



**Counter-proposal by the Centre for Internet and
Society: Draft Information Technology
(Intermediary Due Diligence and Information
Removal) Rules, 2012**

Contents

1. Rationale for counter-proposal
2. Text of counter-proposal by the Centre for Internet and Society: Draft Information Technology (Intermediary Due Diligence and Information Removal) Rules, 2012 along with rationale and explanatory text
3. Text of counter-proposal with explanatory text

Rationale for counter-proposal

Important principles for limiting free expression:

Any restriction on freedom of speech should embody and be guided by the following principles, as identified by the UN Special Rapporteur on Freedom of Opinion and Expression:

- legitimacy of purpose
- necessity of limitation
- proportionality of limitation
- predictability of restriction
- transparency of censorship
- natural justice and due process

Main problems with existing rules:

1. Creating a new standard for content removal incompatible with Indian law.

Under Indian law, **published material can ordinarily only be removed subsequent to a court order or an executive order**. These rules, however, require intermediaries to remove material within 36 hours of a complaint, **without a court or an executive finding of illegality**.

2. Shifting of blame from offending users to intermediaries.

It makes the 'intermediary', including ISPs like BSNL and Airtel responsible for objectionable content that their users have put up. This kind of 'vicarious' liability is only normally created for extreme situations like the Bhopal Gas tragedy. Because of this shift of blame that could take place if they don't remove anything that is complained about within 36 hours, **intermediaries resort to over-censoring of even legitimate content**.

3. Intermediary has to judge content instead of courts or tribunals.

Under the current rules, the **intermediaries have to judge whether the complaint is valid** and correctly identifies content declared unlawful under Rule 3(2) of the Information Technology (Intermediaries Guidelines) Rules 2011. Intermediaries are neither legally equipped to make that judgment, nor should they be tasked with making that call: **decisions on legality of content should only be made by a judicial or quasi-judicial authority that records its decisions in speaking orders**. Even in the recently-amended Copyright Act, a court order is required to follow a complaint to an intermediary about copyright infringement. When intermediaries are asked to decide on unlawfulness, they tend to over-censor (as shown by CIS research).

4. No chance given to defend legitimate content, no due process.

The current rules allow **allegedly offensive content to be removed even without informing the user who uploaded that content, and without giving the user any chance to defend the content's legality**. So, even material put up by a political party can be removed based on *anyone's* complaint, without telling that party. This was done against a site called "CartoonsAgainstCorruption.com". This goes against Article 19(1)(a) of our constitution which guarantees the right to freedom of speech and expression.

5. No proportionality.

A DNS provider (i.e., the person who gives you your web address) is an intermediary who can be asked to **'disable access' to a website on the basis of a single offensive page, even though the rest of the site has nothing objectionable**. The Rules do not prevent this from happening.

6. Lack of transparency.

No information is required to be provided that content has been removed. It's a black-box system, with no one, not even the government, knowing that content has been removed following a request. **Currently, even the government does not know how many web pages have been removed after these Rules have come into effect.**

7. No differentiation between intermediaries.

A one-size-fits-all system is followed where an e-mail provider is equated with an online newspaper, which is equated with a video upload site, which is equated with a search engine. This is like **equating the post office and a magazine editor as being equivalent for defamatory speech**, even though post office doesn't know the content of the defamatory speech it carries and a magazine editor would. This is a **violation of Article 14** of the Constitution, which requires that unequals be treated unequally by the law.

8. Vague and unconstitutional requirements.

"Disparaging speech", as long as it isn't defamatory, is not criminalised in India, and can't be criminalised because the Constitution does not allow for it. Still, that is an example of **perfectly legal content that is treated as unlawful content under the Intermediaries Guidelines Rules**. Content "relating to gambling" in print is not unlawful, but now all Internet intermediaries are required to remove any content that promotes gambling.

9. Allows private censorship.

The Rules allow **any person to get content removed based on a mere complain without proof of an illegal act having been committed (as is required by s.79 of the IT Act)**. There are no safeguards to prevent this from happening. In fact, intermediaries are provided an incentive to over-censor. **If an intermediary resists any complaint for being false, frivolous, etc., it risks losing the immunity provided by s.79 of the IT Act.**

10. Presumption of illegality.

The Rules are based on the **presumption that all complaints (and resultant mandatory taking down of the content) are correct**, and that the incorrectness of the take-downs can be disputed in court (if the user discovers on her own that the content has been removed). This is contrary to the presumption of validity of speech used by Indian courts, and is akin to prior restraint on speech. Courts have held that for content such as defamation, prior restraints cannot be put on speech, and that civil and criminal action can only be taken post-speech.

11. Government censorship, not 'self-regulation'.

The Rules require all intermediaries (presumably all over the world, since the IT Act states that it has extraterritorial applicability) to change their terms of service in conformance with Rule 3(2). The DIT says these are industry best-practices in existing terms of service agreements (see DIT press release on May 11, 2011 titled 'Exemption from Liability for Hosting Third Party Information: Diligence to be Observed under Intermediary Guidelines Rules'). **It is 'self-regulation' only if a company chooses the terms of its terms of service agreement, and 'government regulation' if the government dictates those terms of service.** Thus, the DIT is quite clearly wrong in stating, "rules do not provide for any regulation or control of content by the Government".

Proposed changes

1. Same basic standard as offline content, but with suitable modifications

The proposed rules require material to be removed without court orders in some cases (see Rules 7 and 8) and require court orders in all other cases (see Rules 6, 9, and 10.) In some cases, material may be removed for up to 6 months without court orders, but will need to be put back up if no court order is forthcoming. (See Rules 6 and 10.) Lastly, the rules allow intermediaries to remove material without court orders if the material violates their terms of service. (See Rule 11.)

2. Intermediaries generally not liable for users' actions

The proposed rules ensure that unless the intermediary refused to remove information despite having actual knowledge of the commission of an unlawful act, or actually contributed to that unlawful act, it would not be liable for the acts of its users. (See Rules 6, 7, 8, 9, 10, and Rule 2(1)(f) read with .)

3. Intermediary does not exercise subjective judgment on lawfulness of content

Under the proposed rules, the intermediary does not have to exercise its judgment about the lawfulness of the content. It is only required to remove it based on objective tests. If it decides to remove certain content despite not being required to, it may do so, but will have to provide reasons to back up its decisions to prevent arbitrary misuse of powers (see Rule 11).

4. Users given an opportunity to defend legitimate content

The revised rules allow users whose content is complained about to choose to defend it. If the user chooses to contest a complaint (via a "counter-notice"), they are agreeing to potentially face a legal battle, but with the effect that the intermediary will be required to keep the contested content up. This way both sides will be represented. (See Rules 6 and 10.)

5. Principle of proportionality

Under the proposed rules, a DNS provider (i.e., the person who gives you your web address) cannot be asked to 'disable access' to a website on the basis of a single page, even though the rest of the site has nothing objectionable. (See Rules 5(2) and 5(3).)

6. Transparency around censorship

Under the proposed rules, the user whose content is sought to be removed will always have to be informed about any complaint received by the intermediary, as will the public (via DIT). If content is removed under these rules, the complainant, the user whose content is removed, and the public (via DIT) will have to be notified about any information that is removed. (See Rule 11.) This will allow for the monitoring of the usage of the rules to see if they are being abused or not.

7. Differentiating between intermediaries

The proposed rules treat each kind of intermediary as a separate class (see Rule 3), and prescribes different content removal requirements for them. (See Rules 6-10.)

8. Vague and unconstitutional requirements

Instead of asking intermediaries to prohibit certain classes of information by amending their terms of service, the proposed rules merely require them to remove information that is being used to commit unlawful acts. (See Rules 6-10.) This is the same test as in S.79 of the Information Technology Act, and we believe it is a good test.

9. Lessens the chances of private censorship

Our proposed rules do not rule out private censorship, but they do make it slightly more difficult. In the proposed rules, intermediaries do not have an incentive to remove content, as they do under the current Intermediary Guidelines Rules. Under the current Rules, intermediaries will have to risk liability if they don't remove content that is complained about, as they can be said to have had "actual knowledge" of an unlawful act.

10. Presumption of legality

The proposed rules make it the job of the complainants to show that the content they're complaining about is either illegal or against the terms of service of the intermediary. Thus speech is presumed legal until shown otherwise.

11. Limited government regulation, not 'self-regulation'

Unlike the current Intermediary Guidelines Rules, the proposed rules do not require any intermediary to modify its terms of service.

Text of counter-proposal by the Centre for Internet and Society: Draft Information Technology (Intermediary Due Diligence and Information Removal) Rules, 2012

In exercise of the powers conferred by sub-section (1) of section 87 and clause (zg) of sub-section (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (Central Act XXI of 2000), the Central Government hereby prescribes the following rules, namely: —

1. Short title and commencement. — (1) These rules may be called the Information Technology (Intermediary Due Diligence and Information Removal) Rules, 2012.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions. — (1) In these rules, unless the context otherwise requires, —

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Communication link" means a uniform resource identifier;

(c) "Host" with all its grammatical variations and cognate expressions means to store information or communication links and other activities allied to storage, including, but not limited to, appending programming language syntax, applying filters, adding interactive features, replicating and transmitting, but not including any function which modifies the information or communication link contained therein.

Provided that an intermediary that has most direct control over the use of or access to a uniform resource identifier shall be deemed to be the hosting service for such information or communication link, even if it subcontracts the hosting of the information or communication link reached by using that uniform resource identifier to another intermediary.

(d) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(e) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act and, for the purposes of these rules only, intermediaries shall be of the classes set out in rule 3;

(f) "Modify" with all its grammatical variations and cognate expressions means to alter the integrity of information either by exercise of substantial human editorial control or, with respect to a legal proceeding or claim, if the alteration ipso facto causes an injury that is the subject matter of the legal proceeding or claim;

(g) "Intermediate", in relation to storing of information, means the storing of information in the course of transmission;

(h) "Transient", in relation to storing of information, means storing that is temporary and for a period that is not beyond the time that is reasonably necessary for transmission;

(i) "User" means any person who accesses or uses any computer resource of an intermediary if that intermediary, on behalf of that person, receives or stores or transmits an electronic record, or provides any service to that person with respect to an electronic record.

(j) "Third party provider of information" means a user who has provided the information or communication link that the intermediary hosts or make available;

Provided that if the the information under contention is the outcome of partial information provided by many users, then for the purpose of filing a counter-notice in response to a complaint, only such users specifically denying the unlawfulness of the entire information will be treated as the "third party provider of information".

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Classes of intermediaries. — (1) In these rules, intermediaries shall be of the following classes —

(a) "Hosting services" that host information at the direction of a user, and include, but are not limited to, social networking websites that host user information at the direction of its users, video sharing websites that host videos at the direction of its users, blogging websites that host blogs at the direction of a third party blogger, newspaper websites that host reader comments on news articles at the direction of the reader, e-commerce websites that host product or service details at the direction of the seller.

(b) "Information location services" that make available or host communication links and any information incidental to such communication links for the sole purpose of locating information, and include, but are not limited to, search engines and directories.

(c) "Caching services" that store information for the sole purpose of making the onward transmission of such information more efficient, on the condition that (i) such storing is automatic, intermediate and temporary; (ii) the intermediary does not modify the information contained therein; and (iii) the intermediary complies with conditions on access to the information.

(d) "Access providers" that provide access to a computer network, or transmit information over a computer network at the direction of a user, if the intermediary does not

(i) initiate the transmission;

(ii) select the receiver of the transmission;

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

(iv) store the information or communication link contained in the transmission with the exception of automatic, intermediate and transient storing for the sole purpose of such transmission and with the exception of storing as may be mandated under the Act.

(e) "Residuals", which are intermediaries that are not in the classes of hosting services, information location services, caching services, or access providers.

4. Due diligence by intermediaries. — (1) All intermediaries shall observe the following due diligence while discharging their duties, namely —

(a) The intermediary shall prominently display and publish a privacy policy, and terms and conditions of use of the intermediary's computer resource by any person.

(b) The intermediary shall prominently display and publish the name, address or other contact details of the person or authority to which a complaint made under rule 5 is to be preferred.

(c) The intermediary shall not disclose information identifying a user to a third party who does not have access to such information unless required to do so by any law for the time being in force.

(d) The intermediary shall not modify any information or communication link provided by a third party provider of information.

(2) Without prejudice to the generality of the provisions of sub-rule (1) of this rule, an intermediary shall observe the following additional class-specific due diligence requirements while discharging its duties, namely —

(a) An information location service shall comply with prevailing industry standards pertaining to information location services;

(b) A caching service shall comply with industry standards regarding periodic updating of information.

(3) Notwithstanding the provisions of sub-rule (1) and sub-rule (2) of this rule, there shall not be any general obligation on the intermediary to monitor information or communication links, or to seek facts and circumstances indicating illegal activity on the intermediary's computer networks or computer resources.

5. Complaints. — (1) Any person aggrieved by any information or communication link made available or hosted by an intermediary may prefer a complaint to that intermediary in the form and manner prescribed in Form I.

(2) A complaint for removal of information or communication link under sub-rule (1) should only be preferred to the intermediary with most direct control of the information or communication link such that there is no undue removal of or restriction of access to any lawful information or communication link sought to be removed; provided that any subsidiary or sister concerns of an intermediary shall also be deemed to be the intermediary for the purpose of preferring the complaint under sub-rule (1).

(3) Upon receipt of a complaint for removal of information or communication link under sub-rule (1) by an intermediary that does not have the most direct control of the information or communication link as under sub-rule (2), the intermediary shall immediately respond to the complainant explaining why the complaint to it has been incorrectly preferred, and shall inform the complainant of name, address and contact details of the intermediary to whom the complaint should be preferred under sub-rule (2) to the best of its knowledge.

6. Removal of information by hosting services. — (1) Upon receipt by a hosting service of a complaint for removal of any information being used to commit an unlawful act, it shall immediately provide a copy of the complaint to the third party provider of the information to which the complaint pertains.

(2) The third party provider of the information to which the complaint pertains may prefer a counter-notice in the form and manner prescribed in Form II within forty-eight hours of the receipt of a copy of the complaint where the complaint pertains to any information that was first hosted or last modified within a period of seven days immediately preceding the date of the complaint, and within fourteen days of the receipt of a copy of the complaint where the complaint pertains to any other information.

(3) Upon receipt of a counter-notice by an intermediary under sub-rule (2) of this rule, the intermediary shall immediately provide a copy of the counter-notice to the person who preferred the complaint.

(4) Subject to sub-rules (5) and (6) of this rule, a hosting service shall receive actual knowledge of the unlawfulness of the act only when —

(a) the third party provider of the information accepts the unlawfulness of the act to which the complaint pertains;

or

(b) the intermediary does not receive a counter-notice in conformance with sub-rule (2) of this rule from the third party provider of the information.

(5) Notwithstanding anything contained in this rule, the actual knowledge of the unlawfulness of any act shall lapse if the complainant under this rule fails to obtain, within a period of one hundred and eighty days, a determination of a court of competent jurisdiction as to the unlawful act to which the complaint pertains.

(6) Notwithstanding anything contained in this rule, the actual knowledge of the unlawfulness of any act shall lapse if the third party provider of the information to which the complaint pertains prefers a counter-notice within sixty days of receipt of a copy of the complaint.

(7) Upon receipt of actual knowledge of the unlawfulness of any act or upon receipt of a notification by the appropriate Government under clause (b) of sub-section (3) of section 79 of the Act, a hosting service shall remove the information to which such actual knowledge or notification pertains.

Provided that, in relation to the intermediary, if the actual knowledge of the unlawfulness of any act using any information lapses under sub-rules (5) and (6) of this rule, the intermediary shall immediately restore such removed information.

7. Removal of communication links by information location services. — (1) An information location service shall receive actual knowledge of the commission of unlawful act using any communication link only upon receipt of a complaint accompanied by proof that the information to which the communication link points has been removed or that a court of competent jurisdiction has ordered its removal.

(2) Upon receipt of actual knowledge of the commission of an unlawful act using any communication link or upon receipt of a notification by the appropriate Government under clause (b) of sub-section (3) of section 79 of the Act, an information location service shall remove the communication link and any incidental information to which such actual knowledge or notification pertains.

8. Removal of information by caching services. — (1) A caching service shall receive actual knowledge of the commission of an unlawful act using any information only upon receipt of a complaint accompanied by a written notification that the information for which transmission is sought to made more efficient has been removed or that a court of competent jurisdiction has ordered its removal.

(2) Upon receipt of actual knowledge of the commission of an unlawful act using any information or upon the receipt of a notification by the appropriate Government under clause (b) of sub-section (3) of section 79 of the Act, a caching service shall remove the information to which such actual knowledge or notification pertains.

9. Removal of information by access providers. — (1) An access provider shall receive actual knowledge of the commission of an unlawful act using any information or communication link only upon receipt of a complaint accompanied by an order by a court of competent jurisdiction requiring it to restrict access to such information.

(2) Upon receipt of actual knowledge of the commission of an unlawful act using any information or communication link or upon receipt of a notification by the appropriate Government under clause (b) of sub-section (3) of section 79 of the Act, an access provider shall remove the information or communication link to which such actual knowledge or notification pertains.

10. Removal of information by residuals. — An intermediary of the class “residuals” shall be treated as a hosting service for the purpose of removal of any information or communication link being used to commit an unlawful act.

11. Removal of information due to complaint of violation of terms and conditions of use. — An intermediary of any class may, upon receipt of a complaint under rule 5 and without receipt of actual knowledge, remove any information that is made available or hosted by it if it feels in good faith that such information is in violation of its terms and conditions of use.

12. Transparency and record-preservation. — (1) Upon the receipt of a complaint under rule 5, the intermediary shall provide a copy of the complaint to the Designated Officer under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

(2) In all cases where any information is removed by an intermediary under rules 6, 7, 8, 9, 10, or 11, the intermediary shall notify the Designated Officer under the Information Technology (Procedure and Safeguards for Blocking for Access of

Information by Public) Rules, 2009, the complainant, if any, and the third party provider of the information that has been removed about the fact of removal of information, and provide them the uniform resource identifier of the removed information and a brief description of the removed information, and the complaint.

(3) In the case where the information is removed under rule 11, the intermediary shall provide the Designated Officer under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009, the complainant, if any, and the third party provider of the information that has been removed, with reasons for holding such information to be in violation of its terms and conditions of use.

(4) The Designated Officer under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009 shall maintain a publicly-accessible website that catalogues all the information received under this rule, with personally identifiable information about the complainant and third party provider of information being redacted.

(5) In all cases where any information is removed or access restricted by an intermediary under rules 6, 7, 8, 9, 10, or 11 the intermediary shall preserve the removed information and associated records for at least one hundred and eighty days.

13. Relevance of due diligence on removal requirements — For the purposes of any legal proceeding or claim against an intermediary for any third party information or communication link made available or hosted by such intermediary, the exemption from liability under section 79 of the Act shall not be waived for failure to observe any due diligence or removal requirements under rules 4, 6, 7, 8, 9 or 10 unless such failure bears a reasonable nexus to the prevention of an injury that is the subject matter, or the redress, of such legal proceeding or claim.

A. Details of complainant or representative

1. Name of complainant: _____

1A. If representative of a complainant,
Name of representative: _____

2. Address: _____

3. Telephone: _____

4. Mobile: _____

5. Email: _____

B. Details of unlawful act being complained about

6. Specific identification of every instance of the information or communication link sought to be removed:
URI: _____

7. The detailed allegation of the commission of the unlawful using the information or communication link being complained about, with *prima facie* proof of the commission of the alleged unlawful act:

C. Court order

8. In all cases where the Rules require the submission of a court order, certified copy of the court order:

D. Sworn statement

9. I am not wilfully misrepresenting any facts or averments in this complaint. If any part of this complaint is later proved to be an act of wilful misrepresentation, then I will compensate the intermediary and the third party provider of information or communication link for the damages caused as a result of the complaint or the consequent removal of the information or communication link under contention.

(Signature)
Name, Date, Address

Form II – Counter-notice

[See Rule 6(2)]

A. Details of denial or acceptance of complaint

1. Specific denial or acceptance of all averments and statements in the complaint:

B. Sworn statement

2. I am not wilfully misrepresenting any facts or assertion in this counter-notice. If any part of this counter-notice is later proved to be an act of wilful misrepresentation, then I will compensate the intermediary and the complainant for the damages caused as a result of the hosting or making available of the information or communication link under contention.

(Signature)

Name or online alias, date, address

Counter-proposal with explanatory text

Rule	Proposed rules	Explanation
Preamble	In exercise of the powers conferred by sub-section (1) of section 87 and clause (zg) of sub-section (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (Central Act XXI of 2000), the Central Government hereby prescribes the following rules, namely: —	It is proposed that these rules be notified under s.87(1) in addition to s.87(2)(zg) of the Information Technology Act (“Act”) as the the requirement for removal of information cannot be derived from s.79(2), which is restricted to prescription of due diligence and other guidelines.
1	<p>1. Short title and commencement. — (1) These rules may be called the Information Technology (Intermediaries) Rules, 2012.</p> <p>(2) They shall come into force on the date of their publication in the Official Gazette.</p>	The rules have been renamed “Information Technology (Intermediaries) Rules”, given that they don’t deal only with guidelines for intermediaries to follow, but also provide a content removal system.
2	2. Definitions. — (1) In these rules, unless the context otherwise requires, —	
2 (1) (a)	(a) "Act" means the Information Technology Act, 2000 (21 of 2000);	
2 (1) (b)	(b) "Communication link” means a uniform resource identifier;	
2 (1) (c)	<p>(c) "Host" with all its grammatical variations and cognate expressions means to store information or communication links and other activities allied to storage, including, but not limited to, appending programming language syntax, applying filters, adding interactive features, replicating and transmitting, but not including any function which modifies the information or communication link contained therein.</p> <p>Provided that an intermediary that has most direct control over the use of or access to a uniform resource identifier shall be deemed to be the hosting service for such information, even if it contracts the hosting of the information reached by using that uniform resource identifier to another intermediary.</p>	<p>1) It is proposed that the definition of “Hosting” be added to clarify that modifications of a technical nature are included within the scope of hosting.</p> <p>2) The proviso ensures that the intermediary most directly linked with the hosting is deemed to be the host, as it is in the best position to resolve any dispute with regard to the hosted content.</p>
2 (1) (d)	(d) “Information” means information as defined in clause (v) of sub-section (1) of section 2 of the Act;	Note that “data” is a subset of information, as per s.2(1)(v) of the Act.
2 (1) (e)	(e) “Intermediary” means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act and, for the purposes of these rules only, intermediaries shall be of the classes set out in rule 3;	The five classes are: (i) information location services (e.g., search engines), (ii) caching services (e.g., content delivery networks like Akamai) , (iii) hosting services (e.g. Youtube, Facebook), (iv) access providers (e.g. ISPs), and (v) residual.
2 (1) (f)	(f) "Modify" with all its grammatical variations and cognate expressions means to alter the integrity of information either by exercise of substantial human editorial control or, with respect to a legal proceeding or claim, if the alteration ipso facto causes an injury that is the subject matter of	Alterations such as appending headers to packets or appending advertisements

	the legal proceeding or claim;	should not be construed as modification.
2 (1) (e)	(e) "Intermediate", in relation to storing of information, means the storing of information in the course of transmission;	This definition has been adopted from the Electronic Commerce (EC Directive) Regulations 2002 (UK).
2 (1) (g)	(g) "Transient", in relation to storing of information, means storing that is temporary and for a period that is not beyond the time that is reasonably necessary for transmission;	This definition has been adopted from the Electronic Commerce (EC Directive) Regulations 2002 (UK).
2 (1) (h)	(h) "User" means any person who accesses or uses any computer resource of an intermediary if that intermediary, on behalf of that person, receives or stores or transmits an electronic record, or provides any service to that person with respect to an electronic record.	This definition has been adapted from the definition of 'intermediary' contained in s.2(1)(w) of the Act.
2 (1) (i)	(i) "Third party provider of information" means a user who has provided the information or communication link to an intermediary; provided that if the the information under contention is the outcome of partial information provided by many users, then for the purpose of filing a counter-notice in response to a complaint, only such users specifically denying the unlawfulness of the entire information will be treated as the "third party provider of information".	
2 (2)	(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.	
3 (1)	3. Classes of intermediaries. — (1) In these rules, intermediaries shall be of the following classes —	This classification of intermediaries is influenced by the classifications in: a) Directive 2000/31/EC on electronic commerce, in the EU; b) the Digital Millennium Copyright Act, 2000 of the USA.
3 (1) (a)	(a) "Hosting services" that host information at the direction of a user, and include, but are not limited to, social networking websites that host user information at the direction of its users, video sharing websites that host videos at the direction of its users, blogging websites that host blogs at the direction of a third party blogger, newspaper websites that host reader comments on news articles at the direction of the reader, e-commerce websites that host product details at the direction of the seller.	
3 (1) (b)	(b) "Information location services" that make available or host communication links and any information incidental to such communication links for the sole purpose of locating information, and include, but are not limited to, search engines and directories.	
3 (1) (c)	(c) "Caching services" that store information for the sole purpose of making the onward transmission of such information more efficient, on the condition that (i) such storing is automatic, intermediate and temporary; (ii) the intermediary does not modify the information contained therein; and (iii) the intermediary complies with conditions on access to the information.	
3 (1) (d)	(d) "Access providers" that provide access to a computer network, or transmit information over a computer network at the direction of a user, if the intermediary does not (i) initiate the transmission;	The phrase "automatic, intermediate and transient" is used to describe the storing of packets by an access provider

	<p>(ii) select the receiver of the transmission;</p> <p>(iii) select or modify the information contained in the transmission; and</p> <p>(iv) store the information contained in the transmission with the exception of automatic, intermediate and transient storing for the sole purpose of such transmission and with the exception of storing as may be mandated under the Act.</p>	<p>in a packet switched network. The relevant terms have been defined in the definitions clause.</p> <p>“Access providers” are referred to as “mere conduits” under Article 12 of Directive 2000/31/EC on electronic commerce in the EU.</p>
3 (1) (e)	<p>(e) "Residuals", which are intermediaries that are not in the classes of hosting services, information location services, caching services, or access providers.</p>	
4 (1)	<p>4. Due diligence by intermediaries. — (1) All intermediaries shall observe the following due diligence while discharging their duties, namely —</p> <p>(a) The intermediary shall prominently display and publish a privacy policy, and terms and conditions of use of the intermediary's computer resource by any person.</p> <p>(b) The intermediary shall prominently display and publish the name, address or other contact details of the person or authority to which a complaint made under rule 5 is to be preferred.</p> <p>(c) The intermediary shall not disclose information identifying a user to a third party who does not have access to such information unless required to do so by any law for the time being in force.</p> <p>(d) The intermediary shall not modify any information or communication link provided by a third party provider of information.</p>	<p>Intermediaries should be required to have:</p> <p>1) clear policies with regard to use of their resources or services.</p> <p>2) clear information on complaints mechanism</p> <p>3) a duty not to disclose the identity of pseudonymous or anonymous users unless legally required to do so.</p>
4 (2)	<p>(2) Without prejudice to the generality of the provisions of sub-rule (1) of this rule, an intermediary shall observe the following additional class-specific due diligence requirements while discharging its duties, namely —</p> <p>(a) An information location service shall comply with industry standards pertaining to information location services.</p> <p>(b) A caching service shall comply with industry standards regarding periodic updating of information.</p>	<p>Information location services are expected to comply with the robots.txt standard, and any future industry standards.</p>
4 (3)	<p>(3) Notwithstanding the provisions of sub-rule (1) and sub-rule (2) of this rule, there shall not be any general obligation on the intermediary to monitor information or communication links, or to seek facts and circumstances indicating illegal activity on the intermediary's computer networks or computer resources.</p>	<p>This is in line with Article 15 of the EU E-Commerce Directive. This is needed as a general obligation to monitor will over-burden intermediaries, and is impractical.</p>
5 (1)	<p>5. Complaints. — (1) Any person aggrieved by any information or communication link made available or hosted by an intermediary may prefer a complaint to that intermediary in the form and manner prescribed in Schedule I.</p>	
5 (2)	<p>(2) A complaint for removal of information or communication link under sub-rule (1) should only be preferred to the intermediary with most direct control of the information or communication link such that there is no undue removal of or restriction of access to any lawful information or communication link sought to be removed.</p> <p>Provided that any subsidiary or sister concerns of an intermediary shall also be deemed to be the intermediary for the purpose of preferring the complaint under sub-rule (1).</p>	<p>An intermediary that is not in direct control of the information complained about (for instance, a DNS provider or an ISP) should not be targetted when there is a more appropriate intermediary such as a host.</p>
5 (3)	<p>(3) Upon receipt of a complaint for removal of information or communication link under sub-rule (1) by an intermediary that does not have the most direct control of the information or communication link as under sub-rule (2), the intermediary shall immediately respond to the complainant</p>	<p>An intermediary should inform the complainant if it believes it is not the correct intermediary.</p>

	<p>explaining why the complaint has been incorrectly preferred, and shall inform the complainant of name, address and contact details of the intermediary to whom the complaint should be preferred under sub-rule (2) to the best of its knowledge.</p>	
6	<p>6. Removal of information by hosting services. — (1) Upon receipt by a hosting service of a complaint for removal of any information being used to commit an unlawful act, it shall immediately provide a copy of the complaint to the third party provider of the information to which the complaint pertains.</p> <p>(2) The third party provider of the information to which the complaint pertains may prefer a counter-notice in the form and manner prescribed in Schedule II within forty-eight hours of the receipt of a copy of the complaint where the complaint pertains to any information that was first hosted or last modified within a period of seven days immediately preceding the date of the complaint, and within fourteen days of the receipt of a copy of the complaint where the complaint pertains to any other information.</p> <p>(3) Upon receipt of a counter-notice by an intermediary under sub-rule (2) of this rule, the intermediary shall immediately provide a copy of the counter-notice to the person who preferred the complaint.</p> <p>(4) Subject to sub-rules (5) and (6) of this rule, a hosting service shall receive actual knowledge of the unlawfulness of the act only when —</p> <p>(i) the third party provider of the information accepts the unlawfulness of the act to which the complaint pertains; or</p> <p>(ii) the intermediary does not receive a counter-notice in conformance with sub-rule (2) of this rule from the third party provider of the information; or</p> <p>(iii) the intermediary is unable to contact the third party provider of the information to which the complaint pertains despite its best efforts.</p> <p>(5) Notwithstanding anything contained in this rule, the actual knowledge of the unlawfulness of any act shall lapse if the complainant under this rule fails to obtain, within a period of one hundred and eighty days, a determination of a court of competent jurisdiction as to the unlawful act to which the complaint pertains.</p> <p>(6) Notwithstanding anything contained in this rule, the actual knowledge of the unlawfulness of any act shall lapse if the third party provider of the information to which the complaint pertains prefers a counter-notice within sixty days of receipt of a copy of the complaint.</p> <p>(7) Upon receipt of actual knowledge of the unlawfulness of any act or upon receipt of a notification by the appropriate Government under clause (b) of sub-section (3) of section 79 of the Act, a hosting service shall remove the information to which such actual knowledge or notification pertains.</p> <p>Provided that, in relation to the intermediary, if the actual knowledge of the unlawfulness of any act using any information lapses under sub-rules (5) and (6) of this rule, the intermediary shall immediately restore such removed information.</p>	<p>A hosting service will remove information only if the third party provider of information either agrees to have it removed or does not respond to complaint. If the third party provider of information wishes to defend the content, then the hosting service shall not remove the information: the complainant can proceed directly against the third party provider of information.</p> <p>The hosting service has removed information for non-receipt of a response from the third party provider of information, it will restore the information after 180 days of removing if by that time there is no valid court order declaring it to be used to commit an unlawful act.</p>
7	<p>7. Removal of communication links by information location services. — (1) An information location service shall receive actual knowledge of the commission of unlawful act using any communication link only upon receipt of a complaint accompanied by proof that the information to which the communication link points, has been removed under sub-rule (7) of rule 6, or has been ordered to be removed by a court of competent jurisdiction.</p> <p>(2) Upon receipt of actual knowledge of the commission of an unlawful act using any communication link or upon receipt of a notification by the appropriate Government under clause (b) of sub-section (3) of section 79 of the Act, an information location service shall remove the communication link and any incidental information to which such actual knowledge or notification pertains.</p>	<p>Information location tools shall remove links only when the content that's linked-to has been removed or found to be unlawful.</p>
8	<p>8. Removal of information by caching services. — (1) A caching service shall receive actual knowledge of the commission of an unlawful act using any information only upon receipt of a complaint accompanied by a written</p>	<p>Caching services will remove information only when the original material has been</p>

	<p>notification that the information, for which transmission is sought to made more efficient has been removed or that a court of competent jurisdiction has ordered its removal.</p> <p>(2) Upon receipt of actual knowledge of the commission of an unlawful act using any information or upon the receipt of a notification by the appropriate Government under clause (b) of sub-section (3) of section 79 of the Act, a caching service shall remove the information to which such actual knowledge or notification pertains.</p>	removed or found unlawful.
9	<p>9. Removal of information by access providers. — (1) An access provider shall receive actual knowledge of the commission of an unlawful act using any information only upon receipt of a complaint accompanied by an order by a court of competent jurisdiction requiring it to restrict access to such information.</p> <p>(2) Upon receipt of actual knowledge of the commission of an unlawful act using any information or upon receipt of a notification by the appropriate Government under clause (b) of sub-section (3) of section 79 of the Act, an access provider shall restrict access to the information to which such actual knowledge or notification pertains.</p>	ISPs will restrict access to information only when directed to do so by a court.
10	<p>10. Removal of information by residuals. — An intermediary of the class “residuals” shall be treated as a hosting service for the purpose of removal of any information or communication link being used to commit an unlawful act.</p>	
11	<p>11. Removal of information due to complaint of violation of terms and conditions of use. — An intermediary of any class may, upon receipt of a complaint under rule 5 and without receipt of actual knowledge, remove any information that is made available or hosted by it if it feels in good faith that such information is in violation of its terms and conditions of use.</p>	
12	<p>12. Transparency and record-preservation. — (1) Upon the receipt of a complaint under rule 5, the intermediary shall provide a copy of the complaint to the Designated Officer under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.</p> <p>(2) In all cases where any information is removed by an intermediary under rules 6, 7, 8, 9, 10, or 11 the intermediary shall notify the Designated Officer under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009, the complainant, if any, and the third party provider of the information that has been removed about the fact of removal of information, and provide them the uniform resource identifier of the removed information and a brief description of the removed information, and the complaint.</p> <p>(3) In the case where the information is removed under rule 11, the intermediary shall provide the Designated Officer under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009, the complainant, if any, and the third party provider of the information that has been removed, with reasons for holding such information to be in violation of its terms and conditions of use.</p> <p>(4) The Designated Officer under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009 shall maintain a publicly-accessible website that catalogues all the information received under this rule, , with personally identifiable information about the complainant and third party provider of information being redacted.</p> <p>(5) In all cases where any information is removed by an intermediary under rules 6, 7, 8, 9, 10, or 11 the intermediary shall preserve the removed information and associated records for at least one hundred and eighty days.</p>	<p>The intermediary has to pass on a copy of all complaints to the DIT, which shall publish them with appropriate redactions.</p> <p>The intermediary has to inform the DIT, the complainant, and the person whose information has been removed, of the removal of information. The DIT shall publish this information with appropriate redactions.</p> <p>In case the removal was done without ‘actual knowledge’, for violation of terms and conditions of use, the intermediary shall clear reasons for the removal.</p>
13	<p>13. Relevance of due diligence on removal requirements — For the purposes of any legal proceeding or claim against an intermediary for any third party information or communication link made available or hosted by such intermediary, the exemption from liability under section 79 of the Act shall not be waived for failure to observe any due diligence or removal requirements under rules 4, 6 , 7, 8, 9 or 10 unless such failure bears a reasonable nexus to</p>	Example: Not having a “privacy policy” may not have a reasonable nexus with a legal claim of obscenity against the intermediary, so wouldn’t

	the prevention of the injury that is the subject matter of such legal proceeding or claim, or to the redress of such legal proceeding or claim.	make the the intermediary lose immunity from prosecution under s.79.
--	---	--