

International Journal of Law and Legal Jurisprudence Studies:
ISSN: 2348-8212 Volume 2 Issue 4

**COPYRIGHT ISSUES IN NET NEUTRALITY DEBATE:
A NORMATIVE ANALYSIS**

Author:

Devdatta Mukherjee

Research Scholar (currently pursuing M.Phil. in International Legal Studies), Centre for International Legal Studies, School of International Studies, Jawaharlal Nehru University, New Delhi.

Email id: dvdttmukherjee@gmail.com

Abstract

The debate on network neutrality has raged fervently in recent times. Although verbose arguments have been placed against and in favour thereof, the intertwined issue of online copyright infringement hasn't quite received the deserved attention. Therefore, the paper proposes to focus on the ability of the ISPs to take reasonable actions to prevent the unlawful distribution of copyrighted works over internet. However, such affirmative efforts to protect creators' IP rights might condition, limit or eliminate consumers' fair use opportunities and also their privacy expectations. Abiding by a doctrinal methodology, this paper furnishes a backdrop by elucidating the internet architecture, conceptual contours of net neutrality and aspects and prospects of copyright filtering. Since the inception of the internet occurred much later the promulgation and development of the copyright laws, it has been safely observed that the internet, vis-a-vis the access to contents, could never be, and has never been neutral. The conceptual paradigm of a neutral net must take note of the fact that safeguarding the rights of the copyright owners is paramount as well, and towards this end allow intervention of the ISPs to a certain extent, besides inspiring exploration of new, innovative business models by the content industry. (199 words)

Keywords: Copyright Infringement, Data Packet Sniffing, Intellectual Property Rights, Internet Service Provider, Net Neutrality, Normative Analysis.

Introduction

Hailed almost unanimously as the most significant development on the Internet, the World Wide Web, a user-friendly graphic user interface (“GUI”), was developed to perpetuate a neutral network built on end-to-end principles. Being neutral and therefore primarily uncontrolled platforms, the Internet generally and the Web specifically have spawned a dazzling rate and range of innovation.¹ It has been interesting to note how in quick succession the Internet has evolved from a collaborative project among governments and universities to a commercial medium operated primarily by private ventures.²

The popular metaphor of the Internet as a public sphere, however, has undergone structural transformations. Whilst discussing the structural transformations of the public sphere, Jürgen Habermas clarified that while the market helped create the initial space for civic engagement, it also constantly threatened to colonize public spheres through privatization.³ He referred to this phenomenon as the “re-feudalization of the public sphere,” a process in which the newly created public space would succumb to commercial pressures and reorganize along familiar power hierarchies.⁴ The Internet’s developing third generation⁵ appears poised to exploit technological innovations, expanding broadband access and converging markets with even greater service diversity and market segmentation. This next generation World Wide Web will not appear as a standard, “one size fits all” medium because a class of consumers will expect more and different features, and the content providers would be ready to pay different rates. Undeniably, “network neutrality” does represent the preferable Utopia. Although imagination of a world with two Internets- the first a quick, smooth highway for those who pay more, and the other a slow, bumpy trail for everybody else-⁶ is not yet an absolute reality, the Internet Service

¹ Bill D. Herman (2006), “Opening Bottlenecks: On Behalf of Mandated Network Neutrality”, *Fed. Comm. L.J.*, 59:103, 109-10.

² Rob Frieden (2002), “Revenge of the Bellheads: How the Netheads Lost Control of the Internet”, *Telecomm. Pol’y*, 26: 425, 425- 44.

³ Jürgen Habermas (1989), *The Structural Transformation of the Public Sphere*, (Trans. T. Burger) (MIT Press).

⁴ *Ibid.*

⁵ The Internet’s first generation emphasized network expansion and efforts to promote connectivity with little regard for cost, because a third party (government) subsidized such efforts. The second generation marked a migration from government subsidization to private, commercial network operation. The ongoing migration to a third generation appears to emphasize diversification of services, prices and quality as ISPs pursue price and QOS discrimination opportunities; International Telecommunication Union (March 23-24, 2006), “What Rules for IP-enabled NGN?”, Workshop, [Online: web] Accessed 25 April, 2015, URL: <http://www.itu.int/osg/spu/ngn/event-march-2006.phtml>.

⁶ Muhammad Zulqarnain Zulfi (February 10, 2014), “Net Neutrality: Here is Everything You Need to Know about it”, [Online: web] Accessed 25 April, 2015, URL: <http://indianexpress.com/article/technology/technology-others/net-neutrality/>.

Providers reluctance to stay neutral anymore by noting that providing internet service is essentially a free-enterprise issue is gaining prominence irrespective of the national borders. Re-feudalization of the public sphere of internet is on the rise. Amidst such re-feudalized internet space, the options to prevent, or at least minimize online copyright infringement iss sought to be explored in this paper.

The Focus and the Limitations

Venturing into the net-neutrality debate is not the purpose of this paper. In the wake of the twenty-first century, the Internet Ecosystem has come to include a diverse array of stakeholders who build and depend upon each other's participation.⁷ Taking note of particularly three stakeholders- the provider of a copyrighted content/ copyright creator, the Internet Service Provider (ISP) and the consumer, this paper aspires to delve into the changing role of the ISPs from neutral conduits to active participants in traffic management activities. The focus of the paper shall be the ability of the ISPs to take reasonable actions to prevent the unlawful distribution of copyrighted works over the internet: their capability to "sniff" the packet contents incurring actual or constructive knowledge of what a packet represents; their non-qualification for a status that exempts them from liability for carrying harmful or tortious content, in light of the perceived or actual burden content scrutiny would impose; and their responsibility to examine the content they carry and to provide reasonable safeguards for protecting copyrights, including the possible retention and disclosure of logs that can help identify and punish copyright infringement and other unlawful activities. However, such affirmative efforts to protect creators' intellectual property rights might condition, limit or eliminate consumers' fair use opportunities and also their privacy expectations.

In order to peruse the normative framework of the copyright issues culled out in the context of net neutrality debate, the paper furnishes a backdrop by elucidating the internet architecture, the concept of net neutrality and the aspects and prospects of copyright filtering. Reference has been made to US Copyright Law when ardently necessary to analyse the norms and streamline the debate, and a suggestion incorporated for the Indian legal system, in this otherwise purely normative analysis.

⁷ Sascha D. Meinrath *et.al.* (2011), "Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide", *CommLaw Conspectus*, 19:423.

Deciphering the Internet Architecture

The Internet has been defined to be a network of networks, including public, private, and governmental networks, that have been linked together and that exchange traffic on the basis of a standardized set of protocols.⁸ While there are a variety of protocols that may be used depending on the type of application involved, they generally require that data be broken up into discrete units, or “packets,” that are then passed across the Internet from source to destination.⁹ This attribute has earned the Internet the characteristic of being a ‘packet-switched’ network, wherein fixed circuits are not dedicated for the duration of a communication. Instead, the data that is transmitted, whether files, email, Instant Messages, voice, is broken into small packets. Each packet travels its own route over the Internet. The entire set of contents is reassembled when it is received at the other end.¹⁰

The creators of the internet connected different smaller networks together, they taught all those networks to speak a single common language (the Internet Protocol language), they integrated all those lesser networks into a global whole.¹¹ This decentralized whole is what we call the Internet ‘cloud’, which symbolizes the unpredictability of the path that communications will take from one point to another.¹² To borrow from Jonathan Zittrain, it may be represented in the following form:¹³

⁸ Howard Walthall (2010), “The Net Neutrality Debate: An IP Perspective”, *Landslide*, American Bar Association, 3(1).

⁹ *Ibid.*

¹⁰ Susan Landau (2006), “National Security on the Line”, *J. Telecomm. & High Tech. L.* 4: 409, 424.

¹¹ J. Zittrain (2003), “Be Careful What You Ask For: Reconciling a Global Internet and Local Law”, in A. Thierer and C.W. Crews (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Internet Governance and Jurisdiction. Washington, DC: Cato Institute) 13.

¹² Thomas Schultz (2008), “Curving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface”, *EJIL*, 19 (4): 799-839.

¹³ J. Zittrain (2003), “Internet Points of Control”, *Boston College L Rev*, 44: 653, 656.

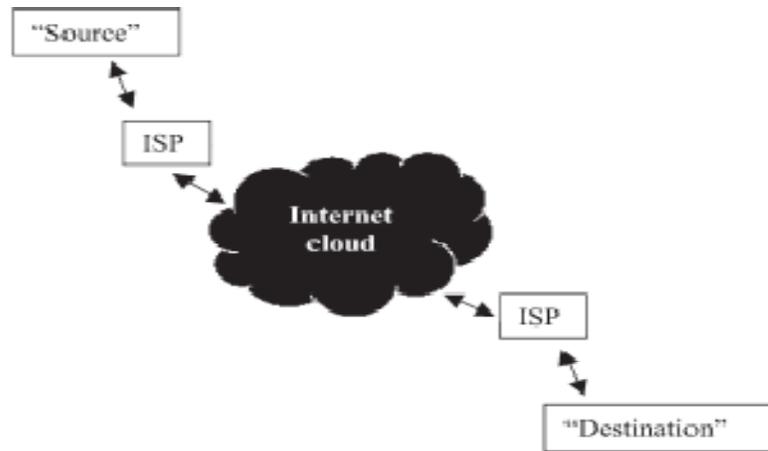


Figure 1: Internet Points of Control as proposed by J. Zittrain

The internet has been connoted to be a suggested architecture for communications networks by its inventors V Cerf and R Kahn when they note:

In essence, the Internet is architecture, although many people confuse that with its implementation. When the Internet is looked at as architecture, it manifests two different abstractions. One abstraction deals with communications connectivity, packet delivery and a variety of End-to-End communication services. The other abstraction deals with the Internet as an information system, independent of its underlying communications infrastructure, which allows creation, storage and access to a wide range of information resources, including digital objects and related services at various levels of abstraction built on architectural principles and follows a layered design.¹⁴

The first of the two abstractions, the End-to-End principle, suggests the following basic design: keeping the network simple while placing its intelligence at its ends.¹⁵ The network should only be endowed with transmitting efficiently data-grams; ‘everything else should be done at the fringes.’ As a result, End-to-End renders the network flexibility and the ability to work with all sorts of data or as Lessig eloquently puts it ‘End-to-End codes a kind of

¹⁴ V. Cerf and R. Kahn (2004), “What Is the Internet (and What Makes It Work)” in M Cooper (ed.), *Open Architecture as Communications Policy: Preserving Internet Freedom in the Broadband Era* (Centre for Internet and Society, Stanford Law School), [Online: web] Accessed 25 April, 2015, URL: https://www.cnri.reston.va.us/what_is_internet.html#xv.

¹⁵ Lawrence Lessig (2002), “The Architecture of Innovation”, *Duke L J*, 51: 1789.

neutrality' to the network.¹⁶ This way, the internet maintains a flexibility in its design as all users can contribute to its architecture. Platform configuration depends on the user's ability to create and implement additional software; control over its architecture 'becomes separable from network ownership' granting end users 'non-discriminatory ability to design the architecture of a communication platform' besides those who own and control its infrastructure.¹⁷

In sync with the second abstraction, internet has been defined as a global information system, and included in the definition, is not only the underlying communications technology, but also higher-level protocols and end-user applications, the associated data structures and the means by which the information may be processed, manifested, or otherwise used.¹⁸ In many ways, this definition supports the characterization of the Internet as an "information superhighway."¹⁹

In contrast to the internet, telecommunications is defined as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."²⁰ Nevertheless, the World Wide Web has succeeded in seamlessly blending the telecommunications links needed to transmit information bits and packets with the content carried over these links.

Delving into the Concept of Net Neutrality

Although the term 'net neutrality' was coined by Columbia law professor Tim Wu, the antiquity of the concept could be traced to the 1800s when Almon Brown Strowger invented an automatic telephone exchange to bypass operators who redirected calls for profit. In general parlance, net neutrality refers to the concept that network operators should not be permitted to

¹⁶ Lawrence Lessig (2000), "Symposium: Cyberspace and Privacy: A New Legal Paradigm?", *Stanford Law Rev*, 52: 991.

¹⁷ Bar and G Sandvig (2000), "Rules From Truth: Post Convergence Policy for Access" (Paper presented at the 28th Telecommunications Policy Research Conference (TPRC) on Communication, Information and Internet Policy, Alexandria, Virginia, USA) 22.

¹⁸ Definition of "Internet", October 24, 1995, Resolution of the U.S. Federal Networking Council, [Online: web] Accessed 25 April, 2015, URL: https://www.cnri.reston.va.us/what_is_internet.html#xv.

¹⁹ *Supra* note 14.

²⁰ It would be pertinent to note that the cable broadband providers do not provide a "telecommunications service" under the relevant legislation and are therefore exempt from mandatory common-carrier regulation; *Nat'l Cable Tel. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967 (2005).

treat different portions of the Internet traffic flowing across their network differently, or, in the words of net neutrality proponents, network operators should be prohibited from “discriminating” against particular types of traffic. The Internet Service Providers (ISPs), providing the so-called “last mile of connection between” their customers and the larger Internet, often for a monthly fee, tend to become the focus of the neutrality proponents. Nevertheless, there are other players in the game. Involved herein are the content creators/owners, the content consumers/users, and companies providing applications and services over the internet.

Net neutrality proposals tend to share a set of common, albeit somewhat ambiguous, themes.²¹ The *raison d'être* for this movement generally rests on the notion of preserving the “openness” and “end-to-end” design of the Internet or the networks over which the Internet runs. Proponents of a Net neutrality rule fear that increased vertical integration by ISPs- that is, the integration of conduit and content within a broadband environment- will greatly diminish the overall neutrality of the Internet as a platform for innovation and communication. The theory is that, as carriers pursue greater service or product integration, they will have the incentive to discriminate against or control other types of applications or activities at the edge of the network. However, in the interest of protecting copyright issues, as elucidated hereafter, the ISPs ought not to be merely neutral conduits, but need to look into the content as well. This has again led to privacy concerns and deemed to constitute a burden on free expression.

It has been noted that “...absent evidence of harm to the local network or the interests of other users, broadband carriers should not discriminate in how they treat traffic on their broadband network on the basis of internet work criteria.”²² Although the newness of the Net neutrality concept “means much unavoidable vagueness as to its operation,” the regulators will be able to enforce the rule by examining the positive versus negative externalities associated with carrier restrictions.²³ The carriers should be left free to impose restrictions on network use if those restrictions generate positive externalities. However, defining positive and negative externalities is open to their own set of disputes, as is the debate over necessity of copyrights. Nevertheless, bearing in mind that the concept of Copyright has been a bargain: society would grant creators a time-limited ability to control and profit from their works before they fall into

²¹ Adam D. Thierer (Jan. 12, 2004), “‘Net Neutrality’ Digital Discrimination or Regulatory Gamesmanship in Cyberspace”, *Policy Analysis*, no. 507, [Online: web] Accessed 25 April, 2015, URL: <http://www.cato.org/pubs/pas/pa507.pdf>.

²² Tim Wu (2003), “Network Neutrality and Broadband Discrimination,” *Journal of Telecommunications & High Technology*, 26, [Online: web] Accessed 25 April, 2015, URL: <http://faculty.virginia.edu/timwu/bbd.pdf>.

²³ *Ibid.*

the public domain, thereby granting the work its libertarian worth as well as incentivizing the utilitarian progress in collective human knowledge, it won't be inappropriate to argue that taking reasonable steps to protect copyright infringement over the internet necessarily has positive externalities associated with it.

Copyright Filtering in Pursuit of Reasonable Network Management

Analysing from the users' perspective, the basic tenets of internet freedom²⁴ entitles and enables the consumers to access the lawful Internet content of their choice; run applications and services of their choice, subject to the needs of law enforcement; connect their choice of legal devices that do not harm the network; and choose their network providers, application and service providers, and content providers of choice.²⁵ Additional to the afore-enumerated freedoms are the principles of non-discrimination and transparency.²⁶ Blocking, throttling and paid prioritization- which refer to outright blocking of content, slowing of transmissions, and the creation of so-called "fast lanes"- encompass most of the practices that net neutrality rules have been intended to eliminate.²⁷ Subject to reasonable network management, a provider of broadband Internet access service must treat lawful content, applications, and services in a non-discriminatory manner.²⁸ This concept of reasonable network management ought to consist of the reasonable practices employed by a provider of Internet access service to reduce or mitigate

²⁴ FCC Internet Policy Statement, FCC 05-151 (adopted Aug. 5, 2005).

²⁵ Although in the case of *Comcast Corp. v. FCC*, 600 F.3d 642, the United States Court of Appeals for the District of Columbia case held that the Federal Communications Commission (FCC) does not have ancillary jurisdiction over Comcast's Internet service under the language of the Communications Act of 1934, thereby vacating a 2008 order issued by the FCC that asserted jurisdiction over Comcast's network management policies and censured Comcast from interfering with its subscribers' use of peer-to-peer software, the Court neither undermined the 'importance of preserving a free and open Internet; nor did it close the door to other methods for achieving this important end'; "FCC Statement on *Comcast v. FCC* Decision", Apr 6, 2010, [Online: web] Accessed 25 April, 2015, URL: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297355A1.pdf.

²⁶ However, on January 14, 2014 in *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014), the United States Court of Appeals for the District of Columbia Circuit vacated the "No blocking" and "No unreasonable discrimination" rules of the FCC Open Internet Order, 2010, and upheld the "Transparency" rule in the same ruling. This ruling has been criticized as the death of network neutrality in the United States; Edward Wyatt, "Rebuffing F.C.C. in 'Net Neutrality' Case, Court Allows Streaming Deals", *New York Times*, [Online: web] Accessed 25 April, 2015, URL: <http://www.nytimes.com/2014/01/15/technology/appeals-court-rejects-fcc-rules-on-internet-service-providers.html> 15.01.2014.

²⁷ The Open Internet Order, FCC, paragraph 14, [Online: web] Accessed 25 April, 2015, URL: <https://www.federalregister.gov/articles/2015/04/13/2015-07841/protecting-and-promoting-the-open-internet>; Jeff Sommer (March 12, 2015), "What the Net Neutrality Rules Say", [Online: web] Accessed 25 April, 2015, URL: http://www.nytimes.com/interactive/2015/03/12/technology/net-neutrality-rules-explained.html?_r=0.

²⁸ Notice of Proposed Rulemaking, *In re* Preserving the Open Internet, GN Docket No. 09-191, WC Docket No. 07-52 (adopted Oct. 22, 2009), [Online: web] Accessed 25 April, 2015, URL: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf.

the effects of congestion on its network or to address quality-of-service concerns; to address traffic that is unwanted by users or harmful; *to prevent the transfer of unlawful content*; or to prevent the unlawful transfer of content; and ought to embody other reasonable network management practices.²⁹ It might safely be inferred that content that infringes a copyright should be treated as “unlawful,”³⁰ thereby enabling the ISPs to take reasonable action to prevent the transfer of unlawful content, such as the unlawful distribution of copyrighted works. Herein arises the role and lies the importance of copyright filtering.

Preserving an Open Internet: The Three Camps Debate on the Propriety of Net Neutrality Regulation

In an attempt to assess the impact of the aforesaid norms on the copyright protection on the Internet, perspectives have been advanced by three lobbies in sync with their commercial interests, which, in turn, have shaped the ongoing debate on the propriety of net neutrality regulation.³¹

First, ISPs argue against the necessity of net neutrality regulations,³² citing that consumer choice and market pressures will provide an appropriate level of protection for consumers. They feel that government regulation in this area will serve only to interfere with their ability to effectively manage and protect their networks, and will stifle continued innovation and improvement in the services available to consumers over the Internet. ISPs contend that the extent to which they attempt to identify or block allegedly infringing material should be left in their discretion, along with all of the other day-to-day network management decisions they must make.³³

²⁹ *Id.* at paragraph 135.

³⁰ The Proposed Rules expressly indicate that content that infringes a copyright should be treated as “unlawful.” *Id.* at paragraph 139.

³¹ *Supra* note 8.

³² In the context of US, this tussle between the FCC and the ISPs has been manifest in the Comcast case, and the FCC Open Internet Order, 2010 vs. Verizon case (2014). The recently released (12 March, 2015) net neutrality rules by the FCC has started a 60-day clock before it takes effect (on June 12), and just minutes after the rules were published in the Federal Register, USTelecom, a consortium of ISPs, filed an injunction against them, arguing that they are “arbitrary, capricious and an abuse of discretion,” and violate federal law; Don Reisinger (April 13, 2015), “Net Neutrality Rules get Published- Let the Lawsuits Begin”, [Online: web] Accessed 25 April, 2015, URL: <http://www.cnet.com/news/fccs-net-neutrality-rules-hit-federal-register-lawsuit-underway/>.

³³ *Ibid.*

Second, companies involved in ‘content creation’ industries, including music, movies, television, and to some extent software, maintain that net neutrality is harmful to the extent they in any way restrict the ability of broadband providers, in collaboration with content owners, to take voluntary measures to deter potentially infringing activity.³⁴

The third view is harboured by the companies that provide applications and services over the Internet, along with certain public interest groups, who tend to favour net neutrality regulation. These groups argue that broadband providers should not be allowed to give preferential treatment to their own content, or to content provided by their business partners, as this would create a “pay to play” system that would disrupt the development of new Internet technologies and businesses. They have expressed concerns that broadband providers may interpret the “reasonable network management” exception to allow the blocking or filtering of lawful content based on the pretext of preventing the transfer of actual (or even suspected) “unlawful content.” They also argue that there is insufficient competition in the broadband market in most areas for consumer choice to prevent abusive conduct.³⁵

The Hot Button Issues

- **Copyright Filtering via Deep Packet Inspection**

The quest of the content industry for a “magic bullet”³⁶ solution to the problem of online copyright infringement- one that would simultaneously eradicate the problem of online file sharing while breathing new life into pre-digital business models, has brought to the fore a form of a technology that promises, albeit not absolutely, to automatically and effectively eradicate copyright infringement online. In order to accurately identify whether any content is unlawful, resort has to be taken to this copyright filtering technology known as deep packet inspection, or DPI. DPI describes a process in which the network’s equipment looks beyond the addressing information (called a header) usually used to direct a packet on to its destination and evaluates

³⁴ *Ibid.*

³⁵ *Ibid.*

³⁶ Mehan Jayasuriya *et. al.*, “Forcing the Net Through a Sieve: Why Copyright Filtering Is Not a Viable Solution for U.S. ISPs”, *Public Knowledge*, [Online: web] Accessed 25 April, 2015, URL: <http://www.publicknowledge.org/paper/pk-filtering-whitepaper>.

the actual contents of the data packet, or even a stream of related packets.³⁷ Although it sounds distinctly Orwellian, such packet inspection provides ISPs with a greater ability to determine whether the traffic they carry respects all intellectual property rights of the content creator. In other words, packet sniffing provides the means for ISPs to determine whether their network has become a medium for the unlawful transport of files to recipients lacking lawful authority to consume, copy, and share intellectual property.³⁸ Combining DPI with content identification software designed to identify particular copyrighted audio or video works might allow broadband providers to identify and filter out infringing content flowing through their networks.³⁹

It is noteworthy that network neutrality qualifies the ISPs for copyright infringement safe harbours,⁴⁰ when the online service providers operate as a neutral, transitory conduit for content, engage in temporary caching or storing of content, and when they provide search tools that link to information created by others, they are exempted from liability,⁴¹ and barred from any monetary damages for direct, contributory, and vicarious infringements. It necessarily follows that in order to qualify for the safe harbour,⁴² ISPs might have to eschew DPI or limit its nature and scope because this process would evidence a non-neutral operating environment where the ISP has the ability to know when copyright infringement takes place. ISPs may soon view network neutrality obligations as providing a less valuable safe harbour if it forecloses their use of DPI. It is practically implausible to activate a neutral network that takes cognisance of copyright, or DPI that retains network neutrality. In application, DPI appears to offer an all or nothing value proposition; either an ISP has the ability to examine content and to discriminate on the basis of several different quality of service variables or it does not. To argue that an ISP can discriminate and still qualify for safe harbours and respect network neutrality would require creative interpretation of what constitutes “actual knowledge” of copyright infringement.

For ISPs actual knowledge can occur when an ISP engages in deep packet inspection. However the ISP might claim that deep packet inspection provides only information sufficient for the ISP to know how to classify, switch, route and process traffic without actual knowledge of whether by transporting a particular bitstream the ISP has facilitated copyright infringement.

³⁷ *Supra* note 8.

³⁸ Rob Frieden (2008), “Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers”, *Fordham Intell. Prop. Media & Ent. L.J.*, 18: 633.

³⁹ *Supra* note 8.

⁴⁰ In an effort to balance the obligation to protect copyright holders with an interest in promoting investment in the Internet and its use as an engine for commerce, Congress included in the DMCA, 17 U.S.C. § 512 (2007), a chapter entitled the Online Copyright Infringement Liability Limitation Act.

⁴¹ *Ellison v. Roberston*, 357 F.3d 1072, 1076-77 (9th Cir. 2004).

⁴² A safe harbor constitutes “an area or means of protection [or a] provision (as in a statute or regulation) that affords protection from liability or penalty.” Black’s Law Dictionary (8th ed. 2004) 1363.

Answers to the questions whether, how, and when an ISP acquires actual knowledge of copyright infringement largely depend on what can and will become standard information contained in Internet packet headers. Arguably ISPs can limit their deep packet inspection to that minimally intrusive level needed to monitor traffic for purposes of “proper” and “routine” classification, switching, routing and processing. Under this scenario an ISP might ignore copyright information, i.e., take no affirmative steps to protect the copyright holder, and simply carry packets containing headers that have copyright usage information that may impact how receivers of a file can use, copy, and resend the file. Some types of Digital Rights Management (DRM)⁴³ can provide enhanced copyright protection without any affirmative efforts by the ISP providing the link between sender and recipient. If this type of DRM becomes an industry standard, then ISPs possibly could transmit without any meddling, scrutinizing or processing, packets containing DRM instructions for processing by equipment on user premises.

The active examination of traffic via DPI raises privacy questions as well. DPI apparently involves a significant invasion into the privacy of the communications being carried over the Internet, tantamount to the Post Office opening and reading people’s mail.⁴⁴ Further, due to technological limitations, copyright filters will harm lawful, protected forms of speech such as parody and satire.

Further, considering the fact that content identification technology is itself in a fairly early stage of development, DPI might land in jeopardy. The systems that have been developed to date have primarily been designed to crawl relatively static repositories of data, including content hosting sites like YouTube, or to monitor smaller private networks.⁴⁵ It could be immensely more difficult and expensive for an ISP to implement such a system to review Internet traffic arriving across multiple network access points in real time without significantly slowing down the traffic itself, adding latency thereto. Additionally, such a filtering system may be unable to review traffic that is encrypted, making encryption an easy solution for those interested in distributing unlawful infringing content and evading detection.

⁴³ Digital Rights Management (“DRM”) refers to the use of technological tools by copyright owners and distributors to regulate the uses of their works, and in particular to restrict reproduction; Nika Aldrich (2007), “An Exploration of Rights Management Technologies Used in the Music Industry”, *B.C. Intell. Prop. & Tech. F.* 051001, [Online: web] Accessed 25 April, 2015, URL: <http://bcptf.org/index.php?option=comcontent&task=view&id=30&Itemid=30>.

⁴⁴ *Supra* note 8.

⁴⁵ *Supra* note 36.

- **Possibility of Affecting Lawful Content: Adverse Impact on Fair Use**

DPI and similar filtering systems may have difficulty identifying instances of the lawful fair use of copyrighted works, running the risk that this category of lawful content could be inadvertently blocked. The modes available for content identification and analysis, like the use of metadata, digital watermarks, or acoustic and visual characteristics (fingerprinting) are all flawed in some way or the other.⁴⁶ Even if they are not, there is every chance that the implementation of copyright filters might result in a technological arms race, wherein users would act to circumvent the filters and the architects of the filters will find themselves caught in a costly, unwinnable arms race.⁴⁷

When network management includes decisions about the use, copying, and sharing of content, hardware and software substitute for people and impose new *ex ante* limitations instead of after the use examination whether infringement has occurred. Using technological intermediaries in lieu of human decision-makers risks expanding DRM to a point where hardware and software operate as proxy censors⁴⁸ as well as repressors of fair use.⁴⁹ It has been noted that

Every permissions-based DRM implementation (in which the user must formally acquire some form of explicit authorization to engage in a particular use of the protected work) simply reproduces a variant of the 'judge on a chip' problem. No such system can ever replicate the experience of fair use in the offline world because the requirement of *ex ante* authorization by the copyright holder or its designee is a departure from offline practice and statutory requirements.⁵⁰

Fair use in an offline environment involves empirical and value judgments based on somewhat ambiguous criteria:

⁴⁶ *Ibid.*

⁴⁷ *Ibid.*

⁴⁸ "To the extent that potential regulators can induce [providers of Internet equipment and services] to disrupt communications, whether by blocking payment to targeted websites, or by embedding obstacles to communication and mechanisms of surveillance in the hardware or software that facilitates communication, they can spawn effective proxy censors"; Seth F. Kreimer (2006), "Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link", *U. PA. L. Rev.*, 155: 11, 17.

⁴⁹ Timothy K. Armstrong (2006), "Digital Rights Management and the Process of Fair Use", *Harv. J.L. & Tech.*, 20: 49, 54.

⁵⁰ *Ibid.*

The copyright law, although carefully worded, simply cannot be expressed in the kind of algorithmic language that is required of computer programs to automate functionality like printing or copying. This is especially true of 'fair use' . . . a deliberately vague exception to the monopoly rights of the copyright holder.⁵¹

Empowering hardware and software to establish and enforce a priori fair use policies usurps decision making by individuals and vests it with an intermediary that has every incentive to take the path of least resistance and lowest cost. If it is costly to distinguish protected from unprotected speech, the proxy censor is likely to abandon the effort to avoid errors and adopt a conscious policy of prophylactic self-censorship that blocks any content that could precipitate the threat of sanctions.⁵²

In view of the difficulties in implementation of a robust DPI filtering system by ISPs, it is possible that the initial decision might have to be made on other grounds, for example, the type (e.g., peer-to-peer) and source of the traffic, as well as evidence (typically provided by content owners) that the source in question had historically been associated with a significant amount of infringing content. Given these looser parameters, it would be at least possible, if not likely, that some lawful content could be included within the traffic affected.

The obscurity of the problem of protecting intellectual property online could be exemplified by the following instance. Under the DMCA Notice and Takedown regime, the illegal content is removed directly from the ISPs hosting it upon their notification from users. To highlight the dangers such regimes pose for free speech, the 2004 study by Christian Ahlert, Chris Marsden and Chester Yung run the following experiment: after having uploaded in a US and a UK ISP hosted website the second chapter from Stuart Mill's on Liberty, which symbolically referred to censorship, they then complained to the hosting ISPs about copyright breach; even though the works of Mill is public domain published in 1869, the UK ISP immediately complied with the takedown request and removed the content.⁵³ In spite of such alarming findings, the relevant legislation continues to maintain its parochial views on property and spatiality.⁵⁴

⁵¹ *Id.* at 52.

⁵² *Supra* note 48.

⁵³ Ch Ahlert *et. al*, "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self Regulation", [Online: web] Accessed 25 April, 2015, URL: <http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf>.

⁵⁴ Argyro P. Karanasiou (2012), "Respecting Context: A New Deal for Free Speech in the Digital Era", *European Journal of Law and Technology*, 3(3), [Online: web] Accessed 25 April, 2015, URL: <http://ejlt.org/article/view/144/266>.

Conclusion

Although the propriety of re-feudalization of the public sphere of internet remains debated, the fact that the free market economy has impacted the internet cannot be contested. In fact, the decision of the ISPs to engage in active management of content results not from an affirmative obligation to do so, but instead the desire to tap new business opportunities accruing from the ability to scrutinize bitstreams. Further, since the inception of the internet occurred much later the promulgation and development of the copyright laws, it would be safe to comment that the internet, *vis-a-vis* the access to contents, could never be, and has never been neutral. Network Neutrality has been called a solution in search of a problem, whose proponents cite the absence of numerous examples of blocking or degradation to back this argument. This is a red herring: there are multiple real-world instances of blocking and impairment.⁵⁵ Instead of venturing into the sceptical utilitarian overtones of the concept of copyright, it would be safer to subscribe to the status quoist stand that in view of the set norms, a limited protection has been advanced to the copyright owners, maintenance of which would generate positive externalities. The quest for absolute net neutrality, in the sense of proscribing any intervention from the part of the ISPs, might worsen the status of online copyright infringement. The conceptual paradigm of a neutral net must take note of the fact that safeguarding the protection accorded to the copyright owners is paramount as well, and towards this end allow the intervention of the ISPs to a certain extent via packet-sniffing.

Despite the marked inefficacies and current inefficiencies in the present copyright filtering mechanism via DPI, one can rarely underestimate its potential in pre-empting online copyright infringement. When an ISP chooses to operate a non-neutral conduit, the ISP, internationally or not, should incur greater responsibility for the content it carries.⁵⁶ Arguably ISPs will have much greater capability to protect intellectual property rights, in light of the contractual quality of service commitments they make to specific customers and the enhanced knowledge of the nature and type of the traffic that traverses their networks. Such technological capability may further condition or eliminate the safe harbour, and quite justifiably so, because ISPs may no longer claim they lack actual knowledge that the material or an activity using the material on the system or network is infringing.

⁵⁵ Save the Internet: Big Lie 3, [Online: web] Accessed 25 April, 2015, URL: <http://www.savetheinternet.com/=lie3>.

⁵⁶ Doug Lichtman & Eric Posner (2006), "Holding Internet Service Providers Accountable", *Su P. Ct. Econ. Rev.*, 14: 221, 257.

If implemented, a copyright filtering mandate would force ISPs to inspect all data transmitted by all Internet users, invading the privacy of hundreds of millions of citizens at the behest of one industry. This would likely have far-reaching consequences for the Internet ecosystem as a whole, disincentivizing investment, innovation and creativity. Therefore, certain alternative modes to prevent online copyright infringement ought to be explored. Notifications could be provided to the ISPs with instructions that make DRM more effective. Instead of relying on piracy protection embedded in files already delivered by an ISP to recipients' computers, active scrutiny of traffic possibly can preempt the transmission of pirated files in the first place.

Further, given the risk of losing a safe harbour, ISPs likely will err on the side of accommodating DRM cooperation requests from copyright holders. ISPs probably will collaborate with copyright holders perhaps going so far as to program hardware with deep packet inspection software that achieve both traffic management goals, to pursue price and QOS diversification, as well as DRM, to mollify copyright holders. Should this scenario play out the current network neutrality debate will have addressed not only the future accessibility of the Internet to users and content providers, but also the future nature and scope of consumers' fair use opportunities to access, copy, and resend content available via the Internet.

By exploring new, innovative business models, the content industry can encourage consumers to purchase entertainment goods even when that same content is available for illegal download online. This fact is evidenced by increases in online music sales, decreases in unlawful music file sharing and strong sales of movie tickets and high-definition physical video products like Blu-Ray discs- all despite the widespread availability of albums and full-length films on P2P file-sharing networks. Additionally, some have suggested that even if unlawful file sharing continues, artists and content companies could still be compensated if they are willing to adopt a more innovative licensing model, such as voluntary collective licensing. Ultimately, the content industry will have to work closely with technologists, innovators and policymakers to find solutions that make sense in a digital economy.

The afore-discussed avenues to protect copyrighted material online ought to provide a cue to the Indian legal system, wherein there are yet no proper laws governing net neutrality. While the Telecom Regulatory Authority of India (TRAI) guidelines for the Unified Access Service license promote net neutrality, they are not enforced. In March 2015, the TRAI released a formal consultation paper on *Regulatory Framework for Over-the-top (OTT) services*, seeking comments from the public. Moreover, certain ISPs have manifestly chosen to be non-neutral. The Information

Technology Act, 2000 does not prohibit companies from throttling their service in accordance with their business interests. In such circumstances, it is possible that an ISP may impose certain types of premium rent on download or surfing. Attaching utmost priority to pre-empting or preventing online copyright infringement, and realizing firstly, that internet has never been neutral vis-a-vis content protection, and secondly, that such neutrality would be a myth in an era marked by free enterprise notions, the Indian legal system should aspire to balance the interests of the copyright holders on one hand, and the consumers on the other. Note should also be taken of the capabilities and limitations of the ISPs with respect to copyright filtering, and alternative modes to protect copyright and innovative business models might call for exploration towards attainment of the objective.

REFERENCES

Primary Sources:

- “FCC Statement on *Comcast v. FCC Decision*”, Apr 6, 2010, [Online: web] Accessed 25 April, 2015, URL: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297355A1.pdf.
- Definition of “Internet”, October 24, 1995, Resolution of the U.S. Federal Networking Council, [Online: web] Accessed 25 April, 2015, URL: https://www.cnri.reston.va.us/what_is_internet.html#xv.
- FCC Internet Policy Statement, FCC 05-151 (adopted Aug. 5, 2005).
- Notice of Proposed Rulemaking, *In re Preserving the Open Internet*, GN Docket No. 09-191, WC Docket No. 07-52 (adopted Oct. 22, 2009), [Online: web] Accessed 25 April, 2015, URL: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf .
- The Open Internet Order, FCC, paragraph 14, [Online: web] Accessed 25 April, 2015, URL: <https://www.federalregister.gov/articles/2015/04/13/2015-07841/protecting-and-promoting-the-open-internet>.

Cases:

- *Comcast Corp. v. FCC*, 600 F.3d 642.
- *Ellison v. Roberston*, 357 F.3d 1072, 1076-77 (9th Cir. 2004).
- *Nat’l Cable Tel. Ass’n v. Brand X Internet Servs.*, 545 U.S. 967 (2005).
- *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

Secondary Sources:

Books:

- Black’s Law Dictionary (8th ed. 2004).
- Habermas Jürgen (1989), *The Structural Transformation of the Public Sphere*, (Trans. T. Burger) (MIT Press).
- Cooper M (ed.), *Open Architecture as Communications Policy: Preserving Internet Freedom in the Broadband Era* (Centre for Internet and Society, Stanford Law School).

- Thierer A. and Crews C.W. (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Internet Governance and Jurisdiction, Washington, DC: Cato Institute).

Articles:

- Ahlert Ch *et. al*, "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self Regulation", [Online: web] Accessed 25 April, 2015, URL: <http://pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf>.
- Aldrich Nika (2007), "An Exploration of Rights Management Technologies Used in the Music Industry", *B.C. Intell. Prop. & Tech. F.* 051001, [Online: web] Accessed 25 April, 2015, URL: <http://bciprf.org/index.php?option=comcontent&task=view&id=30&Itemid=30>.
- Armstrong Timothy K. (2006), "Digital Rights Management and the Process of Fair Use", *Harv. J.L. & Tech.*, 20: 49, 54.
- Bar and Sandvig G (2000), "Rules From Truth: Post Convergence Policy for Access" (Paper presented at the 28th Telecommunications Policy Research Conference (TPRC) on Communication, Information and Internet Policy, Alexandria, Virginia, USA) 22.
- Cerf V. and Kahn R. (2004), "What Is the Internet (and What Makes It Work)" in Cooper M (ed.), *Open Architecture as Communications Policy: Preserving Internet Freedom in the Broadband Era* (Centre for Internet and Society, Stanford Law School), [Online: web] Accessed 25 April, 2015, URL: https://www.cnri.reston.va.us/what_is_internet.html#xv.
- Frieden Rob (2002), "Revenge of the Bellheads: How the Netheads Lost Control of the Internet", *Telecomm. Pol'y*, 26: 425, 425- 44.
- Frieden Rob (2008), "Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers", *Fordham Intell. Prop. Media & Ent. L.J.*, 18: 633.
- Herman Bill D. (2006), "Opening Bottlenecks: On Behalf of Mandated Network Neutrality", *Fed. Comm. L.J.*, 59:103, 109-10.
- International Telecommunication Union (March 23-24, 2006), "What Rules for IP-enabled NGN?", Workshop, [Online: web] Accessed 25 April, 2015, URL: <http://www.itu.int/osg/spu/ngn/event-march-2006.phtml>.

- Jayasuriya Mehan *et. al.*, "Forcing the Net through a Sieve: Why Copyright Filtering Is Not a Viable Solution for U.S. ISPs", *Public Knowledge*, [Online: web] Accessed 25 April, 2015, URL: <http://www.publicknowledge.org/paper/pk-filtering-whitepaper>.
- Karanasiou Argyro P. (2012), "Respecting Context: A New Deal for Free Speech in the Digital Era", *European Journal of Law and Technology*, 3(3), [Online: web] Accessed 25 April, 2015, URL: <http://ejlt.org/article/view/144/266>.
- Kreimer Seth F. (2006), "Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link", *U. PA. L. Rev.*, 155: 11, 17.
- Landau Susan (2006), "National Security on the Line", *J. Telecomm. & High Tech. L.* 4: 409, 424.
- Lessig Lawrence (2000), "Symposium: Cyberspace and Privacy: A New Legal Paradigm?", *Stanford Law Rev*, 52: 991.
- Lessig Lawrence (2002), "The Architecture of Innovation", *Duke L J*, 51: 1789.
- Lichtman Doug & Posner Eric (2006), "Holding Internet Service Providers Accountable", *Su P. Ct. Econ. Rev.*, 14: 221, 257.
- Meinrath Sascha D. *et.al.* (2011), "Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide", *Commlaw Conspectus*, 19:423.
- Reisinger Don (April 13, 2015), "Net Neutrality Rules get Published- Let the Lawsuits Begin", [Online: web] Accessed 25 April, 2015, URL: <http://www.cnet.com/news/fcc-net-neutrality-rules-hit-federal-register-lawsuit-underway/>.
- Save the Internet: Big Lie 3, [Online: web] Accessed 25 April, 2015, URL: <http://www.savetheinternet.com/=lie3>.
- Schultz Thomas (2008), "Curving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", *EJIL*, 19 (4): 799-839.
- Sommer Jeff (March 12, 2015), "What the Net Neutrality Rules Say", [Online: web] Accessed 25 April, 2015, URL: http://www.nytimes.com/interactive/2015/03/12/technology/net-neutrality-rules-explained.html?_r=0.
- Thierer Adam D. (Jan. 12, 2004), "'Net Neutrality' Digital Discrimination or Regulatory Gamesmanship in Cyberspace", *Policy Analysis*, no. 507, [Online: web] Accessed 25 April, 2015, URL: <http://www.cato.org/pubs/pas/pa507.pdf>.
- Walthall Howard (2010), "The Net Neutrality Debate: An IP Perspective", *Landslide*, American Bar Association, 3(1).

- Wu Tim (2003), "Network Neutrality and Broadband Discrimination," *Journal of Telecommunications & High Technology*, 26, [Online: web] Accessed 25 April, 2015, URL: <http://faculty.virginia.edu/timwu/bbd.pdf>.
- Wyatt Edward, "Rebuffing F.C.C. in 'Net Neutrality' Case, Court Allows Streaming Deals", *New York Times*, [Online: web] Accessed 25 April, 2015, URL: <http://www.nytimes.com/2014/01/15/technology/appeals-court-rejects-fcc-rules-on-internet-service-providers.html> 15.01.2014.
- Zittrain J. (2003), "Be Careful What You Ask For: Reconciling a Global Internet and Local Law", in Thierer A. and Crews C.W. (eds.), *Who Rules the Net? Internet Governance and Jurisdiction* (Internet Governance and Jurisdiction, Washington, DC: Cato Institute) 13.
- Zittrain J. (2003), "Internet Points of Control", *Boston College L Rev*, 44: 653, 656.
- Zulfi Muhammad Zulqarnain (February 10, 2014), "Net Neutrality: Here is Everything You Need to Know about it", [Online: web] Accessed 25 April, 2015, URL: <http://indianexpress.com/article/technology/technology-others/net-neutrality/>.