Censoring the Internet: The New Intermediary Guidelines

RISHAB BAILEY

The government's recent actions in notifying the Intermediary Guidelines for the internet with minimal public debate have resulted in the creation of a legal system that raises as many problems as it solves. The regulations as presently notified are arguably unconstitutional, arbitrary and vague and could pose a serious problem to the business of various intermediaries in the country (not to mention hampering internet penetration in the country) and also to the public at large who may face increased instances of censorship and invasion of privacy.

Rishab Bailey (*rishab.bailey@gmail.com*) is a lawyer and is associated with the Knowledge Commons Collective based in New Delhi.

The unprecedented growth of the online world brings with it two major problems for law enforcement – anonymity and dispersion. In order to deal with criminal action on the internet, since it may be practically impossible to physically locate the perpetrator of the crime, what has come to be recognised as the most efficient and/or easiest method of regulating the medium is through the points of access that the public has to any content.

Between every user of the internet and the content being accessed are numerous actors involved in the process of bringing to the user the desired content. These actors carry out a differing range of functions from uploading the content, hosting/storing the content (either permanently or temporarily) to archiving or cataloguing the content or even providing physical access to the internet (as in the case of a cybercafe). Each of these actors through which a user can access content on the internet is an intermediary,[1] and effectively without any intermediaries there is no internet.

An intermediary can theoretically exercise control over the flow of content, possibly making it more efficient for them to deal with instances of offending material. It could however be argued that such a system aims more at assigning liability to a particular actor (consequently an easily identifiable target for damage claims) rather than trying to address the issue of the illegal content in itself. This explains why, for example, governments have found it almost impossible to ban certain websites – they keep reappearing on other servers or in different countries.

As discussed in this article, the aforesaid line of thought has led to a rather disconcerting global movement of the law towards privatising what would ordinarily be in the domain of the judiciary (or in cases, of the executive). This could both increase the costs of conducting business over the internet and instances of unwarranted censorship. There is a need for balance in the policy infrastructure so as to promote free expression without undue interference while at the same time ensuring that criminal offences are dealt with appropriately and without imposing undue costs on innocent parties.

Indian law regulates intermediaries, through the Information Technology Act, 2000 (the "IT Act") and various rules made thereunder, notably the Information Technology (Intermediary Guidelines) Rules, 2011 (the "Intermediary Guidelines"). As discussed further, there has been considerable progress in changing what was an unworkable and inequitable legal regime under the original IT Act, to a more rational regulatory regime in 2009 with the passing of the Information Technology (Amendment) Act, 2008. However, the government's recent actions in notifying the Intermediary

Guidelines (together with a set of regulations governing cybercafes) with minimal public debate, have resulted in the creation of a legal system that raises as many problems as it solves. The aforesaid regulations as presently notified are arguably unconstitutional, arbitrary and vague and could pose a serious problem to the business of various intermediaries in the country (not to mention hampering internet penetration in the country) and also to the public at large who may face increased instances of censorship and invasion of privacy.

This article therefore attempts a critical analysis of the Intermediary Guidelines taking into account the prevalent standards for intermediary liability in the United States (US) and the European Union (EU).

In the US

One of the first precedents on the issue is that of *Cubby Inc vs Compu Serv*, where a district court of New York held that the defendant was not liable for providing access to defamatory material carried on its web-based forum. The court applied the defence of innocent dissemination by a distributor (the general rule that a publisher is subject to liability unless it knew or had reason to know the content). As the defendant had subcontracted for the content, and had exercised no editorial control whatsoever (the court also noted the impracticality of expecting a host to exercise editorial control over large quantities of information), the court classified the defendant as a distributor rather than a publisher. The aforesaid decision can be contrasted to that in *Straton Oakmont vs Prodigy Services*, where the New York Supreme Court held the defendant liable as it purported to moderate content posted on its website.

These decisions however lead to the conclusion that should an intermediary edit or moderate the content on the website (even if not playing an active part in the creation of the content) he could open himself up to liability, so he might actually be better served doing nothing at all and utilising the immunity available under law for distributors (this risk could however be offset by the fact that there may be more public demand for moderated content).

In order to resolve the apparent conflict and to reassure internet service providers, the Communications Decency Act was passed in 1996, which categorically provided safe harbour to intermediaries. As per Section 230, no provider or user of an interactive computer service is to be treated as the speaker or publisher of any information provided by another information content provider. The section further protects service providers from action taken in good faith (thereby allowing service providers to voluntarily restrict access to material deemed by the service provider to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable).[2] The service provider's only other responsibility is to inform its users that commercially available services exist that can moderate the content viewed by the user.

This "safe harbour" provision has been interpreted fairly liberally to afford service providers with near absolute freedom from liability in exchange for voluntary self-censorship. The near absolute protection provided to intermediaries (which is much greater than that provided under the law to traditional media) has however led to decisions that could at best be termed against the basis of the enactment itself – for example, that of *Doe vs America Online* where the defendant was allowed to plead immunity under Section 230, despite having failed to remove content of a paedophiliac nature, after notice of the same. Thereafter there have been further attempts to bring in legislation to regulate in particular, paedophilia, though most such enactments have more often than not failed to come into effect.

The US' experience with issues of regulating free speech through intermediaries can therefore be said to have returned mixed results. On the one hand, it has provided a haven for a huge paedophile market while on the other, the regime providing blanket immunity has reduced the regulatory burden, lowered costs of business and encouraged the freedom of expression.

The US regulates intellectual property issues through the Digital Millennium Copyright Act of 1998. In an attempt to balance the interests of service providers and the copyright industry (music, films, publishing, etc) Section 512 protects registered service providers from claims in the event that they did follow a notice and take-down policy. Upon receiving notice from a copyright holder, the service provider must bar access to the infringing material within two weeks to preserve its statutory defence from liability. The content can be restored if a counter-notice is received, unless the copyright holder files suit.

This system moves away from the liability regime under the Communications Decency Act in attempting to strengthen online intellectual property rights, but has been criticised on numerous grounds[3] including as (a) it has the practical effect of incentivising censorship of material as large amounts of content have been removed by intermediaries upon mere suspicion of infringement or upon receiving false notice, (b) the ease of censorship through this route has made it a worthwhile short-term censorship option to use, and (c) the lack of due process and a judicial role in adjudication.

EU Law

The EU extends protection to intermediaries based entirely on function (broadly similar to the Common Law system used in England). The Electronic Commerce (EC Directive) Regulations 2002, which give effect to the E-Commerce Directive of 2000, divides service providers into three categories and assigns differing grades of liability to each:

- If an intermediary acts as a mere conduit, it is not liable for third party content that it transmits,
- if the intermediary is involved with hosting or cacheing, it is not liable for content that is unknowingly hosted/cached, but if an alleged infringement is brought to their notice, it may potentially be liable, and,
- if the intermediary acts as an author/editor it is liable for third party content so edited or authored.

As per Regulation 19, a host may avail of the immunity offered by the regulations if it

- has no actual knowledge of the content in question. Upon receipt of actual knowledge of the illegality, it must act to remove or disable access to the material as quickly as possible;
- is not aware of facts or circumstances from which the illegality of the content in question should have been apparent;
- was not controlling or in authority over the user responsible for the content.

As in the case of the Digital Millennium Act in the US, the notification of the E-Commerce Directive has also created a situation where it is rational for an

intermediary to immediately disable access to content upon receiving any complaint whatsoever. Further complications have also been seen due to the diverse nature of functions provided by intermediaries, which can often be difficult to categorise. For instance, in the case of *L'Oreal vs Ebay*, it has been held that knowledge required for a web host to acquire liability could be gained through the host's own "voluntary research" thereby potentially affecting the business of all websites that trawl or cache content. Similarly, in *Kaschke vs Gray & Hilton* it has been held that a blog host who corrects the punctuation of a third party post might convert itself from a "host" to an "editor" and in *Twentieth Century Fox Film Corporation vs Newzbin* it has been held that a company that provides indexing of copyrighted files cannot avail of the immunity provided to intermediaries.

In England and other countries in Europe, while there is no one standard for intermediary liability (despite the EC directive), intermediaries continue to enjoy immunity but up to levels far lower than seen in the US. Of course, more importance is attached to the factual circumstances behind the commission of the offence and the possibility of minimalising damage. Intermediaries are therefore more prone to block information than in the US.

The Indian Position

The IT Act, 2000, in Section 79 originally provided all intermediaries with exemption from liability for third party data made available by it, if the intermediary proved that the offence or contravention was committed without its knowledge, or that it had exercised all due diligence to prevent the commission of the offence. This provision placed an extremely high standard of care on intermediaries by placing the burden of proving non-complicity on the intermediary, who had to further satisfy the court that it had taken appropriate measures to pre-empt the offence.

The problem with this section was illustrated with the *Avnish Bajaj*[4] case where the chief executive officer of an online auction site was found guilty of distributing obscene material as users of the site had auctioned a pornographic clip online.

The amendment to the IT Act in 2009, inter alia replaced the existing Section 79 with a new provision, whereby intermediaries[5] were not to be liable for any third party information, data or communication hosted by it, if the various circumstances mentioned in the section were met. The amended Section 79 also empowered the government to lay down "due diligence" criteria for intermediaries to follow.

Despite some criticism[6] the introduction of such a section was undoubtedly required in view of the nature of the business of intermediaries and to protect them from undue legal harassment. The section bears a broad resemblance to the European handling of the issue by adopting a functional approach to intermediary liability (which is commendable in itself).

To further clarify the requirements to claim immunity, the government has recently notified the Intermediary Guidelines in April 2011. The guidelines however fail to build upon the framework provided by the IT Act itself and are at best ill thought-out.

As per the provisions of the Intermediary Guidelines, all intermediaries must prescribe a set of rules and regulations, privacy policy and user agreement for users to access the intermediary's computer resources. The terms and conditions must require the user to abstain from creating or publishing information that inter alia: (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, paedophiliac, 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 whatsoever; (c) harms 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 the addressee about the origins of the message or communicates information that is grossly offensive or menacing in nature; (g) impersonates another person; (h) contains viruses or other malware, etc; and (i) threatens the sovereignty of the nation, national security, incites commission of any cognisable offence, etc.

In the event the intermediary knows of any infringing material, either based on private complaint or from its own knowledge, it must act to take down the infringing material within 36 hours and without providing any notice or hearing to the creator of the supposedly infringing material. Intermediaries must comply with government directions to provide information, etc, as and when required. Every intermediary is required to set up a grievance redressal mechanism through which users may report violations of the various conditions mentioned in the Guidelines.

The Intermediary Guidelines are clearly impractical as they cast obligations well beyond the means of most intermediaries, as defined under the IT Act. It is to be noted that intermediaries include businesses such as cybercafes, online websites, etc, and compliance with its strict requirements is likely to be exceedingly onerous. Further, the need to regulate cybercafes under such a law is unclear, given that the government has simultaneously notified the Information Technology (Guidelines for Cybercafe) Rules, 2011, which cover the rights, duties and obligations of a cybercafe in some detail.

The constitutionality of the Intermediary Guidelines is open to question given that it empowers and obliges intermediaries to weed out pernicious or objectionable information on the internet. With the amount of information available on the internet, it is impossible for an intermediary to ensure that all content made available to users is inoffensive as per the criteria laid down. The crucial point here is that the Intermediary Guidelines fail to mandate any sort of judicial role in the process (the closest concession being a requirement of a "lawful order" by an investigative agency prior to enlisting the aid of any intermediary).

In the normal course, the intermediary is required to make a judgment on the offensive nature of any information and act to take the offending content offline. This is especially noteworthy given that there is no differentiation in the Intermediary Guidelines on the various types of criminal acts that may take place and no recommendations on treating differing crimes differently (for example, a terrorist threat would presumably require greater attention than a blog suspected of maligning a public figure – both are however treated to the same procedure). The intermediary may also be

required to act upon receiving appropriate requests from the public. This is clearly arbitrary and unconstitutional and has tremendous scope for misuse. It should be noted that normally if any person is aggrieved by any information being made public, they may seek remedies – including the relief of injunction – from courts of law, under generally applicable civil and criminal law. There is no rational reason for the inapplicability of such provisions even for information posted on the internet. In the case of search engines and other such intermediaries that regularly trawl the net to catalogue and archive information, it is impractical and unwise to expect them to make an accurate and informed decision on content that breaches the fairly wide wording of the Intermediary Guidelines.

The list of information that is barred includes vague terms such as "is blasphemous"[7] "harassing", "disparaging", "hateful", "or otherwise unlawful in any manner", etc. This is patently in violation of various fundamental rights protected under the Constitution. The Intermediary Guidelines are therefore ambiguous and consequently arbitrary in that they fail to lay down parameters for deciding what is objectionable, disparaging, etc, and what is not. Further, intermediaries are required to act as an agency of the government in censoring offending material and may be liable (or lose immunity under Section 79) for failure to do the same. The list of offensive information is extremely broad (more so than in Sections 69 and 69A of the IT Act). Supreme Court dicta make it evident that if any limitation on the exercise of the fundamental rights under Article 19(1) does not fall within the ambit of Article 19(2) or is not reasonable and just, it cannot be upheld. The removal of content can only be done if it falls under the reasonable restrictions imposed under Article 19(2) of the Constitution, and even then only following a court order. Hence the broad list of proscribed information provided by the Intermediary Guidelines, together with the absence of any fair procedure for determining what is offending material ensures that the Guidelines are ultra vires the Constitution of India.

The constitutionality of the Intermediary Guidelines may also be called into question on the grounds that they enlarge and expand the scope of the IT Act beyond what was originally envisaged. While the government is empowered by the IT Act to frame guidelines for the process of due diligence by intermediaries, the present guidelines go well beyond the scope of what could normally be considered "due diligence". They have widened the scope of the IT Act by listing a broad list of information that can be considered unlawful and then requiring intermediaries to act as a policing agency of the state. It is a settled principle that the conferment of rule-making power by an Act does not enable the rule-making authority to make a rule which travels beyond the scope of the enabling Act or which is inconsistent there with or repugnant thereto. As noted by the Supreme Court,[8] a delegate who has been authorised to make subsidiary rules and regulations has to work within the scope of its authority and cannot widen or constrict the scope of the parent Act or the policy laid down thereunder. It cannot, in the garb of making rules, legislate on the field covered by the parent Act and has to restrict itself to the mode of implementation of the policy and purpose of the parent Act.

It is to be noted also that the existing procedures involved in interception, monitoring and blocking of information (which involves executive action, coupled with multiple stages of review but no judicial role) under Sections 69 and 69A will be rendered useless if information can be censored through the offices of an intermediary. The current Intermediary Guidelines completely remove the (minimal?) safeguards contained in Section 69 and rules framed thereunder, and would make intermediaries answerable to virtually any request from any source accusing any website of breaching these Guidelines – this could seriously hamper the business of any online website.

In practice what the Intermediary Guidelines entail is that any person wanting to block access to certain information can complain of the same to the appropriate intermediary (after ensuring that the complaint falls within one of the fairly ambiguous terms used in the Guidelines), thereby placing the onus of making a decision on the matter to the intermediary. It would have to be a fairly brave intermediary to resist the temptation to just block/delete content despite the potential costs of failing to take action on an accurate complaint. Further, the absence of "a put-back" provision, and the fact that intermediaries are not required to explain or provide reasons for taking down content (even to the author) is cause for concern.

Conclusions

There appears to be a global movement towards adopting a "notice and take-down" policy (the EU regime, the Digital Millennium Act, etc). Such a regime passes the costs of adjudication on to private parties (who in turn are likely to pass them on to users) and may also inhibit free speech. The lack of judicial oversight can be a problematic issue, especially in the case of small businesses or short-term censorship.

The Indian law initially took a step forward with the passing of the IT Amendment Act in 2009 but with the introduction of the Intermediary Guidelines, the safe harbour provided by Section 79 of the Act has been eroded so as to be practically non-existent. The Indian position at the moment seems untenable especially as much of the content accessed in India is created abroad, which means Indian intermediaries will bear the brunt of any liability claims.

The issue of how to deal with intermediary liability is therefore one for which there is no straitjacket answer. However, I believe that any successful system must be built on the following principles that are more compatible with the enhancement of the internet as a medium of communication:

(a) Self-regulation by intermediaries appears to lead to suboptimal enforcement of the law and promotes arbitrariness and decreases transparency by promoting private action in a public sphere.

(b) The law needs to differentiate between intermediaries on the basis of functionality and should provide immunity where the intermediary was not in a position to control or assess the offence (practically or in law).

(c) The law must differentiate between various crimes on the basis of severity and damage and deal with each category appropriately (and possibly through changes in other relevant statutes such as the Copyright Act, Indian Penal Code, etc). For instance, in the case of threats to national security, commission of cognisable offences, etc, a notice and take-down regime should be appropriate. This would enable such

claims to be dealt with expeditiously and prevent damage. Even in the event executive action is found necessary in extreme cases (say involving terror threats), there must be judicial cognisance of the action within a specified time, failing which the attempts to censor must stop. In case of copyright, defamation and obscenity-related claims, there is no reason for a different standard to be applied compared to traditional methods of dissemination of information. It would therefore be appropriate if any complaints received are put through a judicial process prior to censorship. In any event, damages in such situation are likely to be monetary and as such any small delay occasioned by having to take the matter to court would not unduly harm the parties involved (especially as courts are empowered to grant injunctive relief). Such a system would also reduce false claims, and ensure intermediaries are safe from having to make tough decisions about matters they cannot be expected to have expertise in.

(d) Provision of information regarding instances of censorship is a must and therefore judicial and government authorities are best suited to adjudicate on instances where censorship is required. Placing the onus of policing the internet on private intermediaries is clearly impractical and inefficient in the long run.

(e) Merely blocking content is an impractical and unrealistic method to crack down on internet crimes.

NOTES

1 The Information Technology Act, 2000, in Section 2(1)(w) defines an intermediary as "with respect to any particular electronic record, a person who on behalf of another, receives, stores, or transmits that record or provides any services with respect to that record" and specifically includes internet service providers, cybercafes, blog sites and search engines.

2 This is known as a "good Samaritan" clause.

3 Matt Zimmerman, "Freedom of Expression, Indirect Censorship and Liability for Internet Intermediaries", presentation at the Trans-Pacific Partnership Stakeholders Forum, Chile, 15 February 2011, https://www.eff.org/files/filenode//EFF%20presentation%20ISPs%20and%20Freedom%20of%20Expression.pdf, visited on 23 January 2010.

4 *Avnish Bajaj vs State*, 3 Comp. Law Jou. 364 (Del 2005).

5 The definition of an intermediary was also made more explicit with this amendment.

6 Due primarily to (a) the ambiguous nature of the due diligence requirement, (b) no clarity on what was meant by "actual knowledge" and the obligations this would impose on an intermediary, (c) lack of clarity regarding what constitutes altering, modifying information, etc.

7 Not a violation under the IPC.

8 *Agricultural Market Committee vs Shalimar Chemical Works* (1997)5 SCC 516.