1867 regarding awareness of the contents of a newspaper is raised only against the editor whose name appears on the copy of the newspaper. It was held way back in 1880 that publisher of a newspaper is responsible for defamatory matter published in such paper whether he knows the contents of such paper or not.[64] Reading the above two provisions together it is to be examined as to what is the position of A as an intermediary? Whether A exercised editorial control over the contents which he places on his bulletin board? If it is true then it is immaterial whether A actually exercised this control in respect of the incriminating statement against Z. As it is a matter of defamation the exemption given to a service provider in section 79 on the basis of absence of knowledge of the incriminating matter is immaterial. In matter of publication of defamatory statement the law under section 499 is strict and various judicial decisions also signify that the publisher cannot escape liability under the simple pretext of being unaware of the disputed material. Perhaps because murdering a man's reputation by a libel may be compared to murdering a man's person, in which all who are present and encouraging the act are guilty, though the wound was given by one only.[65] The chairman of a company owning the newspaper in which the offending news item is published cannot be held liable unless it is shown that he was somehow concerned with the publication of the defamatory news item.[66] Thus,

63. S. 499-Whoever by words, either spoken or intended to be read, or by signs or by visible representation, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.

64. *McLeod,* (1880) 3 All 342.

65. *Bacon's* Abrid. Vol. IV at 457.

"publication" carries with it direct and unconditional responsibility to the content published. The harm caused by publication is irreversible so far the reputation of a person goes. It is something which cannot be undone. In such a case holding only the writer or originator of the content liable is insufficient. Earlier, for example, if a newspaper, containing defamatory matter was sent by post from Calcutta, where it is published, addressed to a subscriber at Allahabad, the publication of such defamatory matter would be at Allahabad;[67] today its transmission on the internet where it is read by millions at the click of a button is the global publication of the defamatory material. The person responsible for such a global transmission is not the originator but the online service provider and his liability thus should not be restricted to a few tricky words that it was without his knowledge and he exercised due diligence to prevent it.[68] Being holders of unimaginable information, the position of a service provider is much more powerful than that of a publisher of a newspaper or magazine and hence the liability of a service provider, so far the offences of defamation, breach of privacy, child pornography etc. are concerned must be strict and should not be susceptible of being lost in the legal jargon. The simple reason for this is that these are the crimes which do not only affect the individual victim but erode the social and democratic fabric of the society. Even the freedom of speech as guaranteed under the Indian Constitution[69] is not unbridled. It is also saddled with certain restrictions which are given in article 19(2). These restrictions contain *inter alia*, *defamation* as a ground on which the freedom given under article 19(1)(a) can be authoritatively taken away. Thus, even the fundamental right to speech and expression cannot be used to harm the reputation of anyone. If service providers are not brought within the liability *qua* publisher it will be very difficult to disprove service provider's plea that he had no knowledge of the defamatory statement in the content as far as they are in the role of a *host* and are not functioning as *mere conduits*. At least when the service providers are employing technological scanning gadgets or are scrutinizing the contents they should not be allowed to take the plea of "no knowledge" regarding a particular piece of information. Moreover, in section 79(a) the interpretation of the term "network service provider" must be interpreted beyond "an intermediary" and must be specifically sub-categorized to include various roles an

66. Ratanlal & Dhirajlal, *The Indian Penal Code* 492 (1987).

67. *Girjashankar Kashiram* (1890) 15 Bom 286.

68. S. 79 IT Act.

69. Constitution of India guarantees to its citizens six personal freedoms under Art. 19. The first of these is under Art. 19 (1) (a) freedom of speech and expression which is the *sine qua non* of the democratic set up in India.

intermediary is involved in during the process of transmission so as to prevent them from avoiding liability in some individual-cum-society-related crimes like defamation, child pornography, etc.

VI Comparative Study

Various legislations discussed above regarding the liability of online intermediaries have underlined certain common principles: *firstly*, the intermediaries are given immunity from liability whether civil or criminal; *secondly*, the immunity is from third party content; *thirdly*, the defence of no-knowledge and reasonable care is also allowed to be taken. The contours of such immunity differ from country to country and United States ranks first in the list of countries showing a liberal attitude which is obviously for the sake of freedom of speech and expression since the first amendment in United States guarantees it. Section 230 of the Communications Decency Act, 1996 chose to "promote the continued development of the internet and other interactive computer services and other interactive media" and "to preserve the vibrant and competitive free market".[70] Section 230 was enacted to rewrite the law on immunity of service providers which suffered a jolt by the stern verdict of Stuart L. Ain J in the *Prodigy* case. The judgment drew an analogy between a publisher of a newspaper who enjoys editorial control over the contents of the newspaper and an online intermediary which (in the view of the judge) in the given case was enjoyed by the defendants. In view of the court "*a distributor or deliverer of defamatory material is considered a passive conduit and will not be found liable in the absence of fault.*"[71] The court referring to a decision says that a newspaper is more than a passive receptacle or conduit for news, comment and advertising[72] and says that with the editorial power comes liability. The conclusion reached thereby is that the online intermediary in *Prodigy* had exercised editorial control and is hence liable for the incriminating material. The purpose[73] of the enactment of section 230 as given in the Conference Report is to undo the effect of the decision of *Prodigy* and to immunize ISPs against defamation liability. In contrast to the United States, in Germany in December 1995 a German CompuServe official was criminally

70. *Supra* note 27 at 1042.

71. *Auvil* v. *CBS* 60 Minutes, 800 F. Supp. 928,932.

72. *Miami Herald Publishing Co.* v. *Tornillo,* 418 US 241, 258.

73. The purpose of s. 230: "One of the specific purposes of this section is to overrule *Stratton Oakmont* v.*Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material. The conferees believe that such decisions create serious obstacle to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services." *Supra* note 27 at

prosecuted for distribution of child pornography.[74] In response to prosecutors' notice CompuServe's German subsidiary blocked access to over 200 USENET newsgroups which were suspected by the investigators of carrying pornographic material. Felix Somm, the managing director of CompuServe was prosecuted under an Act prohibiting publications which are deemed harmful for children. They sought to hold Somm liable for CompuServe's provision of access to USENET newsgroups containing pornographic material. Though German legislature passed an Act to limit the liability of ISPs for third-party communications, but the court taking a stern action refused to apply the changed law and even refused to accept the defense argument that it is technically impossible to filter out all offensive material on the internet.[75] Again United Kingdom and other European countries have stricter laws against defamation than the United States, and fewer defenses.[76] Thus, in the case of *Godfrey* v. *Demon Internet Ltd.*[77] the court held an ISP, Demon Internet liable for third-party content. Here the plaintiff informed the Demon Internet to delete a forged message about him on the USENET newsgroup by some person. The Demon Internet failed to do it and Godfrey sued for defamation. When the defendant (Demon) took the defense of "innocent dissemination" as given under the UK Defamation Act which is available on the ground of "reasonable care" and no-knowledge and no reason to believe that he was publishing a defamatory material, the court refused to accept it on the ground that Godfrey had informed him of the posting. The UK court though discussed the US cases – *CompuServe, Prodigy* etc., but refused to follow them. As for section 230 of CDA the court commented "In my judgment the English 1996 [Defamation] Act, did not adopt this approach or have this purpose".[78] Thus, every country has its own legal culture which in spite of having some common principles of jurisprudence do have varying shades of interpreting them. India appears to be closer to the interpretation made by the UK courts as in India too due to the prevailing cultural ethos and constitutional dictates offences like obscenity, pornography and defamation are bitterly countenanced by the society.

---

74. *Id.* at 1058.

75. The prosecutors believing that the new law insulated Somm from liability and they themselves appealed the conviction. The court of appeal agreed and threw out the conviction. *Id.* at 1058.

76. *Id.* at 1059.

77. E.M.L.R. 542. (Q.B.) (1999).

78. The case subsequently settled: Demon agreed to pay Godfrey 15,000 pounds plus legal costs, which could exceed 200,0000 pounds. Demon's own legal costs were nearly 500,000, *supra* note 27 at 1059.

VII Monitory regime

On a general note one may infer that online intermediaries are relishing more immunities than facing liabilities. As noted above, as these fall into myriad roles throughout the "value chain"[79] and as crimes like pornography etc. affect the society at large, the regulation and monitoring of these actors becomes indispensable.

However, the monitoring and regulation becomes a complex task with the introduction of new technological changes. As different from the traditional telecommunication society which is a regulated one, the information society is fraught with technological revolutions as "the convergence of broadcasting, telecommunications and IT industries has allowed text, data, video audio and images to be reduced to a binary code before transmission to the end-user often rendering it impossible to know what type of content is being transmitted. This is the case with the internet where data is reduced to uniform packets transmitted using the TCP/IP protocol."[80] To bring them under the monitory framework, the UK and US have, however, responded differently. The starting approach of these countries has been to apply the telecommunications regulatory framework to the activities of ISPs and ASPs.[81] As technical and commercial convergence calls for unified regulatory framework for ISPs, the attempt has been to unify the hitherto distinct broadcast and communication monitoring systems before applying it to them. However, slight difference in the approach of these two internet giant countries of the US and UK is felt which is discussed below.

United States: In the US the approach of the Federal Communications Commission (FCC) has been to not to extend the 'common carrier' status to ISPs which 'has resulted in an effective three-way split in the regulation of ISP services in the United States.'[82] The first among these is telecommunications company ISPs which are treated as 'common carriers' under Title II of the Communications Act, 1934 and on whom there is obligation fixed , under sections 201-205 USC 'to offer services under tariff to all those who request it on rates, terms and conditions that are just, reasonable and nondiscriminatory.'[83] Falling under this category, the ISPs act as mere conduits and are not liable for the content. Secondly, there are cable company *ISPs* which

79. *Supra* note 26 at 401.
80. *Id.* at 402.
81. Internet Service Providers and Application Service Providers. *Id.* at 401.
82. Chris Reed (Ed.), *Computer Law* 343 (2003).
83. *Ibid.*

lack the status of 'common carriers'[84] and they are regulated both at the municipal and federal level. Lastly, there are access only ISPs which provide 'information service' or 'enhanced services' and are usually left unregulated. In sum, the regulation of online intermediaries is passing through a transformation where their status as 'common carriers' is controversial and still not clear as some of these are partaking both of mere carrier and actual supplier of contents over the internet. As for future 'the FCC appears unlikely to drop its policy of benign non-regulation of both the cable ISP and access-only ISP sectors, as it regards the exponential growth of the Internet in the last decade as having been significantly spurred by the overall lack of federal regulation.'[85]

United Kingdom: As the cable network industry barges into the traditional telecommunication and broadcasting industry, in the UK the early attempt has been to "…adapting the telecommunications regulatory framework to the activities of ISPs and ASPs."[86] That did not prove very successful as understandably, despite the communication commonness, the traditional broadcast industry and the present internet industry have more differences than similarities. In the UK, British telecommunications has been the giant in the field of telecommunication and broadcasting so far the regulation of activities etc. is concerned. Another authority, the Director General of Telecommunications, Office of Telecommunications or OFTEL implements its regulation policies through'licensing'of telecommunications. Under the Telecommunications Act, 1984 any person who 'runs' a telecommunications system[87] requires a license to do so. With the absence of the explanation of the term 'runs' , the extension of the license requirement in the internet arena raises complexities as there are a number of agencies in the 'value

84. Controversy surrounds this status as often the cable company operators offer basic telecommunications, Internet connectivity and TV/video, and due to technological convergence 'they are obliged to open their networks to potential ISP competitors' hence there is demand for giving them some form of 'common carrier' status. *Id.* at
343, 344.

85. *Id.* at 346.

86. *Supra* note 26 at 401.

87. A 'telecommunications system' is defined under s. 4(1) of the Telecommunications Act, 1984 as:

"... system for the conveyance, through the agency of electric, magnetic, electro-

(a) speech, music and other sounds;

(b) visual images;

(c) signals serving for the impartation (whether as between persons and persons, things and things or persons and things) of any matter otherwise than in the form of sounds or visual images ,or

(d) signals serving for the actuation or control of machinery or apparatus."

chain' and it becomes unclear as on which of these the license obligation falls. Transmission of illegal content over the system is considered as a breach of license thus bringing the internet content provider within its purview. The EU Directive (97/33) as implemented into UK law by statutory instrument[88] establishes "a regulatory framework for securing in the community, the interconnection of telecommunications networks and in particular the interoperability of services...."[89] The licensing rules in the UK recognize the distinction between *systems* and *services* on the one hand and distinction between *voice* and *data* on the other.

By virtue of the first category of distinction namely *systems* and *services* as given in the Telecommunications Act, 1984 the internet access providers which have management control of their own routing and/or switching are the ones who are considered persons who 'run' the system and hence fall under the licensing regime. By this analysis the content provider on the internet does not fall under the persons who 'run' the system and hence do not need a license; thus "a company which establishes a page on the world wide web will use a host to store the data which makes up the web page, but neither the host (unless it is also an access provider), nor the web site owner is necessarily involved in the routing and switching of messages and, therefore, requires no license under the Telecommunications Act."[90]

As regarding *voice* and *data* the EU rules differentiate between the two. Under the EU rules *voice* service providers are subject to individual licensing requirements while the *data* service providers are generally not under the obligation. As the UK rules provide for the licensing of 'systems' rather than 'services' it does away with the distinction between *voice* and *data* so long the person is 'running' the system and it needs a license whether the running is for *voice* or *data* service.

VIII Conclusion

Carte blanche insulation of online intermediaries from liability in the name of free flow of information is not feasible legally. Western countries have shown a comparatively liberal attitude in this respect as the aim of the directive has not been to establish liability but to limit the liability which arises out of national laws of member states.[91] China has shown stern attitude whereas they believe in encouraging people to use internet in an ethical way, enhancing the sense of moral of internet and stopping the flow of harmful information on the internet and have

88. S.I. 1997 No. 293.
89. *Supra* note 26 at 404.
90. *Id.* at 405.
91. Recital 50: The European Union E-commerce Directive, *supra* note 28.

decided to regulate ISPs by imposing on them obligation to monitor and control the content that passes through their system.[92] In contrast, section 15 of the directive reveals that no general obligation exists for ISPs to monitor information.[93] India's approach in this respect has been piecemeal and far from satisfactory. Though in UK there has been a proposed *possession offence*[94] regarding the obscenity content, that alone will not purge the entire net of the legally unwanted material and in that country too extra-legal approaches are being made to tackle the monstrous problem.[95] In the United States as ISPs are exempted under the Communications Decency Act companies are resorting to John Doe lawsuits[96] whenever they are the victims of defamatory material online and ISPs are given the responsibility to disclose the identity of the anonymous users in response to the subpoenas issued by the courts. The ISPs are, however, acting in a cooperative manner[97] in disclosing the identity of the anonymous defendant referred to as Doe. As defamation and obscenity take the highest toll of internet-related litigations and as such wrongs erode the social fabric of a society, in India, apart from a carefully crafted law provision, litigation in this field should be encouraged so that judicial interpretations enrich the virgin provisions in this most demanding field of law.

---

92. Chinese Measures on the Administration of Internet Information Services 2001; Chinese Interim Regulations on the Administration of Internet Publishing 2002. Internet Society of China *available at* www.dfn.org/voices/china/selfdiscipline.htm

93. But Recital 47 of the Directive says that it does not mean that the ISP cannot have general monitoring in a specific case, *supra* note 28.

94. *Supra* note 4.

95. A self-regulation model like the Internet Watch Foundation (IWF) operates a hotline to which individuals can report sites containing illegal content. Again British Telecom services such as BT Internet block access to sites listed by IWF as containing illegal content. (*Observer* 6 Jun 2004*)* and greater responsibilities are being imposed on the developers of software and technology.

96. A John Doe law suit is a tactic used by plaintiffs to identify an unknown person who allegedly committed some type of tortuous or illegal act online. For example, if a plaintiff learns of a defamatory posting on an internet site or of illegally downloaded music files, the plaintiff may be unable to identify the publisher
of the statement or the downloader of the files, for purposes of bringing a lawsuit. Thus, the plaintiff may bring a lawsuit against John Doe and use the lawsuit to issue a subpoena to the internet site in hopes of obtaining identifying information. Depending on the type of wrongful conduct, the subpoenaed party could include an independent internet service provider, a third party internet portal or an interactive computer service. F. Lawrence Street & Mark P Grant, *Law of the Internet* 3-87
(2004).

97. See, Robert Trignaux, "Indignant Business Attack the Privacy of