

2 CMET (2015) 52

Online Privacy v Piracy: Internet Service Providers Caught between the Devil and the Sea

by

Upkar Agrawal* & Anmol Jassal**

Abstract — The service of internet is sine qua non for exchange of data and information in the present era of Information Technology. It is wisely said that when we become habitual of a thing, it unknowingly becomes an addiction. Similarly, the utility of internet has risen to such levels that it has given birth to a plethora of legal problems, due to an ineluctable interface with the routine life of a modern human. Two of such challenges are Copyright Infringement and Online Privacy. In this backdrop, the role of an Internet Service Provider as a saviour in the protection of these rights is paramount, as they provide the infrastructural backbone for internet service, which basically involves transmission of packets of data over a digital network. However, the present set of legislations in India, comprising of the Information Technology Act, 2000 along with allied rules, amendments and the Copyright (Amendment) Act, 2012 create a slippery ground for ISPs whether to see or not to see into the private records of a user, which are otherwise protected under the Information Technology rules (hereinafter I.T. rules) as well as the Constitution of India, so as to ascertain the offence of copyright violation. The interface of Copyright laws and I.T. Laws has given rise to certain anomalies, which have been analyzed in this paper through a simultaneous perusal of the provisions of the Information Technology Act, 2000, the Copyright Act, 1957 and the Copyright Rules, 2013. The extant law dealing with online copyright infringement and privacy must be revised. There is a strong need to enact a consolidated legislation to cater to online piracy and right to privacy. In order to arrive at this conclusion, the authors have adopted the empirical research approach.



Keywords - Internet, Copyright, Privacy, Internet Service Provider, Intermediary.

INTRODUCTION

This paper specifically deals with two prominent aspects of internet use, namely piracy and privacy vis-à-vis the liability of an Internet Service Provider (hereinafter 'ISP'). At the outset, it is clarified that piracy would axiomatically mean copyright infringement while privacy would imply protection from encroachment on sensitive or personal data on the internet and disclosure of IP addresses.

The role of ISPs in protecting copyright and privacy on the internet is paramount. However, the present set of legislations and rulings by the courts have created an impasse for such organizations to choose between the competing rights of an internet user that are paripassu. The intermediary finds itself in a dilemma to block, intercept or examine the personal sensitive data and records, for which it has to take several

permissions from central agencies, or to expeditiously block the content which is infringing someone's copyright and provide the identity of the infringer to the copyright owner for judicial purposes. However, seeing the other side of the coin, it might lead to violation of Data Protection laws and Privacy of an individual if not pursued in accordance with the rules prescribed.

This paper highlights the discordance between the Copyright Rules, 2013 and Information Technology Act, 2000 (as amended in 2008) and allied rules which creates a situation for the ISPs in which they find themselves between the devil of preventing copyright infringement and sea in the form of privacy protection.

KEY DEFINITIONS

This section provides brief meaning and definitions of the key terms discussed in this paper.

PRIVACY ON THE INTERNET:

The right to privacy is known to have originated from an essay published in Harvard Law Review in 1890.¹ The Black's Law Dictionary² defines privacy as "right to be let alone; the right of a person to be free from unwarranted publicity; and the right to live without unwarranted interference by



Page: 54

the public in matters with which the public is not necessarily concerned".³ The right to privacy has been analyzed with respect to the rights inter se private parties and the constitutional right against the state.⁴

The scope of privacy for the current issue is associated with the sensitive personal data or information⁵ regarding the IP addresses and location stored or processed under lawful contract or otherwise with the intermediaries, which in the present case, would specifically mean the internet service providers. Now, this information regarding every single internet user needs to be protected by an internet service provider,⁶ the failure of which will amount to breach of privacy or confidentiality.⁷

ONLINE COPYRIGHT INFRINGEMENT:

The traditional meaning of copyright infringement is the 'violation of the right which is exclusively provided to a copyright owner or proprietor.' Three of the exclusive rights exercised by a copyright holder subject to section 52⁸ are:

- i. Right of communication to the public;
- ii. Right of reproduction of that particular copyrighted material; and
- iii. The storing of it in any medium by electronic means.

The dissemination of copyright works online potentially implicates both the right of communication to the public and the right of reproduction. It is not correct to say that any work published online carries with it implied consent that it can be modified, reproduced or circulated to others. Hosting service providers are instrumental in making webpages stored in servers available to the public. The transmission of work over the internet will normally result in several acts of reproduction. Furthermore, an access provider may choose to 'cache' the content retrieved from internet on his own installations, in order to speed up the retrieval by his customers. Therefore, there is a complex process of infringement which can take place in case of online copyright infringement. Consequently, the role of intermediary against such a menace is quintessential.

INTERNET SERVICE PROVIDER:

In the United States, the Digital Millennium Copyright Act, 1998 (hereinafter DMCA) ⁹ defines 'service provider' in a two-fold manner. Section 512(k)(1)(a) of the Act provides that ISP is an entity offering transmission, routing or providing of connections for digital online communications, between or among points specified by a user, of the material of user's choice, without modification to the content of material as sent or received. Also, Section of the Act 512(k)(1)(b) defines service provider as provider of online services or network access or the operator of facilities. Therefore, a broad and comprehensive definition of an ISP is given under DMCA which may also include universities and other institutions providing internet access to their students, professionals, researchers etc.

Under the English law, the definition of a 'service provider' is "any person providing an information society service".¹⁰ Further, information society service would mean 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service'.

Section 2(w) of the Information Technology Act, 2000 (as amended in 2008)¹¹ defines ISP as:

"'Intermediary' with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes."

Therefore, the entire information provided on the internet between a content creator and consumer is facilitated by an intermediary.

TAXONOMY OF PRIVACY

Internet is a huge platform which facilitates exchange of information which is stored, uploaded, downloaded, linked or distributed through electronic media such as computers, mobile phones etc. With this rampant

increase in the usage of internet services, its users may also post some personal information¹² online. This has resulted in several instances of loss of personal information such as koobface, a malicious program that stole personal information of Facebook users and sold it for wrongful gains.¹³ Also, the *Double Click case*¹⁴ and *Real Networks case*¹⁵, where the defendants, without authorization, not only collected plaintiffs' personal sensitive information, but also sold that information to third parties for gain.

Daniel J. Solove¹⁶ has devised certain parameters to check various kinds of 'harm' which encroachment of the right to online privacy can possibly cause. These harms have been categorized into four types, i.e. information collection, information processing, information dissemination and invasion.¹⁷ Therefore, there arose a need of strong pro-privacy laws in order to retain the sanctity of internet vis-à-vis the universal right of privacy¹⁸.

1. INTERNATIONAL REGIME:

Privacy protection has been a key issue for many international organizations, which deal in protecting the interests of online consumers. The Organization for Economic Cooperation and Development (hereinafter OECD) drafted the guidelines on 'Protection of Privacy and Trans Border Flow of Personal Data', commonly known as Privacy Guidelines, 1980.¹⁹ The APEC also framed a privacy policy in 1994, in order to promote appropriate privacy protection for personal information, particularly from the adverse effects of unauthorized intrusions and the abuse of personal information. APEC laid down nine core principles, inter alia, 'preventing harm', 'requirement of notice', 'collection limitation', 'uses of personal information', 'choice', 'integrity of personal information', 'security safeguards', 'access and correction' and 'accountability'.²⁰ APEC Privacy framework is a guiding ray for many countries which are in their nascent stages of formulating an effective regime for the protection of right to privacy.



Page: 57

In the United States, the Fourth Amendment lays down that the right to privacy must not be violated by conducting search and seizure unless there is a probable cause shown on oath, the place to be searched is described and the person or things that are to be seized are identified. The set of legislations namely, Electronic Communication Privacy Act²¹, Computer Fraud and Abuse Act, Video Privacy Protection Act, Sarbanes-Oxley Act, 2002, to state a few, has ushered a strong pro-privacy regime in the United States for protection of personal sensitive information of the netizens. Also, United States courts in *United States v. Barth*²² and *United States v. Reyes*²³, have held that every individual has the same expectation of privacy in any electronic data storage device as individual will have in a closed container.

In United Kingdom, Data Protection Act, 1998 was passed to govern the protection of personal data within the United Kingdom. According to this act, the personal data of consumers cannot be collected without express consent. Furthermore, the data collected with due authorization may only be used for authorized purposes only and cannot be disclosed to the third parties without express consent of the customer.

Similarly, the European Union passed the Data Protection Directive, 2002 aimed at protecting the consumers' privacy and providing laws in general to protect sensitive personal data in the cyberspace. Article 7 of this directive deals with the data protection, security providing for data security and retention principles to be followed by all internet service providers which provide internet services in EU countries. It requires that the retained data (for investigation purposes) will be maintained in same quality and is secured in the same manner as data on the internet network; also, adequate technical and organizational measure will be taken to prevent loss due to unlawful intrusion, unauthorized disclosure and accidents. Further, the retained data is supposed to be destroyed on expiry of the retention period.

It can be clearly inferred that the concept of privacy as a basic right is well recognized in the digital world. Taking a cue from various foreign jurisdictions, India has also codified the international principles on privacy in her municipal law in the form of Information Technology Act, 2000 (hereinafter I.T. Act) and the allied rules.

2. DIGITAL PRIVACY PROTECTION IN INDIA:

Right to Privacy in India is not codified as a right but is mainly a result of judicial activism and wisdom. It was interpreted to be a part of

Article 21, i.e. Right to Life and Personal Liberty, of the Constitution of India in *People's Union for Civil Liberties (PUCL) v. Union of India*²⁴. Online privacy in India is a relatively newer concept as compared to other international jurisdictions. Though, the Information Technology Act, 2000 was enacted earlier in the decade, the actual implementation of the Act was facilitated by the Information Technology (Amendment) Act, 2008 and the rules provided thereunder. Under this amended Act and Rules, there are elaborate provisions which make it mandatory for the intermediary to ensure the protection of personal data and respect the privacy of its users.

A. Information Technology Act, 2000 (hereinafter I.T. Act) (as amended by I.T. (Amendment) Act, 2008):

Under the I.T. Act, a body corporate possessing, dealing or handling any 'sensitive personal data or information in the digital form' will have to pay compensation on failure to protect such data.²⁵ Also, violation of privacy of a person with respect to transmission, capture or publication of private images and videos has been made punishable under the Act.²⁶ Intermediaries must preserve and retain information so collected as prescribed by the Central Government.²⁷ The Central Government has also been vested with exclusive power of interception/monitoring/decryption, blocking the public access²⁸ of the same or of any information through any computer resource under different circumstances²⁹ and for the purposes of maintaining cyber security³⁰. It appoints the National Nodal Agency for control and recording of such data in respect of Critical Information Infrastructure Protection (CERP).³¹ Penalty for the breach of confidentiality, privacy and disclosure of information in breach of lawful contract is punishable for intermediaries.³² Additionally, intermediaries are strictly liable, if they connive with a cyber offender to breach the right to privacy of a netizen.³³

B. Information Technology (Intermediaries guidelines) Rules, 2011:

Rule 3(1) r/w 3(2)(b) provides that it is compulsory for the intermediary to publish its 'privacy policy' before a user starts availing its services and if

any user fails to comply with this policy, he shall be debarred from accessing that content as per Rule 3(6). These rules are meant for the protection from copyright infringement as well as violation of privacy of the content provider.

C. Information Technology (Reasonable security practices and procedures and sensitive personal Data or Information) Rules, 2011:

These rules are meant for the protection against unlawful disclosure of IP addresses and personal information of the user who is availing the service of an intermediary. Under Rule 4, it is obligatory for the intermediaries to formulate a privacy pPolicy to be complied with by it. In case the intermediary wants to track the IP address of the user, it cannot do so without obtaining his consent, as per Rule 5(2).³⁴ But, in these cases too, the liberty to access such information is subject to two conditions imposed by Rules 5(4) and 5(7). Firstly, it is limited for the time period for which authorization in this regard is granted. Secondly, the user has the right to refuse his consent or he can also withdraw his consent at a later stage. But, one of the main fallouts of this condition is that if the central or state government authorizes such disclosure, then the consent of the user is immaterial. Also. Rule 6 and Rule 8 expressly prohibit

disclosure of the IP addresses to any third party, which is checked through a yearly audit.

D. Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009:

Any activity of the user of an internet service, whether of sending/receiving of mails, messages, chats or any other personal information comes within the meaning of internet traffic. Section 69B (3) and Rule 3 r/w Rule 4 seek to protect such traffic data from unlawful disclosure. Collection of such data is permissible only upon authorization of a nodal officer.

Under Rule 6 and Rule 7, it is the responsibility of the intermediary to abide by the rules and procedure pertaining to the maintenance of secrecy and confidentiality of data, which is subject to a bimonthly review. Such data cannot be stored for a period exceeding nine months as provided in Rule 8, except in certain cases, such as preventing intrusion or spreading of a computer contaminant and maintaining cyber security, as specified in Section 69B(1).



Page: 60

E. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009:

Rule 2(d) provides that any interception, monitoring or decryption of information can take place only after permission from Secretary in the Ministry of Home Affairs in case of *Central Government* and Secretary-in-charge of the Home Department in case of *State Government* or Union Territory. In cases of emergency situations and remote areas, Rule 3 authorizes the head of law enforcement agency in that area or Inspector General of Police or any other officer of an equivalent rank to control and monitor traffic. He has to decide on the issue of interception within 3 days and has to further get that direction affirmed by the competent authority within 7 days. If such authority does not grant the requisite affirmation, the previous direction becomes defunct. The regime of privacy protection in India goes to the extent of requiring the authorities to consider all alternative means of extracting information before giving any direction under Rule 8. Rule 20 and Rule 21 affix liability upon intermediary's for maintenance of confidentiality and secrecy of such records as obtained through interception, monitoring and decryption.

F. Internet Services License (ISP) Agreement:

There is a responsibility on an ISP to protect the privacy of communications transferred over its network. This includes securing the information and protecting it against unauthorized interception, unauthorized disclosure, ensuring the confidentiality of information, and protecting against over-disclosure of information, except when consent has been given.³⁵

In addition to the aforesaid rules, data protection and privacy is also regulated by the provisions of Penal Code, 1860, Indian Telegraph Act, 1885 (Rule 419A), Indian Contract Act, 1872, Specific Relief Act, 1963, Consumer Protection Act, 1986 and Information Companies (Regulation) Act, 2005.

Recently, in *Amar Singh v. Union of India*³⁶, the Apex Court held that on receiving a request for interception of someone's personal data or calls, the authenticity of such request must be verified along with proper authorizations before moving forward with such a request. The failure to comply with the same would lead to violation of privacy of an individual and liability for such an act shall fall upon the intermediary.



Conclusively, it can be inferred that India follows a strong online privacy regime, comprising of an all-round protection to privacy of its netizens in the form of various legislations and allied rules.

ONLINE PROTECTION TO COPYRIGHT

It is undeniable that one of the most valuable assets for any commercial enterprise or an individual is its intellectual property which requires a substantial investment of time, money and creativity. In the age of information technology, the protection of IPRs requires great attention and a dedicated policy structure. The need for protection of such rights has a twofold rationale - firstly, to provide an incentive to the creator or innovator and secondly, to provide encouragement to research and development by means of such incentives. This section highlights the international regime regarding copyright protection under the Copyright Act, 1957.

1. INTERNATIONAL SCENARIO:

Achieving homogeneity in the laws related to IPRs is a fairly challenging task because IPRs are territorial in nature and different countries adopt different standards on requirement of registration, protection of moral rights³⁷, term of protection and other allied issues. Therefore, due to this trans-national nature of IPRs in the digital world, it becomes necessary to have a uniform code for their protection.

A. World Intellectual Property Organisation (WIPO):

WIPO had been instrumental in harmonizing copyright issues across many countries. The WIPO Copyright Treaty, 1996³⁸ and the Performances and Phonograms Treaty, 1996³⁹ are two landmark agreements addressing IP issues especially with relation to copyright. WIPO Copyright Treaty, 1996 is a special agreement under Berne Convention, to which India is not a party. Its scope is limited to protection of original expressions and excludes business methods or mathematical algorithm/formulas. The WIPO Copyright Treaty, 1996 discusses the basic principles of Copyright Protection, i.e. right to distribution, communication to public, rental rights and other exclusive rights of the author. Nevertheless, these principles are mirrored in the Copyright Act, 1957 in India. The WIPO Performances and Phonograms Treaty, 1996 was entered into force on 20th May, 2002. It aims to protect IPRs of performers and producers of phonograms. Again, India is a non-



signatory to this treaty but, nevertheless, the provisions in the Copyright Act are in line with the basic tenets of this treaty.

However, the Act fails to address the nuances and suggest techno-legal measures to protect IPRs in the cyberspace. The non-ratification by most of the countries and absence of detailed provisions to deal with online copyright infringement mars its effectiveness.

B. World Trade Regime and TRIPS (Trade related aspects of Intellectual Property Rights):

The WTO has contributed to the protection of IPRs through the TRIPS agreement.⁴⁰ The prime objective of this treaty is to arrive at a homogeneous set of laws that

promote protection of intellectual property including copyrights. Since the passing of the TRIPS agreement, several countries amended their domestic laws or enacted new legislations to protect IPRs. India is a party to the TRIPS agreement and is under an obligation to implement its provisions under its domestic legislations.

TRIPS agreement, however, is not competent to combat online infringement of IPRs. Certain scholars have advocated that a combination of the TRIPS regime along-with WIPO could be made applicable to the cyberspace. The former could provide guidance on the issue of digital copyrights while the latter can be useful for its implementation.⁴¹

C. Online Copyright Protection - European Union (EU) measures:

*In EU, few directives have been passed in connection with protection of IP on the internet including the Directive 91/250/EEC on protecting computer programs as literary works, Directive 93/83/EEC for copyrights relating to satellite broadcasting and cable retransmission and Directive 2001/29/EC on copyright and related rights. The EU Copyright Directive in its Article 6 envisages the pronouncement of 'technological measures' and obligates the member states to implement measures in this regard.

D. United Kingdom Copyright Designs and Patents Act, 1988:

As per section 17 of the Act, 'copying' implies storing the work in any medium by electronic means. Also, Section 27 states that reprographic copying of a copyrighted material is its infringement. Therefore, the provisions



of Indian Copyright (Amendment) Act, 2012 (discussed later) mirror the provisions of this Act with respect to online copyright infringement.

E.U.S. Digital Millennium Copyright Act, 1998 (hereinafter DMCA):

The DMCA, published on 14th May, 1998 made the production and distribution of technology that provides a means to circumvent copyright protection mechanisms as unlawful. In cases where software is used to infringe the copyright, it is unlawful.⁴² It imposes both civil and criminal penalties for tampering with DRM systems making it a complex cyberspace law. Further, the act seeks to implement the treaties that were signed at the WIPO Geneva Conference, 1996. The DMCA, in very limited circumstances, allows the cracking of Copyright protection devises including for research in encryption technologies, assisting interoperability issue and enhancing computer security. Furthermore, it bans the manufacture, sale or distribution of devices which crack copies and passwords for illegally copying softwares.

It cannot be denied that a mechanism to prevent the online copyright infringement is there in existence, although not implemented. But, it is definitely recognized as an important issue internationally across different jurisdictions. However, the lack of uniformity across different jurisdictions is a major hindrance in achieving an environment in which copyright infringement on the internet enjoys protection.


2. ONLINE COPYRIGHT PROTECTION REGIME IN INDIA:

A detailed description of copyright protection on the internet under the Copyright Act, 1957 with subsequent amendments and rules r/w Information Technology Act, 2000 and its subsequent amendments and rules is provided as under:

A. Copyright Act, 1957 (as amended in 2012):

Section 14(a)(i), 14(c)(i)(A), 14(d)(i)(B), 14(e)(ii) recognizes the concept of storing of copyrighted work in any electronic means as an exclusive right of the copyright holder.⁴³ A Compulsory License is required for the purposes of selling,

publishing or communicating such copyrighted work.⁴⁴ In cases of infringement of such works, civil remedy of imprisonment for 6

 Page: 64

months to 3 years or fine to the tune of Rs. 50,000 - Rs. 3,00,000 or both is provided for along with compensation to the victim.⁴⁵

B. Copyright Amendment Rules, 2013:


In pursuance of the license mentioned above, the procedural terms and conditions for such license have been provided under Chapter V of the Rules. Also, the copyright holder must be informed via notice about the usage of his/her work and due reward in the form of the royalty has to be given to the author, artist or performer.⁴⁶

Chapter VII of the Copyright Amendment Rules, 2013 sanctions statutory license for cover versions of sound recording in respect of any literary, dramatic or musical work under sub-section (1) of section 31C.⁴⁷ Further, a notice of such intention to the owner of the copyright in such works and to the Registrar of Copyrights; at least fifteen days in advance of making the cover version must be given. In respect of the same, payment to the copyright holder in form of royalties for minimum fifty thousand copies and if the number is more than this, for all the copies of the cover version is to be made, at the rates determined by the Board.⁴⁸ Also, the cover version should not be communicated, sold or published in a manner which is deceptively similar to that of original version.⁴⁹

Provision for right to complaint by a copyright holder in case of storage of transient or incidental copies of works is a part of the rules. An expeditious action in respect of such complaint shall be taken (removal of such content within 36 hours).⁵⁰ Also, the importation of infringing copies must be under the directions and surveillance of Central Board of Excise and Customs.⁵¹

C. Information Technology Act, 2000 (as amended in 2008):

Section 43 r/w Section 65 & 66 provide for penalties and compensation for damage to computer, computer system, computer programs or data, etc. It necessarily protects the copyright with respect to computer softwares and information.⁵²

 Page: 65

The Central or State Government is empowered for interception, monitoring or decryption of any information through any computer resource for investigation of any offence which covers copyright infringement.⁵³ An intermediary is made liable for any offence if it colludes with the offender knowingly. Also, if it fails to exercise due diligence to prevent the commission of an offence, it can be held liable for that offence.⁵⁴ Section 81 provides an overriding effect to Copyright Act, 1957 over I.T. Act, 2000.⁵⁵

D. Information Technology (Intermediaries guidelines) Rules, 2011:

A duty is entrusted upon an intermediary under Rule 3(2)(d) not to host, display, upload, modify, publish, transmit or share any information that infringes any copyright. Also, under Rule 3(4), an expeditious (within 36 hours) removal of such content as mentioned above must be endeavoured. Intermediary is also supposed to make information relating to such offence available to the competent authority for the

purposes of investigation.

E. Information Technology (Reasonable security practices and procedures and sensitive personal Data or Information) Rules, 2011:

Rule 6 requires intermediaries to make available the personal sensitive information for the purposes of investigation on proper authorization by a competent authority.

F. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

Rule 3 provides for interception/monitoring/decryption of any information on authorization of competent authority⁵⁶ (mentioned above for these rules in Privacy section) for purposes of Section 69(2) of the I.T. Act, 2000.⁵⁷ Section 24 reasserts the necessity of interception/monitoring/decryption in case of fulfilment of intermediary's duty and services.

Therefore, a fence has been planted to protect the copyrighted work on internet in India.



Page: 66

INTERNET SERVICE PROVIDER'S LIABILITY IN INDIA - CAUGHT BETWEEN THE DEVIL AND THE SEA

The internet can potentially impose all three types of liability on an intermediary i.e., Direct and Indirect (which includes Vicarious and Contributory Liability).

Direct liability⁵⁸ would necessarily be incurred if Sec. 79(3)(a)⁵⁹ of I.T. Act is given effect to by an intermediary i.e., intentional collusion with the offender to commit an unlawful act. Vicarious liability, on other hand, arises when an intermediary possesses the right and ability to supervise the infringing conduct⁶⁰ and ignores its responsibility to prevent the unlawful act⁶¹. Both direct and vicarious liability regimes are examples of strict liability, which do not require that the alleged offender must have knowledge of the unlawful act.⁶² It has been stated that imposing strict liability on ISPs for third party copyright infringement would lead to ISPs gradually going out of business due to adverse judgement or policing costs necessary to keep infringing material off their systems⁶³, thereby posing a threat to affordable information access.⁶⁴

Contributory liability means that the Internet Service Provider "with knowledge of an unlawful act causes or materially contributes to the infringing conduct of another⁶⁵ i.e., substantial participation".⁶⁶ Therefore ISPs can be made liable for contributory infringement as knowledge is its essential element.⁶⁷ The element of knowledge may be satisfied in different ways i.e., specific notice of infringement⁶⁸, recent release or popularity



Page: 67

of the work copied⁶⁹, physical control over the copying process⁷⁰, ability to track the infringement⁷¹, advertisement and solicitation of infringement⁷² etc.

Therefore, the liability of an ISP can vary according to different cases and is a mix strict and indirect liability principle.

1. THE PRIVACY CASE:

As seen in the first section of the paper, the liability of an intermediary in

maintenance of privacy of an internet user is immense. In India, the liability of an intermediary has been codified in I.T. Act, 2000 and the allied rules. The importance of authorization for storing, hosting, decrypting, monitoring or intercepting any information regarding the internet is necessary and codified as a compulsory norm across all the statutes and rules.

Now, the problem to counter breach of privacy on the internet starts with the non-recognition of a possible infringement due to cookies and web bugs. Use of cookies which gets installed on the hard drive of a user is fairly common in behavioural advertising i.e., when a user visits a web page that it has already visited before, the cookies will point out the same. The website once revisited will capture the cookies data which is stored without the permission of the user and advertise its products or services according to the last visiting preferences.

Some cookies may even communicate sensitive personal data about a user to an advertising agency which might be shared through a network of such agencies. Also, certain social networking sites such as Facebook have been resorted to by such third parties to pass on sensitive personal information about its members without authorization of the users. Similarly, a web bug is in the form of a graphic that lies on a website or in the form of an 'enhanced' email message that makes it possible for a third party to check the person who reads a web page or an e-mail message. Also, the advent of proxy websites and URL(s) which alter the real location and language of a privacy infringer has posed great challenges to protect the right to privacy.

The liability of an ISP with respect to protection of the right to privacy is still not clear. Therefore, an Internet Service Provider can even be made liable for an act which it has neither committed nor could have possibly controlled.



2. THE COPYRIGHT INFRINGEMENT CASE:

Paterson J said, 'What is worth copying is prima facie worth protecting'.⁷³


The I.T. Act, 2000 addresses a few issues relating to protection of copyright in the internet as is discernible from sections 43 and 79; however, it has been done in a piecemeal fashion. One of the pitfalls of these provisions is their failure to address the issues relating to online copyright protection with proper clarity and detail.

There are two schools of thought as to whether an ISP should be made liable for the acts of Copyright Infringement by some third party on its network:

A. Arguments in favour of fixing the Liability of an ISP for Copyright Infringement by third parties:

- i. The real perpetrator behind copyright infringement is anonymous and very difficult to track down. ISP's, on the other hand, are easily identifiable, which are either located in same jurisdiction⁷⁴ or easily be tracked down⁷⁵.
- ii. The monetary argument which goes against the Intermediaries is that they are economically sound⁷⁶ to compensate the copyright holder.
- iii. ISPs are hailed as the controllers of internet services and thus have close access to the material being circulated on the internet⁷⁷. Also, they are capable of either block and remove or deny the access of such copyright protected work to the public.⁷⁸
- iv. Also, it is an easier way to enforce the laws of one's country on an ISP providing services in the domestic jurisdiction rather than some other jurisdiction where no

relief can be claimed.

 Page: 69


B. Arguments against the liability of an ISP for copyright infringement by a third party:

- i. ISP's often resort to immunity of being a passive common carrier⁷⁹ and a mere conduit of data transmission⁸⁰ with a little or no control over the data being transmitted over their network.
- ii. It is impossible for the ISPs to track all the content passing through their network systems given the huge tracts of data being exchanged. Therefore, an ISP is a mere facilitator of information exchange and not a content creator⁸¹.
- iii. If an ISP exercises due diligence and expeditiously removes an infringing content, it cannot be said to be liable, as already discussed.
- iv. If liability standards for ISPs are made strict, it would scuttle the growth of ISPs and there will be no incentive to provide internet services.⁸²

In India, according to the Section 52(1)(b) & (c) Copyright Act, 1957 (as amended in 2012) r/w the Rule 75, Copyright Rules, 2013, the ISPs are completely absolved from the liability of copyright infringement. The transient or incidental storage of work for purely technical transmission has been exempted from copyright infringement. It is similar to the Notice Takedown Mechanism as present U.S. DMCA, 1988. The rules regarding the take down mechanism have been provided for in the copyright rules. It provides two-fold protection to ISPs that firstly, they are passive intermediaries⁸³ and secondly, if an ISP removes the copyright infringing content, it won't be held liable.⁸⁴

3. ISP'S DILEMMA - TO SEE OR NOT TO SEE:

The cyber-criminals use internet as a weapon to intrude into the protected computers that store sensitive information regarding a country's national defense or to commit other cyber-crimes such as copyright infringement.⁸⁵ In order to prevent the commission of such crimes it is essential to impose certain reasonable restrictions on one's right to privacy.⁸⁶

 Page: 70

However, the Indian Parliament, to cope up with such challenges of the digital age, modified and amended the existing legislations by supplementing them with the necessary procedural guidelines. In pursuance of the same, I.T. (Amendment) Act, 2008; Copyright (Amendment) Act, 2012; Copyright Rules, 2013; Information Technology (Reasonable security practices and procedures and sensitive personal Data or Information) Rules, 2011; Information Technology (Intermediaries guidelines) Rules, 2011; Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009; Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 were enacted for ensuring protection of privacy and fight against online copyright infringement. Now, a simultaneous reading of the above rules, as presented in the earlier sections, is required to understand the discordance between these legislations in their quest to protect Copyright and Privacy.

Rule 75(2), Copyright Rules, 2013 provides for expeditious removal or denial of access of the copyright infringing content within 36 hours of the time of the receipt of the written complaint.

But, the rules for blocking of access of information from public are contained in Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. These rules are made under 69A (2)⁸⁷ of the I.T. Act, 2000 which provides for blocking of access of information to public in exclusive circumstances i.e., "in the interest of sovereignty and integrity of India, defense of India, and security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above". Therefore, this section has a narrower scope than Section 69 which includes the phrase "investigation of any offence".⁸⁸ The only set of rules which are applicable under Section 69(2) are Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, which do not provide for the removal or denial of access to any content. Also, these rules along with the other I.T. safeguard rules provide for number of permissions which need to be taken for undertaking any act such as Blocking, Interception, Monitoring and Decryption by an ISP, which further requires a minimum of 48 hours to be acted upon by the authorizing agencies.⁸⁹




Therefore, technically there are no rules as to authorization which needs to be obtained under Rule 75(2) except for Intermediary Guidelines rules which in themselves, provide for observation of other rules.⁹⁰ Now, if an ISP proceeds with the blocking, removal or denial of access within 36 hours, it would result in violation of 2009 Blocking Rules or Interception, Monitoring and Decryption rules and certainly would amount to breach of the right to privacy⁹¹ and would be liable under Sections 69, 69A and 69B of the I.T. Act.

On the other hand, if it attempts to obtain permission under these rules, the ISP will not be granted permission, as the ground for blocking or denial of public access does not cover Copyright Infringement. Also, if it goes for the permission under Interception, Monitoring and Decryption Rules, it won't be able to take the requisite permission within the stipulated time of 36 hours, as mandated by Rule 3 of the these rules. Moreover, the maximum period for which the permission can be granted is 180 days under Interception, Monitoring and Rules and the maximum period of content blocking under Blocking Rules is 21 days, as per Rule 8, which is an inadequate time period for investigation of any offence.

In certain cases, it could be possible for an intermediary to re-upload a non-infringing content after the expiration of the said period of twenty one days, as laid out under the recently amended Section 52, which offers protection from being liable for infringement on account of transient or incidental storage of a work or performance. Despite of the fact that the intermediary guidelines do not expressly provide for such an option, yet, a synchronized reading of the Copyright Act and intermediary guidelines may lead to such a possibility.⁹²

As a corollary to this, if an ISP does not block the copyright infringing content, it would be made liable under Section 79(2) r/w Section 79(3) of the I.T. Act, 2000 for not exercising due diligence by removal of Copyright Infringing content even after receiving of notice.

In addition to this, "The fact that both Sections 79 and 81 contain non-obstante clauses has made it extremely difficult to interpret the two Sections harmoniously, to pinpoint which Section supersedes the other, and to understand what the law on the subject is"⁹³ that whether the Copyright Act

 Page: 72

overrides the I.T. Act's Section 79 or not and it is due to this controversy over applicability of Section 79 to cases of copyright infringement, that there was a move to amend and introduce exceptions within the copyright law itself.⁹⁴


This controversy is best illustrated by the two cases filed by Super Cassettes ('SCIL') against Yahoo MySpace.⁹⁵ On 30 May 2008, the Delhi High Court issued a notice to Yahoo Inc. and its Indian subsidiary Yahoo Web Services (India) Pvt. Ltd upon a suit filed by SCIL, owner of the largest Indian music label 'T-Series' for infringement of their copyright caused by unlicensed streaming of SCIL's copyrighted works on Yahoo's portal video.yahoo.com.⁹⁶ In the MySpace decision, a single judge bench of Delhi High Court held that the ISPs, as a part of their due diligence, must make an effort to check infringement prior to the uploading of videos or other online content. This incontrovertibly implies that the intermediaries should screen all user generated content to check for copyright infringement before making the content available online.

In the recent case of *Bazee.com*, the company and its officials were made liable for non-removal of obscene content on the website only for a period of 2 days even without knowledge of the same.⁹⁷

Therefore, the anomalies between various provisions of Information Technology Act, 2000 and the Copyright Act, 1957 have left ISPs high and dry with the dilemma to see or not to see the records of a netizen and regulate or monitor them accordingly.

CONCLUSION

Article 19 of the Constitution of India, which provides for reasonable restrictions on the rights conferred by it, is a glaring example of how conflicts between competing rights have been resolved. Similar seems to be the case with privacy and piracy. On one hand, there are numerous cases⁹⁸ where the government authorities have misused their powers to infringe upon the privacy of a netizen. On the other hand, the Indian entertainment industry loses 80% of its revenue due to copyright violations.⁹⁹ However,

 Page: 73

the Parliament failed to show its vigilance when amending I.T. Act, Copyright Act and the rules with the intent to curb the menace of piracy along with due regard to the right to privacy of the internet users, which has been highlighted in the earlier sections. Also, the 'notice and takedown regime'¹⁰⁰ as envisaged under Rule 75 of the Copyright Rules, 2013 is not a full proof solution as it inherits the risk of 'wrongful takedown'. Also, the privacy and confidentiality clauses across various I.T. Rules are unclear and merely directory in nature without any proper benchmark with respect to standards of privacy to be maintained. Although, the responsibility to maintain the privacy and curb piracy lies both with the Government and an ISP but the I.T. Act only provides for the liability of an intermediary. However, there lies a ray of optimism for the ISPs if a comprehensive legislation is enacted shooting down all controversies and

confusions.

There is a need of internationalization of rights in a two-fold manner. Firstly, recognition of rights of copyright holders should take place at international level giving it a proper recognition under Private International Law. Secondly, the priority level of the competing rights of privacy and copyright must be strictly laid down in order to avoid multifarious decisions by the courts leading to an environment of uncertainty.

At the national level, a possible solution to the present problems is redesigning of legislations adopting a horizontal approach i.e., addressing the issues of online copyright violations with respect to the liability of ISPs in a single legislation so as to avoid confusion and disharmony.

It is needless to say that the internet has become a very indispensable part of our lives. Therefore, it has been rightly declared as a fundamental right in some countries.¹⁰¹ The growth of internet is largely dependent on the infrastructure provided by ISPs. Therefore, there is a need for incentivizing them instead of making them reel under the burden of expensive litigation and arresting the development of this prospective fundamental right i.e., internet.

* Rajiv Gandhi National University of Law, Punjab.

** Rajiv Gandhi National University of Law, Punjab.

¹ Warren and Brandeis, 'The Right to Privacy' [1890] 4 Harvard LR 193.

² Bryan A Garner, *Black's Law Dictionary* (6th edn., OUP) 19.

³ *ibid.*

⁴ *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632.

⁵ Reasonable Security (Practices and Procedures and Sensitive Personal Information) Rules, 2011, r 3.

⁶ Information Technology Act, 2000, s 2(w).

⁷ Information Technology Act, 2000, s 72 r/w Reasonable Security (Practices and Procedures and Sensitive Personal Information) Rules, 2011, r 6(3).

⁸ Copyright Act, 1957, s 51.

⁹ David Clark, *Design and Operation of the Internet*; (3.11, 1997) 16.

¹⁰ BG Joseph and DP Wasyluk, *Copyright Issues on the Internet and the DMCA*, Practising Law Institute-Patents, Copyrights, Trademarks and the Literary Property Course Handbook Series, 451, (2003) 451.

¹¹ The Information Technology (Amendment) Act, 2008.

¹² R. Rajagopal (n 165).

¹³ Fernando M Pinguelo and Mueller Bradford., 'Virtual Crimes, Real Damages: A Primer on cybercrimes in the United States and Efforts to Combat Cybercriminals' (2011) 16(1) *Virginia Journal of Law and Technology* 34.

¹⁴ *Double Click Inc Privacy Litigation, In re*, 641, US Dist LEXIS 27099 (2002).

¹⁵ *Olsen v. Real Networks*, C99-1817, WD Washington, (1999).

¹⁶ Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 *UPAL REV* 477, 482, 483.

¹⁷ Alexandra B Klass, 'Tort Experiments in the Laboratories of Democracy' (2009) 50 *WM & MARY L REV* 1501, 1526.

¹⁸ European Convention on Human Rights 1950, art 8; International Covenant on Civil and Political Rights 1966, art 17.

¹⁹ 'OECD Guidelines on the Protection of privacy and Trans Border Flow of Personal Data' (OECD)

<<http://www.oecd.org/document/18/03343en2649342551815186111100.html>> accessed 22 April 2015.

²⁰ APEC Privacy Principles (APEC) <www.austlii.edu.au/~graham/APEC/APECv10.doc> accessed 20 April 2015.

²¹ Electronic Communication Privacy Act, 18 U.S.C. pp. 2701-2712, <cpsr.org/issues/privacy/ecpa86/> accessed 15 April 2015.

²² 26 F Supp 2d 929, 936-37 (WD Tex 1998).

²³ 922 F Supp 818, 832-33 (SDNY 1996).

²⁴ *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.

²⁵ IT Act, 2000, s 43 A.

²⁶ IT Act, 2000, s 66 E.

²⁷ IT Act, 2000, s 67 C.

²⁸ IT Act, 2000, s 69 A.

²⁹ IT Act, 2000, s 69.

³⁰ IT Act, 2000, s 69 B.

³¹ IT Act, 2000, ss 70 & 70 B.

³² IT Act, 2000, s 72 & 72 A.

³³ IT Act, 2000, s 79(3).

³⁴ Information Technology (Reasonable security practices and procedures and sensitive personal Data or Information) Rules, 2011, r 5(2).

³⁵ Internet Services License (ISP) Agreement, Cls. 32.1, 32.2(i), (ii), r/w Cl. 32.3

³⁶ *Amar Singh v. Union of India*, (2011) 7 SCC 69.

³⁷ Indian Copyright Act, 1957, s 57.

³⁸ 'The WIPO Copyright Treaty 1996' (WIPO) <http://www.wipo.int/treaties/en/text.jsp?file_id=295166> accessed 25 April 2015.

³⁹ 'Performances and Phonograms Treaty' 1996 (WIPO) <<http://www.wipo.int/treaties/en/ip/wppt>> accessed 25 April 2015.

⁴⁰ 'TRIPS Agreement 1994' (WTO) <<https://www.wto.org/english/tratope/tripse/wtowipe.html>> accessed 25 April 2015.

⁴¹ Susan A. Mort, 'The WTO, WIPO & the Internet: Confounding the Borders of Copyright and Neighbouring Rights' (1997) 8 Media & Entertainment Law Journal 173.

⁴² *Universal City Studios Inc. v. Reimerdes*, 111 F Supp 2d 294 (SDNY 2000).

⁴³ Copyright Act, 1957 (year), ss 14(a)(i), 14(c)(i) (A), 14(d)(i) (B), 14(e)(ii).

⁴⁴ Copyright Act, 1957 year, ss 31A, 31C & 31D.

⁴⁵ Copyright Act, 1957 year, s 55.

⁴⁶ Copyright Amendment Rules, 2013, Ch.-V.

⁴⁷ Copyright Act, 1957 year, s 31 C.

⁴⁸ Copyright Amendment Rules, 2013, r 27.

⁴⁹ Copyright Amendment Rules, 2013, r 24.

⁵⁰ Copyright Amendment Rules, 2013, r 75.

⁵¹ Copyright Amendment Rules, 2013, r 79.

- ⁵² IT Act, 2000, ss 43, 65, 66.
- ⁵³ IT Act, 2000, s 69.
- ⁵⁴ IT Act, 2000, s 79(3).
- ⁵⁵ IT Act, 2000, s 81.
- ⁵⁶ Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r 3.
- ⁵⁷ IT Act, 2000, s 69(2).
- ⁵⁸ Mark F. Radcliffe, 'Drafting and Negotiating Internet License Agreements' [2003] 754 Prac. L. Inst/Pat 1035, 1063.
- ⁵⁹ IT Act, 2000, s 79(3)(a).
- ⁶⁰ *Shapiro, Bernstein & Co. v. HL Green Co.*, 316 F 2d 304, 307 (2nd Cir 1963).
- ⁶¹ IT Act, 2000, s 79(3)(b).
- ⁶² Irina Y. Dmitrieva, 'I Know It When I See It: Should Internet Service Providers Recognise Copyright Violation When They See It?' 16 Santa Clara Computer & High Tech LJ (2001) 233, 235.
- ⁶³ Justin Hughes, 'The Internet and the Persistence of Law' (2003) 44 B.C.L. Rev. 359, 383-386.
- ⁶⁴ Timothy L. Skelton, 'Internet Copyright Infringement and Service Providers: The Case for a Negotiated Rulemaking Alternative' (1998) 35 San Diego L. Rev 219, 303.
- ⁶⁵ Melville B. Nimmer and David Nimmer, Nimmer On Copyright (2002) Sec. 12.04[A][2]; *Gershwin Publishing Corp. v. Columbia Artists Management Inc*, 443 F 2d 1159, 1162 (2nd Cir 1971).
- ⁶⁶ *Fonovisa Inc v. Cherry Auction Inc*, 847 F Supp 1492, 1496 (ED Cal 1994).
- ⁶⁷ *Sega Enterprises Ltd. v. MAPHIA*, 857 F Supp 679, 686 (ND Cal 1994),; *Religious Technology Center v. Netcom On-Line Communication Services Inc*, 907 F Supp 1361, 1375 (ND Cal 1995),; *Playboy Enterprises Inc v. Russ Hardenburgh Inc*, 982 F Supp 503, 514 (ND Ohio 1997).
- ⁶⁸ Angela R. Dean, 'Expanding the Doctrines of Vicarious and Contributory Copyright Infringement' (1997) 4 Vill. Sports and ENT LJ 119, 144, 145.
- ⁶⁹ *Universal City Studios Inc v. American Invsco Management Inc*, (1981) 217 USPQ 1076, 1077.
- ⁷⁰ *RCA Records v. All-Fast Systems Inc*, 594 F Supp 335, 339 (SDNY 1984).
- ⁷¹ *Sega Enterprises Ltd. v. MAPHIA*, 948 F Supp 923, 931-, 32 (ND Cal 1996).
- ⁷² *Columbia Pictures Industries Inc v. Aveco Inc*, 800 F 2d 59, 62 (3rd Cir 1986),; *Wales Industries Inc v. Hasbro Bradley Inc*, 612 F Supp 510, 518 (SDNY 1985).
- ⁷³ *University of London Press Ltd. v. University Tutorial Press Ltd.*, (1916) 2 Ch 601.
- ⁷⁴ V.K. Unni, "Internet service provider's liability for copyright infringement - How to clear the misty Indian perspective" (2001) 8 Rich. J. of Law and Tech, <<http://www.richmond.edu/jolt/v8i/art.html>> accessed 25 April 2015.
- ⁷⁵ Rowland Diane and Macdonald Elizabeth, *Information Technology Law*, (3rd edn, Cavendish Publishing, Great Britain 2005) 494,-, 498.
- ⁷⁶ Osborne D, 'Copyright And Trademark Infringement On The Net-Looking to the Internet Service Provider First', <<http://www.iprights.com/cms/templates/arts.aspx?artid=146&zonecid=2>> accessed 28 April 2015.
- ⁷⁷ Ryder Rodney D, Guide to Cyber Laws: Information Technology Act, 2002, *E-Commerce, Data Protection & the Internet*, (1st edn, Wadhwa Nagpur Law and Practice 2001) 551-562.
- ⁷⁸ Sieber U, 'Criminal Liability for the Transfer of Data in International Networks-New Challenges for the Internet', (Computer Law and Security Report).
- ⁷⁹ Sagar Jagdish, Thomas Zakir and Mittal Raman, 'Study Material on "Copyright and Internet (Paper-III)", Indian Law Institute (2007), 1,-42.

- ⁸⁰ *Sony v. Universal Studios*, 907 F Supp 1361, 1367 (ND Cal 1995).
- ⁸¹ *Religious Technology Center v. Netcom On-Line Communication Services Inc*, 907 F Supp 1361 (ND Cal 1995).
- ⁸² Mukherjee S, 'Liability of Internet service providers for copyright Infringement on the Internet: US vis-a-vis Indian position', <<http://www.legalservicesindia.com/arts/>> accessed 24 April 2015.
- ⁸³ IT Act, 2000, s 79(1).
- ⁸⁴ IT Act, 2000, s 79(2).
- ⁸⁵ Information Technology (Intermediaries Guidelines) Rules, 2011, r 2(d).
- ⁸⁶ The Constitution of India, art 19(1)(g).
- ⁸⁷ Information Technology (Procedure And Safeguards For Blocking For Access Of Information By Public) Rules, 2009, r 3; Information Technology Act, 2000, s 69A (2).
- ⁸⁸ Information Technology Act, 2000, s 69(2).
- ⁸⁹ Information Technology (Procedure And Safeguards For Blocking For Access Of Information By Public) Rules, 2009, r8; Information Technology (Procedure And Safeguards For Interception, Monitoring And Decryption Of Information) Rules, 2009 r 3.
- ⁹⁰ Information Technology (Intermediaries Guidelines) Rules, 2011, rr 6, 8.
- ⁹¹ *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
- ⁹² Singh S & Singh V, 'Internet Service Provider Liability for Copyright Infringement', (2010) 3 (10) Indian Legal Impetus <<http://SinghassociatesIn/Intello-Property/2.Html>> accessed 26 April 2015.
- ⁹³ Saikia N, 'ISP Liability and the Parliamentary Standing Committee's Recommendations', (2010) <<http://Copyright.LawmattersIn/2010/11/Isp-Liability-Andparliamentary.Html>> accessed 26 April 2015.
- ⁹⁴ *ibid.*
- ⁹⁵ *Super Cassettes Industries Ltd. v. Yahoo Inc*, CS (OS) No. 1124 of 2008 (Del), Order for Ad Interim Injunction, 30-5-2008, Case Status: Pending, <http://Delhihighcourt.Nic.In/Dhc_Case_Status_Oj_List.Asp?Pno=138814> accessed 25 April 2015.
- ⁹⁶ *Super Cassettes Industries Ltd. v. MySpace Inc*, 2011 SCC OnLine Del 3131.
- ⁹⁷ *Avnish Bajaj v. State (NCT of Delhi)*, 2004 SCC OnLine Del 1160 : (2005) 3 Comp LJ 364 (Del).
- ⁹⁸ Prashant Iyengar, 'Online Privacy: IP Addresses and Expedious Disclosure of Identity in India' [2011], <<http://ssrn.com/abstract=1875659>> accessed 25 April 2015.
- ⁹⁹ Brandon Hammer, 'Smooth Sailing: Why the Indian Film Industry Remains Extremely Successful in the Face of Massive Piracy', *Journal of Sports & Entertainment Law*, Harvard Law School., Vol 5, (2014).
- ¹⁰⁰ Digital Millennium Copyright Act, 1998, s 512.
- ¹⁰¹ 'United Nations Declares Internet Access a Basic Human Right', (June 3, 2011) *The Atlantic*, <<http://www.theatlantic.com/technology/archive/2011/06/united-nations-declares-internet-access-a-basic-human-right/239911/>> accessed 25 April 2015.

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.