Filtering of Content and Intermediary Liability

Filtering

1. Books

1.1 Access Denied: The Practice and policy of Global Internet Filtering (R. Deibert et al., eds., MIT Press, 2008)

This book provides a comprehensive treatment of issues surrounding internet filtering by addressing the manner in which filtering is achieved technologically, placing filtering within the legal framework, discussing the ethics that binds corporations to the politics of censorship. The book also has OpenNet Initiative's regional and country profiles.

1.2 Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace (R. Deibert et al., eds., MIT Press, 2010)

A sequel to the previous publication (*Access Denied*), OpenNet Initiative's recent release has six more essays on filtering on the internet along with regional and country profiles. Filtering is no longer restricted to the more obvious methods of blocking URLs, IP addresses or using key words, all of which are part of the Chinese-style first generation filtering techniques. Second and third generation methods have emerged whereby take down notices, virus attacks, denial of service attacks and other less obvious means are employed to control content on the internet, especially in countries that form part of the OSCE. Cyberspace is the very environment we inhabit and under these changed

circumstances, the manner in which states control the internet assumes significance. Freedoms are under threat even as states exercise wide powers under the guise of security and this is changing the very nature of society. Information infrastructure then is under threat by new generation methods of control and this book provides a glimpse into these current developments.

See:http://books.google.com/books?id=ZojiQG4irWEC&printsec=frontcover&hl=es#v=onepage&q&f=false

1.3 Y. Akdeniz and K. Altiparmak, Internet: Restricted Access – A Critical Assessment of Internet Content Regulation and Censorship in Turkey (Freedom of Expression Program in IHOP, 2008)

This book traces the legal history of Law 5651, which is the legislation that allows for internet filtering in Turkey. This then is assessed within the paradigm of the EU policy on internet content filtering. Given Turkey's unique position in Europe, the development of internet censorship here is of significance in assessing how the European Court of Human Rights' approach to freedom of expression plays out here.

2. Articles

2.1 A Starting Point: Legal Implications of Internet Filtering (A publication of the OpenNet Initiative, JEL Classifications: O380, K420, K390, 2004)

The most common grounds for filtering are morality and national security. While some countries make laws specifically for the internet, others employ the same laws for all media and yet others apply general law. Regardless of this, civil liberties are affected. Issues of jurisdiction, choice of law and enforcement that riddle internet filtering are discussed. In this piece by OpenNet Initiative, while filtering is considered to be an inevitable outcome, the argument is for a transparent, technically viable, legally sound and country-specific standard.

2.2 B. E. Bambauer, Filtering in Oz: Australia's Foray into Internet Censorship (University of Pennsylvania Journal of International Law, vol. 31, no. 2, p. 493, 2009-10)

Australia's proposed law on internet censorship is not new to the cyber community, but by being the first western liberal democracy to openly adopt this policy, the author argues that this portends a shift in the manner in which filtering will be perceived by western democracies. The author assesses

filtering in Australia against the touchstone of openness, transparency, narrowness and accountability.

2.3 C. Callanan et al., Internet Blocking – Balancing Cybercrime Responses in Democratic Societies (Open Society Institute, 2009)

A comprehensive article on internet filtering, the author examines the meaning of 'blocking', the motivations for adopting such a method of regulation, the methods by which filtering on the internet is attempted, the relationship between filtering and the law before making an argument for balancing fundamental freedoms that come in conflict with filtering by applying the three part test of legality, legitimacy and necessity.

2.4 Internet filtering in Singapore in 2004-05: A Country Study (OpenNet Initiative, 2005)

The government in Singapore regulates cyberspace through access control in the form of licensing or through legal pressures of prosecution and there is minimal regulation by means of technical filtering. Only a handful of sites are blocked, and this is more for symbolism than as an effective manner of filtering internet content. The lack of technical filtering however does not make the regulation any less effective; on the contrary this perhaps allows for greater regulation.

2.5 J. G. Palfrey, Local Nets: Filtering and the Internet Governance Problem (chapter in Jack Balkin et al., 'The Global Flow of Information', 2010)

While states argue that filtering is a necessary exercise well within the exercise of their sovereignty, the lack of a mechanism that protects rights while securing the interest of the public is necessary. The need then is to ensure that countries build a sustainable model of filtering that will determine the shape we wish the internet and information technology to take.

2.6 J. Weckert, What is so Bad about Internet Content Regulation? (Ethics and Information Technology, Kluwer Academic Publishers, 2000)

Whether the internet *can* be regulated is just as much a concern as whether it *should* be, given that other media are already regulated. Mill's consequentialist arguments as also his harm principle are considered as standards by which to measure the necessity and degree of censorship on the internet.

Although the author believes that there exist moral justifications for regulating the internet, irrelevance of frontiers and technological impossibility make regulation as we know it ineffective. Greater research and international cooperation are advised.

2.7 N. W. Netanel, Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory (California Law Review vol. 88, no. 2, p. 395, 2000)

In this article, the author evaluates the cyberian claim that a self-governing cyber space is the most conducive to realizing liberal democratic values. His argument is that an unregulated cyberspace would not benefit liberal democratic ideals since the majority can and will suppress the minority even in cyber-space, thus necessitating filtering and other forms of regulation.

2.8 P. A. Craddock, Legal Implication of Internet Filtering (King's College London, LLM Dissertation, 2010)

Tracing the history of filtering with the *Yahoo!* case as the starting point, the author discusses the methodology of filtering employed by different states. The legal framework in Europe that would apply specifically to ISP-level filtering is then discussed. Freedom of expression can be lawfully restricted if the three part test of legality, legitimacy and necessity is fulfilled. The author discusses these tests and then seeks to locate filtering within this to determine its validity.

2.9 P. H. Ang, How Countries are Regulating Internet Content

(See http://www.isoc.org/inet97/proceedings/B1/B1_3.HTM)

In this paper, the manner in which internet content is regulated in United States, France, Singapore, China and South Korea is briefly outlined. The attempt is to ascertain different methods by which internet content is regulated. While the models adopted reflect some of the features adopted in other media, it is argued that the same have to be adjusted to meet the specific requirements of the internet. There may perhaps never be a universal model, but given the many different existing paradigms, countries need not have to formulate a new policy but can draw inspiration from existing policies after which adjustment for cultural differences can be incorporated.

2.10 P. M. Garry, The Flip Side of the First Amendment: A Right to Filter (Michigan State Law Review p.57, 2004)

The author argues that the American courts have been unnecessarily liberal in deciding the scope of freedom of speech permissible on the internet given the propensity of misuse of cyberspace. Legal decisions vis-à-vis filtering is discussed to determine the course taken by the courts this far and the future course they will steer.

2.11 Race to the Bottom – Corporate Complicity in Chinese Internet Censorship (Human Rights Watch, vol. 18, no. 8(c), 2006)

In a comprehensive article that traces the methods employed by the Chinese government to control content on and access to the internet, HRW assesses ICP licenses and filtering. Excessive control of the internet amounts to violation of the right to freedom of speech and expression and unfortunately the government is not the only one violating this right as it has more than ample support from corporate players on the internet.

Statute

LOPPSI [France] – The Loppsi 2 (loi d'orientation et de programmation pour la performance de la sécurité intérieure - law on guidelines and programming for the performance of internal security) is a bill on National Security approved by the French government. One of the most controversial provisions of the draft legislation is the one that allows ministerial orders to direct ISPs to block certain URLs.

See:http://www.theregister.co.uk/2010/02/17/france_ip_law/,
http://www.edri.org/edrigram/number9.1/loppsi-2-adopted-assembly
http://www.spiegel.de/international/europe/0,1518,678508,00.html

Intermediary liability

1. Relevant Laws

1.1 Communication Decency Act of 1996 (USA) [hereinafter CDA]

The CDA was passed in order to effectively tackle indecent and obscene content on the internet. The law was however stuck down for the most part in *Reno v. ACLU [521 U.S 844 (1997)]* for violating the First Amendment. A provision that still remains however is s. 230, also called the Good Samaritan clause. It allows for intermediaries on the internet to escape liability as long as they are merely internet service providers and not information content providers. This provision has assumed significance over the past in cases of defamation on the internet.

1.2 Digital Millennium and Copyright Act of 1998 (USA) [hereinafter DMCA]

The DMCA was passed in order to prevent copyright violation on the internet. s. 512 creates a safe harbor for online service providers from being held liable for infringing information on the internet as long as they comply with the notice-and-take-down policy.

1.3 The EU Electronic Commerce Directive 2000/31/EC

This directive of the European Parliament and of the Council adopted in 2000 was adopted for regulating electronic commerce. The directive also creates a legal framework for intermediary liability under s. 4. If the service is that of a mere conduit, or providing cache services or hosting content then the service is not liable as long as certain conditions are satisfied. This is the most well defined legal provision on intermediary liability in Europe.

1.4 Information Technology Act 2000, as amended in 2008 along with

1.5 Rules of 2011 (India) [hereinafter IT Act]

India is one of the few countries to have a specific provision for the intermediary liability. Provisions of the Act have been recently amended to accommodate changing dynamics of the internet. s. 2(w) of the Act defines an intermediary and s.79 grants immunity to intermediaries under certain circumstances. Recently, the government of India notified rules under s. 79 called The Information Technology (Due Diligence Observed by Intermediaries Guidelines) Rules, 2011 which allow intermediaries to remove "objectionable" content without notifying the user. Objectionable content includes content that is blasphemous, capable of inciting hatred, is ethnically objectionable, infringes

patents and threatens India's unity or public order. All these are vague provisions for most of them have not been defined either in any legislation or in any judicial pronouncement.

2. Case Law

2.1 U/s.230 CDA

2.1.1 Batzel v. Smith [333 F.3d 1018 (9th Cir. 2003)]: Smith sent an email to Cremers who ran a website on stolen art, writing to him about Betzel's collection of paintings which she inherited as the descendent of Hitler's right hand man. The contents of this mail were made public by posting on the website and mailing through listserv. Following this, Batzel proceeded against Smith, Cremers Museum Security Network, the website. The court held that the website was merely a service provider and hence immune under s.230 CDA. As for Cremers, immunity was upheld. Although there was the issue of whether the information provider intended to provide the information, it was held that a service provider would reasonably presume that there was indeed such an intention.

2.1.2 Ben Ezra, Weinstein and Co. v. America Online [339 F.3d 1119 (9th Cir. 2003)]: Information about the stock price and share volume in the plaintiff company was provided to the defendant by third parties. This information turned out to be false. AOL however was held to be merely a service provider having had no role in the development of the content thus excluding it from liability under s. 230 CDA.

2.1.3 Blumenthal v. Drudge and American Online, Inc.: This was a defamation case in which the first defendant wrote of the plaintiff's abuse of the latter's spouse. The second defendant was however merely a service provider and hence immune under s.230.

2.1.4 Carafano v. Metrosplash [333 F.3d 1018 (9th Cir. 2003)]: The court had to consider to what extent a computer matchmaking service would be legally responsible for false content in a dating profile provided by someone posing as another person. It was held that the website was providing internet services and was hence immune under s. 230 CDA.

2.1.5 Doe v. MySpace [No. 1:06-cv-00983-SS (W.D. Tex 2007)]: Peter Solis and Julie Doe were both minors who purported to be adults on the social site, MySpace. They arranged to meet one day when the latter allegedly sexually assaulted the former. The question before the court was whether MySpace, which was the internet service provider, was also an information content provider, and it was answered in the negative. Plaintiff further argued that MySpace ought to have exercised greater duty of care which was dismissed by the court. Thus MySpace was eligible to claim immunity under s.230 of the CDA.

2.1.6 Fair Housing v. Roommate.com [489 F.3d 921 (9th Cir. 2007)]: The defending website was an intermediary that helped match roommates. Those availing of this service were required to answer a

questionnaire requiring personal information which included an open-ended question. Several councils argued that the Fair Housing Act was violated and roommate.com was to be held liable for the same. Since the search mechanism and e-mail notifications resulted in roommate.com being neither a passive pass-through of information provided by others nor merely a facilitator of expression, it was a content provider making it liable. However, vis-à-vis the open ended questions, it was also held that since roommate.com did not prompt, encourage or solicit any information provided by some of its members, it was not an information content provider and was hence eligible to seek immunity under s.230 of the CDA.

2.1.7 Fair Housing v. Roommate.com [521 F.3d 1157 (2008)]: The Ninth Circuit revised its previous decision en banc to widen the ambit of immunity under s.230 of the CDA. As long as the intermediary merely organizes and makes cosmetic changes to content that was already user generated, it retains immunity. Here, the information content providers were users of the website and not the website itself; the intermediary was not involved in the creation or development of content.

2.1.8 Grace v. eBay [2004 WL 214449 (2004)]: The information provided by a third party about a commodity on sale on the defendant's website would not make the defendant liable as it was merely a service provider.

2.1.9 Optinrealbig.com v. Irontransport Systems [323 F.Supp.2d 1037 (N.D.Cal. 2004)]: Plaintiff was a sender of spam and the defendant collected complaints against senders of spam and then forwarded these to ISPs that provided services to the senders of spam. In the instant case, the plaintiff's contention was that the defendant was curtailing its legitimate business unnecessarily. However the defendant could legitimately seek cover under s.230 since it was merely service provider that forwarded complaints received, perhaps aggressively so, but it had no role in the creation of the content.

2.1.10 Zeran v. America Online [129 F.3d 327 (4th Cir. 1997)]: There was a defamatory message on AOL and the appellant-plaintiff wanted this to be removed although this was not complied with, and the case was dismissed on the ground that AOL was not liable. It was argued by the appellant-plaintiff on appeal that the notice requirement meant that the interactive service provider was liable, but the court held again that AOL was immune from liability under s. 230 of the CDA.

2.1.11 See here for more cases and analysis - http://ilt.eff.org/index.php/Defamation:_CDA_Cases

2.2 U/s. 512 DMCA

2.2.1 Corbis Corporation v. Amazon.com, Inc., et al. [351 F.Supp.2d 1090 (W.D. Wash. 2004)]: Amazon was held to be immune from liability if it was engaged in selling an item by someone not affiliated to it, even if this involved the violation of copyright, due to the safe harbor provision.

2.2.2 Hendrickson v. eBay [165 F. Supp. 2d 1082 (C.D. Cal. 2001)]: Pirated versions of DVDs of a movie were being distributed on the defendant website and hence it was alleged to be involved in secondary copyright infringement. The plaintiff had sent a notice, but this was found to be inadequate. It was held that the site would only be liable if it had constructive knowledge, which it did not in the instant case. Besides, the defendant could not be held to have the ability to control merely due to the ability to block information.

2.2.3 In Re: Aimster Copyright Litigation [252 F. Supp. 2d 634 (N.D. Ill. 2002)]: Due to Aimster's willful blindness to what was transpiring when music was being swapped on its site, it was held to be in violation of the DMCA and hence the site was shut down. No immunity could be sought here as there was constructive knowledge, and besides Aimster was more than a service provider as it enticed netizens to download music.

2.2.4 IO Group, Inc. v. Veoh Networks, Inc [586 F. Supp. 2d 1132 (N.D. Cal. 2008)]: Veoh could obtain safe harbor protection for the media that they were streaming, although several of these were openly violative of the copyright law. This was because they complied with the take down policy, removing all content for which they received notice on the ground of copyright violation. Since necessary measures were undertaken under appropriate circumstances, Veoh was not violating copyright laws.

2.2.5 Perfect 10, Inc. v. CCBill LLC [488 F.3d 1102 (9th Cir. 2007)]: Plaintiff was the publisher of an adult entertainment magazine and owned the site perfect10.com. It was alleged that the defendants violated copyright, trademark, and state unfair competition, false advertising and right of publicity laws by providing services to websites that posted images stolen from Perfect 10's magazine and website. Immunity was sought under both the safe harbor clause under the DCMA and s.230 of the CDA. Partially reversing the district court's decision, the court here remanded certain issues to the district court to ultimately decide whether the safe harbor provision could indeed apply to the defendants. In so far as CDA was concerned, the defendants were held to be eligible for s.230 immunity.

2.2.6 See here for more cases and analysis

http://ilt.eff.org/index.php/Copyright:_Digital_Millennium_Copyright_Act

3. Articles

3.1 H. B. Holland, In Defence of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism (Kansas Law Review, vol.56, p. 101, 2008)

The author makes a case in defence of s. 230 of the Communications Decency Act which is placed within the broader scheme of internet governance. It is argued that this provision

assumes further significance owing to emerging changes in the internet in the form of web 2.0 that allows for community generation of content.

3.2 J. N. Azriel, Social Networking as a Communications Weapon to Harm Victims: Facebook, Myspace, and Twitter Demonstrate a Need to Amend Section 230 of the Communications Decency Act (John Marshall Journal of Computer & Information Law, vol.26, p. 415, 2009)

The dynamics of social networking sites are such that they allow for user-generated content creation and leave scope for abuse of rights. In light of the growing number of social networking sites, there is a need to amend existing laws to tackle new problems. The author seeks to look at the changing nature of the internet and make a case for changing existing law.

3.3 M. A. Lemley, Rationalizing Internet Safe Harbours (Journal of Telecommunications and High Technology Law, vol. 6, p. 1010, 2007; Stanford Public Law Working Paper No. 979836)

The author believes that it would be an impossible task to make intermediaries succeed in filtering all content considered to violate the law. The patchwork of safe harbor provisions consisting of s. 1114(2) of the Lanham Act along with s.230 of the Communications Decency Act and s. 512 of the Digital Millennium create a disparate body of law vis-à-vis intermediary liability and there is a need for standardizing the law. The best mechanism to adopt, argues the author, is the safe harbor provision under the less popular Lanham Act; originally created for protection from trademark infringement.

3.4 S. F. Kreimer, Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link (155 University of Pennsylvania Law Review 15, p.11, 2006-2007)

The architecture of the internet makes it difficult to ascribe liability on speakers or listeners directly and hence liability is fixed on private intermediaries who are clink in the armour. The author argues that this move poses a threat to the freedom of speech as intermediaries will have less incentive to protect free speech than individual speakers and market forces do not have the power to balancing rights. Interestingly, the doctrinal basis for the protection of the freedom of speech is drawn from the McCarthy-era.

3.5 S. Friewald, Comparative Institutional Analysis in Cyberspace: The Case for Intermediary Liability for Defamation (Harvard Journal of Law and Technology, vol. 14, no. 2, 2001)

In this article, the author seeks to determine which institution – Congress, courts or the market – must determine the scope of intermediary liability. He does so by exploring various methodologies such as the public choice theory, transaction cost economics and legal processes. The comparative institutional analysis is used to determine the best mechanism by which internet intermediaries can be held liable in the specific instance of defamation. Not only is the preferred institution analysed, the author provides an analysis for what would emerge if other institutions are given the authority to determine intermediary liability. The author urges courts to take a greater look at comparative institutional analysis to determine the role of law in cyberspace.