

# CIS Para-wise Comments on Intermediary Due Diligence Rules, 2011

*Centre for Internet and Society* | 2011-02-25

Pranesh Prakash

*On February 7th 2011, the Department of Information Technology, MCIT published draft rules on its website (The Information Technology (Due diligence observed by intermediaries guidelines) Rules, 2011) in exercise of the powers conferred by Section 87(2)(zg), read with Section 79(2) of the Information Technology Act, 2000. Comments were invited from the public before February 25th 2011.*

---

## **A. General Objections**

A number of the provisions under these Rules have no nexus with their parent provision, namely s.79(2). Section 79(1) provides for exemption from liability for intermediaries. Section 79(2) thereupon states:

79. Intermediaries not to be liable in certain cases—

(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 hosted; 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.

Therefore, by not observing any of the provisions of the Rules, the intermediary opens itself up for liability for actions of its users. However, many of the provisions of the Rules have no rational nexus with due diligence to be observed by the intermediary to absolve itself from liability.

## **B. Specific Objections**

### **Rule 2(b), (c), and (k)**

(b) “Blog” means a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Usually blog is a shared on-line journal where users can post diary entries about their personal experiences and hobbies;

(c) “Blogger” means a person who keeps and updates a blog;

(k) “User” means any person including blogger who uses any computer resource for the purpose of sharing information, views or otherwise and includes other persons jointly participating in using the computer resource of intermediary

### **Comments**

It is unclear why it is necessary to specifically target bloggers as users, leaving out other users such as blog commenters, social network users, microbloggers, podcasters, etc. It makes the rules technologically non-neutral.

### **Recommendation**

We recommend that these 3 sub-rules be deleted.

## Rule 3(2)

**3. Due Diligence observed by intermediary.**— The intermediary shall observe following due diligence while discharging its duties.

(2) The intermediary shall notify users of computer resource not to use, display, upload, modify, publish, transmit, update, share or store any information that : —

- (a) belongs to another person;
- (b) is harmful, threatening, abusive, harassing, blasphemous, objectionable, defamatory, vulgar, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically or otherwise 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) discloses sensitive personal information of other person or to which the user does not have any right to;
- (g) causes annoyance or inconvenience or deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
- (h) impersonate another person;
- (i) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
- (j) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation.

## Comments

Firstly, such ‘standard’ terms of use [^1] might make sense for one intermediary, but not for all. For instance, an intermediary such as site with user-generated content (e.g., Wikipedia) would need different terms of use from an intermediary such as an e-mail provider (e.g., Hotmail), because the kind of liability they accrue are different. This is similar to how the liability that a newspaper publisher accrues is different from that accrued by the post office. However, forcing standard terms of use negates this difference. Thus, these are impractical.

Secondly, read with the legal obligation of the intermediary to remove such information (contained in rule 3(3)), they vest an extraordinary power of censorship in the hands of the intermediary, which could easily lead to the stifling of the constitutionally guaranteed freedom of speech online. Analogous restrictions do not exist in other fields, e.g., against the press in India or against courier companies, and there is no justification to impose them on content posted online. Taken together, these provisions make it impossible to publish critical views about anything without the risk of being summarily censored.

Thirdly, while it is possible to apply Indian law to intermediaries, it is impracticable to require all intermediaries (whether in India or not) to have in their terms of use India-specific clauses such as rule 3(2)(j). Instead, it is better to merely require them to ask their users to follow all relevant laws.

Individual instances of how these rules are overly broad are contained in an appendix to this submission.

## Recommendation

We strongly recommend the deletion of this sub-rule, except clause (e).

### Rule 3(3)

(3) The intermediary shall not itself host or publish or edit or store 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).

## Comments

This sub-rule is ultra vires s.79 of the IT Act, which does not require intermediaries not to “host or publish or edit or store any information”. In fact, s.79(2) merely states that by violating the provisions of s.79(2), the intermediary loses the protection of s.79(1). It does not however make it unlawful to violate s.79(2), as rule 3(3) does. This makes rule 3(3) ultra vires the Act.

## Recommendation

This sub-rule should be deleted.

### **Rule 3(4)**

(4) The intermediary upon obtaining actual knowledge by itself or been brought to actual knowledge by an authority mandated under the law for the time being in force in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act expeditiously to work with user or owner of such information to remove access to such information that is claimed to be infringing or to be the subject of infringing activity. Further the intermediary shall inform the police about such information and preserve the records for 90 days

### **Comments**

This rule is also ultra vires s.69A of the IT Act as well as the Constitution of India. Section 69A states all the grounds on which an intermediary may be required to restrict access to information [^2]. It does not allow for expansion of those grounds, because it has been carefully worded to maintain its constitutional validity vis-a-vis Articles 19(1)(a) and 19(2) of the Constitution of India. The rules framed under s.69A prescribe an elaborate procedure before such censorship may be ordered. The rules under s.69A will be rendered nugatory if any person could get content removed or blocked under s.79(2).\*\*\*\*

This rule requires an intermediary to immediately take steps to remove access to information merely upon receiving a written request from “any authority mandated under the law”. Thus, for example, any authority can easily immunize itself from criticism on the internet by simply sending a written notice to the intermediary concerned. This is directly contrary to, and completely subverts the legislative intent expressed in Section 69B which lays down an elaborate procedure to be followed before any information can be lawfully blocked.

If any person is aggrieved by information posted online, they may seek their remedies—including the relief of injunction—from courts of law, under generally applicable civil and criminal law. Inserting a rule such as this one would take away the powers of the judiciary in India to define the line dividing permissible and impermissible speech, and vest it instead in the whims of each intermediary. This can only have a chilling effect on debates in the public domain (of which the Internet is a part) which is the foundation of any democracy.

### **Recommendation**

This rule should be modified so that an intermediary is obliged to take steps towards removal of content only when (a) backed by an order from a court or (b) a direction issued following the procedure prescribed by the rules framed under Section 69A.

### **Rule 3(5) & (7) & (8) & (10)**

(5) The Intermediary shall inform its users that in case of non-compliance with terms of use of the services and privacy policy provided by the Intermediary, the Intermediary has the right to immediately terminate the access rights of the users to the site of Intermediary;

(7) The intermediary shall not disclose sensitive personal information;

(8) Disclosure of information by intermediary to any third party shall require prior permission or consent from the provider of such information, who has provided such information under lawful contract or otherwise;

(10) The information collected by the intermediary shall be used for the purpose for which it has been collected.

### **Comments**

These sub-rules have no nexus with intermediary liability or non-liability under s.79(2). For instance, it is unreasonable to say that an intermediary may be held liable for the actions of its users if it does not inform its users about its right to terminate access by the user to its services. Furthermore, not all intermediaries need be websites, as sub-rule 5 assumes. An intermediary can even be an “internet service provider” or a “cyber cafe” or a “telecom service provider”, as per rule 2(j) read with s.2(1)(w) of the IT Act.

The requirements under sub-rules (7), (8), and (10) are rightfully the domain of s.43A and the rules made thereunder, and not s.79(2) nor these rules.

### **Recommendation**

These sub-rules should be deleted, and sub-rules (7), (8), and (10) may placed instead in the rules made under s.43A.

### **Rule 3(9)**

(9) Intermediary shall provide information to government agencies who are lawfully authorised for investigative, protective, cyber security or intelligence activity. The information 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 written request stating clearly the purpose of seeking such information.

### **Comments**

This provision is ultra vires ss.69 and 69B. Rules have already been issued under ss.69 and 69B which stipulate the mechanism and procedure to be followed by the government for interception, monitoring or decrypting information in the hands of intermediaries. Thus under the Interception Rules 2009 framed under

Section 69, permission must first be obtained from a “competent authority” before an intermediary can be directed to provide access to its records and facilities. The current rule completely removes the safeguards contained in s.69 and its rules, and would make intermediaries answerable to virtually any request from any government agency. This is contrary to the legislative intent expressed in Section 69.

### **Recommendation**

We recommend this sub-rule be deleted.

### **Rule 3(12)**

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

### **Comments**

The rules relating to how and when the Indian Computer Emergency Response Team may request for information from intermediaries is rightfully the subject matter of s.70B(5) [3] and the rules made thereunder by virtue of the rule making power granted by s.87(2)(yd). The subject matter of rule 3(12) is not liability of intermediaries for third-party actions, hence there is no nexus between the rule-making power, and the rule.

### **Recommendations**

We recommend that this sub-rule be deleted.

### **Rule 3(14)**

(14) The intermediary shall publish on its website the designated agent to receive notification of claimed infringements.

### **Comments**

It is unclear what “infringements” are being referred to in this sub-rule. Neither s.79 nor these rules provide for “infringements”. The same reasoning applied for rule 3(4) would also apply here. It would be better to require the intermediary to publish on its website a method of providing judicial notice.

### **Recommendations**

Delete, and replace with a requirement for the intermediary to publish on its website a method of providing judicial notice.\*\*\*\*

### **Footnotes**

1. For instance, the Section B(1) of the World of Warcraft Code of Conduct “When engaging in Chat, you may not: (i) Transmit or post any content or

language which, in the sole and absolute discretion of Blizzard, is deemed to be offensive, including without limitation content or language that is unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, hateful, sexually explicit, or racially, ethnically or otherwise objectionable.

2. It is only “in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above” that intermediaries may be issued directions to block access to information.
3. 70B(5) states that the The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.