IT Rules vis-à-vis International Standards

India's Intermediary Liability Regime

Shehla Rashid Shora

Fellow, Asia Internet Coalition

New Delhi, 2013

Contents

Executive Summary

India's Information Technology Act (2000) was amended in 2008 to include, among other provisions, Section 79- the 'safe harbor' provision under which Internet intermediaries like Facebook, Google, etc. can claim exemption from prosecution or liability for user-generated content. In 2011 the rules under this provision, commonly known as IT Rules, were notified, and these contain "due diligence" requirements for intermediaries- conditions under which the intermediaries can claim exemption from liability. These Rules have come under severe criticism for their adverse effects on freedom of expression and their constitutionality is now being challenged in the Supreme Court of India.

The Constitution of India provides for reasonable restrictions to freedom of expression under limited grounds. However, the restrictions under the IT Rules go much beyond these grounds. The IT Rules are also in violation of international human rights standards relating to freedom of expression and provided mainly in the ICCPR (International Covenant of Civil and Political Rights) to which India is a signatory. The UDHR (Universal Declaration of Human Rights) and the ICCPR make it amply clear that the choice of a medium does not constitute grounds for putting additional curbs on freedom of expression. Article 19 of the ICCPR states that every person shall have the right to freedom of expression, including the right to seek, receive and impart information through the medium of their choice.

The UN Human Rights Committee has issued a clarification, by way of general comment number 34, stating explicitly that free speech guarantees under Article 19 apply equally well to the Internet and other electronic communication.

Furthermore, in a joint declaration in 2011, four UN special rapporteurs, including Mr. Frank La Rue, recommended that intermediaries should not be held liable for content generated by others unless they have specifically intervened or refused to obey a court order. The IT Rules stand in opposition to these recommendations, as intermediaries can be held liable for third-party content even if they are not involved in the creation or modification of such content. They can also be held liable even when no court order has been issued, that is, in the event of non-compliance with a private complaint.

Apart from being arbitrary and broad, the IT Rules also allow private censorship. That is, a private party can send a takedown notice to the intermediary, who, fearing prosecution, might take it down to be on the safer side, and the user whose content has been taken down will not be notified, meaning that, unless the affected user discovers on their own, they would not be aware of the takedown. This takes away from the user a chance to defend herself or himself, or to challenge the takedown. The UN Special Rapporteur for freedom of expression, Mr. Frank La Rue, has made it clear that private censorship mechanisms are unacceptable. This view is echoed by civil society, industry and policy experts.

Finally, although not directly concerned with takedown requests, is the "due diligence" requirement under which an intermediary must provide information and assistance to the government or any of its agencies, in order to claim exemption from liability. No procedure or tests for proportionality and necessity for such an exercise have been mentioned anywhere. India does not have a privacy law at the

time of writing and this requirement, therefore, can have severe chilling effects on freedom of expression.

It is, thus, clear that the IT Rules are in contravention of both India's own constitutional guarantees of freedom of expression as well as the internationally accepted human rights standards. India must revisit its intermediary liability regime to uphold human rights.

Introduction

According to the IAMAI (Internet and Mobile Association of India) the number of Internet users in India had reached 205 Million in October, 2013 and was projected to increase to 213 Million by December, 2013. India is next only to the US and China in terms of number of Internet users. The number of Facebook users has been registering phenomenal growth with around 114 Million MAUs (monthly active users) at the end of November, 2013, representing over 50% of the total Internet user base.

In July, 2013 India had crossed 20 million Twitter users, according to a study by IAMAI and IMRB International, a market research firm. China, the world's most populous country, maintains strict controls over the content that can be accessed in its territory. Chinese users do not, officially, have access to Twitter; and Google transferred delivery of their search results from China to Hong Kong in 2010 following heavy regulation on content and apprehensions of liability. This places India, with its growing Internet user base, as an increasingly important emerging market for Internet giants such as Facebook, Google, Twitter, eBay, etc. In fact, research firm eMarketer has predicted that India will overtake the US in the number of Facebook users by 2016[1]. These statistics point out that an increasing number of people in India are using social media platforms to express themselves in overwhelming numbers.

Newer platforms such as Quora and Youth Ki Awaaz are emerging as popular forums of discourse and debate among young people. This means that Indians are not only consumers of technology but also active producers of content. Companies like Facebook, Twitter and Google (through its various services such as YouTube, Google plus, Blogger, GMail etc.), which serve as platforms to facilitate communication over the Internet, are known as "intermediaries", as they are not usually involved in producing content but only in hosting it. There are other types of intermediaries such as Internet Service Providers (ISPs) which operate at a lower level and control the physical infrastructure that allows us to access the Internet. At one level or the other, we all use services provided by these 'intermediaries' to communicate and to express ourselves over the Internet.

Internet intermediaries are bound by certain laws governing the content that they host. They can be asked to take content down, pass on user information to the government or block access to a website. Takedown of content is made possible by the rules notified under Section 79 of India's Information Technology Act. These rules, being the focus of this paper, have been reproduced in Appendix A for the reader's convenience. These will be analysed in the light of international human rights standards as well as the Indian Constitution itself. Failure, on part of intermediaries, to take down content can result in prosecution. Since the intermediary is not the author of such content, prosecution in this way goes against the principle of natural justice. Furthermore, these rules provide for private censorship in that a private party can send a takedown request and failure to comply with it can result in prosecution. Additionally, the grounds for takedown are extremely broad and also vague in their applicability. The intermediaries are not required to inform the user whose content has been taken down, implying that the affected user does not get a chance to appeal against censorship.

Finally, the IT Rules make it mandatory for intermediaries to provide user

information to the government or any of its agencies for the investigation of any crime, as part of the "due diligence" requirements for seeking protection under Section 79 of the IT Act. However, no clear procedure for demanding user information has been defined. Also, it is not required that disclosure of user information be in conformity with principles of necessity and proportionality[2]. This assumes more importance, given the fact that India does not have a law for the protection of privacy.

Intermediary Liability and Freedom of Expression in India

In India, intermediary liability became a contested issue in the early 2000's when the CEO of an e-commerce portal, Avnish Bajaj, was arrested for a leaked sex tape that was uploaded to the portal by a third party. The portal, baazee.com was later acquired by e-bay[3]. Although India's Information Technology Act was passed by the Parliament in the year 2000, Bajaj's arrest in 2004 highlighted the need for offering some protection to Internet intermediaries. In 2008, Section 79 of the IT Act, meant to be the 'safe harbor' provision, was introduced through an amendment and the Rules under it were notified in 2011 as the Information Technology (Intermediaries guidelines) Rules, 2011 commonly known as IT Rules, 2011. However, contrary to their stated purpose of providing 'safe harbor' to intermediaries in some situations, the Rules implicate intermediaries even if they aren't involved in modifying the content. Any private individual can send a complaint to an intermediary demanding removal of content and failure to do so could lead to criminal prosecution. Fearing prosecution, many intermediaries may choose to take content down, thus resulting in private censorship without the involvement of law enforcement agencies or courts at all. This provision has been misused, most famously, in the case of political cartoonist Aseem Trivedi whose website hosting provider was forced to take down his website 'cartoonsagainstcorruption.com' on a private complaint. The hosting provider, Big Rock, later issued a statement clarifying that they were forced to affect the takedown because failure to do so could have resulted in criminal prosecution[4]. Trivedi, along with his aide, Alok Dixit, launched a campaign against the IT Rules known as 'Save Your Voice' in January, 2012[5].

An annulment motion, seeking to overturn the IT Rules, was moved in the upper house of the Parliament of India by an MP, Mr. P Rajeev in May, 2012. Even though the motion was defeated, the Minister for Communications and Information Technology, Mr. Kapil Sibal assured the house that broader discussions on the Rules would be held[6]. The Centre for Internet and Society (CIS), a leading civil society organisation based in Bangalore, has developed an alternative to IT Rules[7]. In what CIS calls a 'policy sting', it sent frivolous complaints to seven Internet intermediaries asking for removal of content under the IT Rules. Six out of the seven intermediaries complied, thereby substantiating the alleged chilling effect of the IT Rules[8].

While intermediaries in some instances have bowed down to frivolous or motivated complaints fearing prosecution, Mr. Faisal Farooqui, CEO of review portal mouthshut.com, is currently challenging the IT Rules in the Supreme Court of India. Tired of responding to frivolous takedown complaints, legal notices and court summonses, including a fake one, Mr. Farooqui decided to challenge the constitutional validity of the IT Rules in India's apex court in a public interest litigation filed in April, 2013[9]. A parliamentary committee on subordinate

legislation that had been constituted to look into various intermediary liability provisions submitted its report in March, 2013. The report clearly says, among other things, that the committee expects the Communications and Information Technology Ministry to have a fresh look at the IT Rules, so as to remove ambiguity[10]. At the time of this writing, no action has been taken on the report by the Ministry.

The Constitution of India and IT Rules

Article 19(1)(a) of the Indian Constitution guarantees, to all Indian citizens, the right to freedom of expression. Article 19(2) permits the Government of India to make laws that impose reasonable restrictions on this right in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

However, the scope of the IT Rules is very broad and restrictions under these far exceed both the scope of Article 19(2) as well as the definition of what may constitute a "reasonable restriction". Again, in case of defamation, for example, the aggrieved party has to obtain an injunction from the court to get the allegedly defamatory material seized or stopped from being circulated, online or offline. However, this provision allows any private party to bypass the whole procedure and simply send a notice to the intermediary. In this way, the onus of deciding whether the content is prima facie defamatory is transferred to the intermediary. Also, it also implicates the intermediary in the crime, if, say, the content is indeed harmful and not taken down.

Further, the IT Rules have employed very vague terminology and included terms like "ethnically objectionable", "grossly harmful", "disparaging", "hateful", etc. Even if interpreted narrowly, there is ample scope for abuse in these terms. The government has often reasoned that intermediaries themselves have guidelines for content posted on their website and that they understand the scope of these terms. This argument is completely unacceptable, to say the least. Intermediaries' community guidelines can be extremely strict or extremely lenient and can be changed by them at will. It is not acceptable for us to rely upon the posting guidelines of intermediaries. To illustrate by way of example, a feminist portal may not tolerate the misogynistic posts of the kind that, say, Reddit would. However, it is possible that a post may be misogynistic but not illegal. The reason that this point is even being explained is that the government repeatedly offers this as if it were an unproblematic explanation.

Intermediary liability and human rights

This section borrows from a policy brief prepared recently by Article 19, an international organization that works on issues of freedom of expression. In particular, the human rights standards cited here have been taken from the said brief titled, "Internet Intermediary: Dilemma of Liability", which outlines principles for internet intermediary liability. One of the aims of this paper is also to extend these to India, as Article 19's policy brief does not contain the word 'India' even once. In this section, the IT Rules will be analysed in the light of international human rights standards, an exercise that has not been undertaken yet.

Article 19 of the Universal Declaration of Human Rights (UDHR) guarantees the right to freedom of expression in broad terms as a right that includes the right "to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers."

Article 19 of the ICCPR states that:

0. Everyone shall have the right to freedom of opinion.

a. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

It is clear from the two provisions above that online and offline speech cannot be treated differently merely because of a difference in the medium used. However, as has been explained in the previous section, mechanisms for private censorship exist only for online content and not for offline content. Also, the IT Rules make illegal certain types of content which may be perfectly legal offline. It can, therefore, be safely said that the IT Rules are in contravention of both the ICCPR and the UDHR, to which India is a signatory.

In September 2011, the UN Human Rights Committee (HR Committee), a treaty monitoring body for the ICCPR, issued General Comment No 34[11] which states that:

0. Article 19 of ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and internet-based modes of expression.[12]

a. States parties to the ICCPR must consider the extent to which developments in information technology, such as internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[13] In particular, the legal framework regulating the mass media should take into account the differences between the print and broadcast media and the internet, while also noting the ways in which media converge.[14]

The four special mandates on the right to freedom of expression have highlighted in their Joint Declaration[15] on Freedom of Expression and the Internet of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the internet. In particular, they recommend that tailored approaches for responding to illegal online content should be developed, while pointing out that specific restrictions for material disseminated over the internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

Article 19(3) of the ICCPR permits the following restrictions on the right to freedom of expression:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order, or of public health or morals.

Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put the right itself in jeopardy[16]. The method of determining whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must: (i) be provided by law; (ii) pursue a legitimate aim; and (iii) conform to the strict tests of necessity and proportionality[17].

The IT Rules provide for restrictions far greater than those provided in Article 19(3) of the ICCPR and Article 19(2) of the Indian Constitution.

The same principles apply to electronic forms of communication or expression disseminated over the Internet[18]. In particular, the UN Human Rights Committee noted that:

> Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government[19].

In their 2011 Joint Declaration on Freedom of Expression and the Internet[20], the four special rapporteurs on freedom of expression recommended that:

0. No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information;

a. Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;

b. ISPs and other intermediaries should only be required to take down content following a court order, contrary to the practice of notice and takedown.

This is clearly not the case in India, as the mere failure to remove content following a request is adequate ground for prosecution under the current IT Rules, regardless of whether the intermediary has intervened in the content or not. Furthermore, the IT Rules do not require the complainant to cite any legal order while requesting a takedown.

About such private censorship mechanisms, the UN Special Rapporteur on freedom of expression in 2011 stated that:

> Censorship measures should never be delegated to a private entity, and […] no one should be held liable for content on the internet of which they are not the author. Indeed, no State should use or force intermediaries to undertake censorship on its behalf[21].

Quoting directly from the Article 19 brief, "This is not simply a matter of intermediaries not having the relevant legal expertise to make such judgments, but a more fundamental matter of legal principle: i.e. that measures affecting fundamental rights should be applied by an independent court rather than by private bodies."[22]

He further recommended that, in order to avoid infringing internet users' right to freedom of expression and right to privacy, intermediaries should only implement restrictions to these rights after judicial intervention; that intermediaries should be transparent about measures taken with the user involved and, where applicable, with the wider public; that they should provide,

if possible, forewarning to users before implementing restrictive measures; and they should strictly minimise the impact of any restrictions to the specific content involved. Finally, the Special Rapporteur has emphasised the need for effective remedies for affected users, including the possibility of appeal using procedures to be provided by the intermediary and by a competent judicial authority.

As we know, this is not the case in India. The IT Rules require neither that a court order be obtained, nor that the affected user be warned before or after the takedown. Transparency and minimization of restrictions are nowhere prescribed as norms in the IT Rules or in the IT Act of India. Again, there exists no mechanism whereby an affected user can appeal for their content to be restored.

Quoting, again, from Article 19's policy brief, "[Notice-and-takedown] procedures have been criticised for being unfair. Rather than obtaining a court order requiring the host to remove unlawful material (which, in principle at least, would involve an independent judicial determination that the material is indeed unlawful), hosts are required to act merely on the say-so of a private party or public body. This is problematic because hosts tend to err on the side of caution and therefore take down material which may be perfectly legitimate and lawful. For example, in his report, the UN Special Rapporteur on freedom of expression noted":

> while a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown. Moreover, given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by overcensoring potentially illegal content. Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences[23].

Toward Alternatives

In the light of the applicable human rights standards, Article 19 has made four key recommendations for intermediary liability laws:

1. Web hosting providers or hosts should in principle be immune from liability for third-party content when they have not been involved in modifying the content in question.

2. Privatised enforcement mechanisms should be abolished. Hosts should only be required to remove content following an order issued by an independent and impartial court or other adjudicatory body which has determined that the material at issue is unlawful. From the hosts' perspective, orders issued by independent and impartial bodies provide a much greater degree of legal certainty.

3. Notice-to-notice procedures should be developed as an alternative to notice and takedown procedures. These would allow aggrieved parties to send a notice of complaint to the host. Notice-to-notice systems should meet a minimum set of requirements, including conditions about the content of the notice and clear procedural guidelines that intermediaries should follow.

4. Clear conditions should be set for content removal in cases of alleged serious criminality.

As has been shown in this paper, India's intermediary liability guidelines stand in stark opposition to these key recommendations. Considering the fact that India is a signatory to the UDHR and the ICCPR from which all the observations/recommendations, made by the Human Rights Committee, the Special Rapporteur and by Article 19 itself, follow, the issue comes across as much more serious.

Policy analysts, activists and legal experts working in India have highlighted this issue repeatedly and have even proposed alternatives to the existing IT Rules.

Appendix A- Section 79 of the Information Technology Act and the Information Technology (Intermediaries Guidelines) Rules, 2011 (IT Rules, 2011)

Section 79. INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hasted by him.

(2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted; or

(b) the intermediary does not—

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if—

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or othorise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Information Technology (Intermediaries Guidelines) Rules, 2011

The intermediary shall observe following due diligence while discharging his duties, namely: —

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

(a) belongs to another person and to which the user does not have any right to;

(b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

(c) harm minors in any way;

(d) infringes any patent, trademark, copyright or other proprietary rights;

(e) violates any law for the time being in force;

(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

(g) impersonate another person;

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.

(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2):

provided that the following actions by an intermediary shall not amount to hosing, publishing, editing or storing of any such information as specified in sub-rule: (2) —

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes,

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer

resource, the Intermediary has the right to immediately terminate the access or usage lights of the users to the computer resource of Intermediary and remove non-compliant information.

(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance.

(8) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2011.

(9) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to "perform thereby circumventing any law for the time being in force:

provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

---

[1] 'India Leads Worldwide Social Networking Growth', *eMarketer*, 19 Nov, 2013, http://www.emarketer.com/Article/India-Leads-Worldwide-Social-Networking-Growth/1010396 Retrieved on 21 Dec, 2013

[2] 'International Principles on the Application of Human Rights to Communications Surveillance', *Necessary and Proportionate*, 10 Jul, 2013 https://en.necessaryandproportionate.org/text Retrieved on 20 Dec, 2013

[3] 'Baazee.com - India's leading online marketplace - was acquired by eBay Inc. - The World's Online Marketplace', *eBay*, 31 Jan, 2005 http://pages.ebay.in/community/aboutebay/news/pressreleases/corporate/aquisition.html Retrieved on 19 Dec, 2013

[4] Shashank, 'cartoonsagainstcorruption.com – BigRock's Stance and a Sequence of Events', *Big Rock*, 25 Sep, 2012 http://bigrock.com/blog/general/cartoonsagainstcorruption-com-bigrocks-stance-and-a-sequence-of-events Retrieved on 20 Dec, 2013

governance/counter-proposal-by-cis-draft-it-intermediary-due-diligence-and-information-removal-rules-2012.pdf Retrieved on 20 Dec, 2013

[10] 'COMMITTEE ON SUBORDINATE LEGISLATION (2012-2013) (FIFTEENTH LOK SABHA) THIRTY-FIRST REPORT', PRS India, 21 Mar, 2013 http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf Retrieved on 30 Dec, 2013

[15] 'International Mechanisms for Promoting Freedom of Expression JOINT DECLARATION ON FREEDOM OF EXPRESSION AND THE INTERNET', *Article 19*, 2011 http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf Retrieved on 30 Dec, 2013