Intermediaries, users and the law – Analysing intermediary liability and the IT Rules

Software Freedom Law Center

Table of Contents

Intermediary liability and the IT Rules

The criminal complaint filed by a journalist in a Delhi Court against Google, Facebook and other internet companies has resulted in a debate on liability of these companies in respect of user generated content hosted by them. Earlier, Kapil Sibal, the Minister for Communications and Information Technology created a ruckus when he purportedly asked Internet companies like Google and Facebook to pre-screen offensive content.

In this debate, in addition to analysing the liability faced by these companies, it is important to understand how users could be affected by any legislation that seeks to regulate the conduct of these companies. The Internet has become a platform for sharing of information and ideas and it is important to preserve the free and open nature of the medium.

Who are intermediaries?

In discussions about internet companies, the word intermediary often finds mention. An understanding of this term is important as it is used extensively in the Information Technology Act, 2000, the legislation that governs the field in India.

Intermediaries are entities that provide services enabling the delivery of online content to the end user Let us look at the players involved in this chain:

Internet Service Providers(ISP) – ISPs like Airtel and MTNL help users to get connected to the internet by means of wired or wireless connections.

Search engines – These are web sites like Google and Bing that help users to search for specific information on the web and provide links to web-sites having content relevant to the search terms given bye the user.

DNS providers – These service providers translate the domain names(eg. www.sflc.in) to addresses (eg. 64.202.189.170) that can be understood by computers.

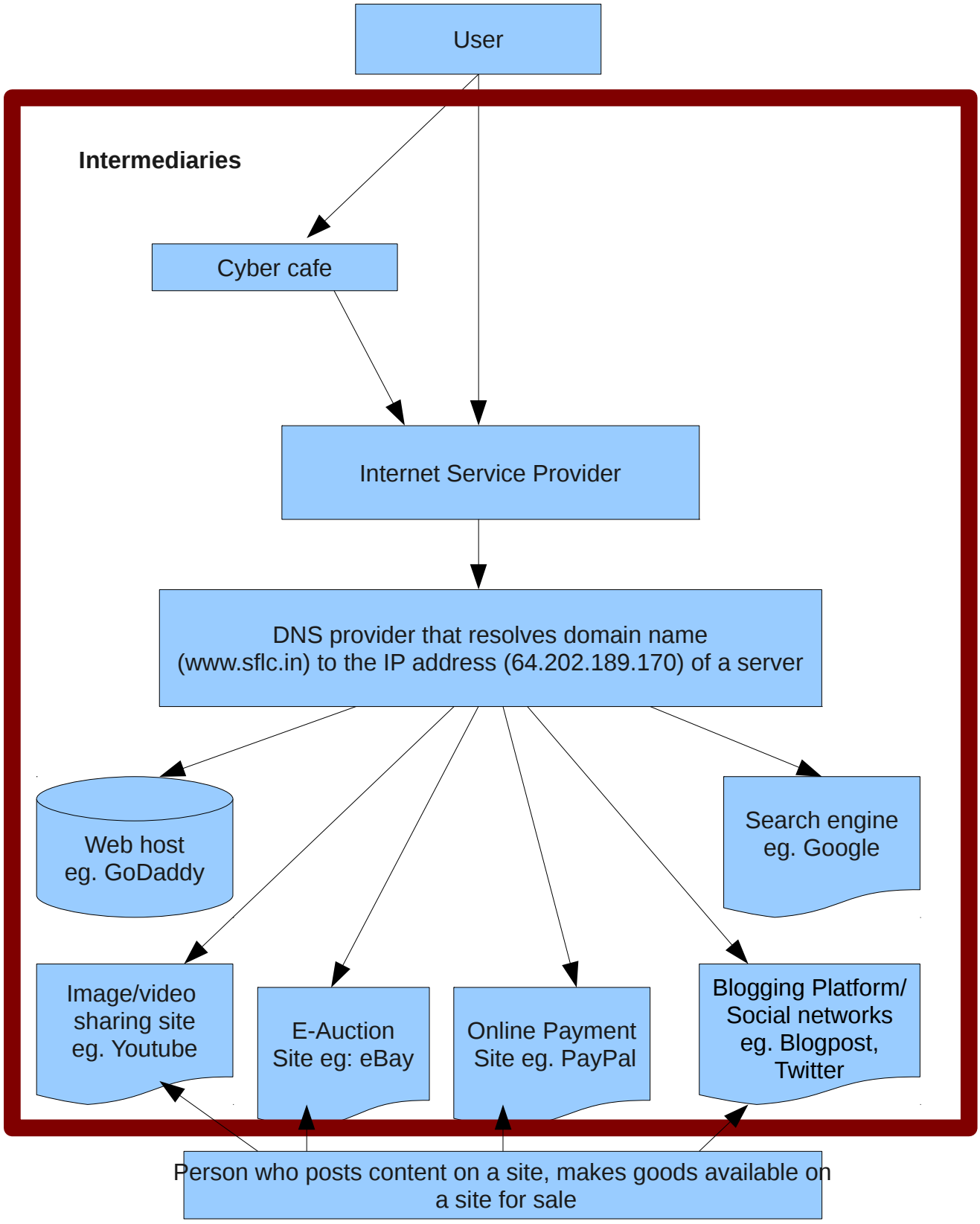
Web hosts – These are service providers like Godaddy.com that provide space on server computers to place files for various web sites so that these sites can be accessed by users

Interactive websites: This includes social media sites like Facebook and Twitter that act as platforms to store and retrieve content, blogging platforms like Blogspot and Wordpress, auction sites like eBay, and payment gateways like PayPal. The pictorial representation gives an overview of the intermediaries involved in a common internet transaction.

Cyber Cafes – It means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public. The Information Technology Act, 2000 includes cyber cafes also under the ambit of the definition of intermediaries.

The legal provision:

Section 2 (w) of the Information Technology Act,2000 (IT Act, 2000) defines ***Intermediaries*** *as - "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes Telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.*



Intermediaries and liability for user generated content

The best illustration for the liability of intermediaries is the Baazee case in which Avnish Bajaj, the CEO of Baazee.com, an auction portal, was arrested for an obscene MMS clip that was put up for sale on the site by a user. The Baazee case showed the legal risks that corporates in the online business space could be exposed to. Although the content is not generated by the intermediaries, in some cases, they could be held liable for offences committed by users while utilising their services. The Delhi High Court while considering a petition to quash the criminal proceedings against Avnish Bajaj in this case, found that the website which hosted the MMS could be held to be liable for 'Sale etc... of obscene books' under Section 292 of IPC as well as Section 67 of IT Act, 2000 relating to publishing of information which is obscene in electronic form.

The Baazee.com case resulted in an appeal by the industry to amend the Information Technology Act, 2000 by providing protection to intermediaries from liabilities arising out of user-generated content. The Information Technology (Amendment) Act, 2008 amended Section 79 of the It Act, 2000 to provide for a safe – harbour protection to intermediaries.

What is safe – harbour protection?

The intermediaries like ISPs, web hosts, social networking sites and blogging platforms play an important role in dissemination of information by providing tools and platforms that allow users to access the Internet, host content, share files and transact business. Websites like Blogspot, Youtube and Facebook only provide a platform for users to post their content, and do not have any editorial control over this content.

Governments across the world realised that these intermediaries must be given protection from legal liability that could arise out of illegal content posted by users, considering the importance of these intermediaries in the online space and the fact that their mode of operation was quite different from the traditional brick-and-mortar business. Countries like the US and members of the European Union, and India now provide protection to intermediaries from such user generated content. Such protection is often termed as a 'safe harbour' protection.

Safe Harbour protection in India

The amended Section 79 of the Information Technology Act, 2000 gives the intermediaries protection from liabilities that could arise out of any legal action initiated on the basis of user generated content. The intermediaries get protection from legal liability that could arise from any action of users that is considered illegal as per the IT Act, 2000 or any other legislation.

Legal Provision:
Section 79 of the Information Technology Act, 2000: Exemption from liability of intermediary in certain cases.—(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-section (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted 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 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.

(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 otherwise 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.

Explanation.—For the purpose of this section, the expression “third party information” means any information dealt with by an intermediary in his capacity as an intermediary.

The safe harbour protection available to intermediaries is conditional upon their observing "due diligence" while discharging their duties and observing guidelines issued by the Government in this regard. These guidelines have now been issued in the form of the Information Technology (Intermediary Guidelines) Rules, 2011. Hence these rules are very important from the standpoint of liability of intermediaries. (Please refer to page 31 for the text of the Rules).

How do the intermediary rules operate?

The new intermediary rules mandate the intermediaries to impose a set of rules and regulations on users. The rules further specify the terms of such regulations and this includes a broad list of categories of content which should not be posted by users.

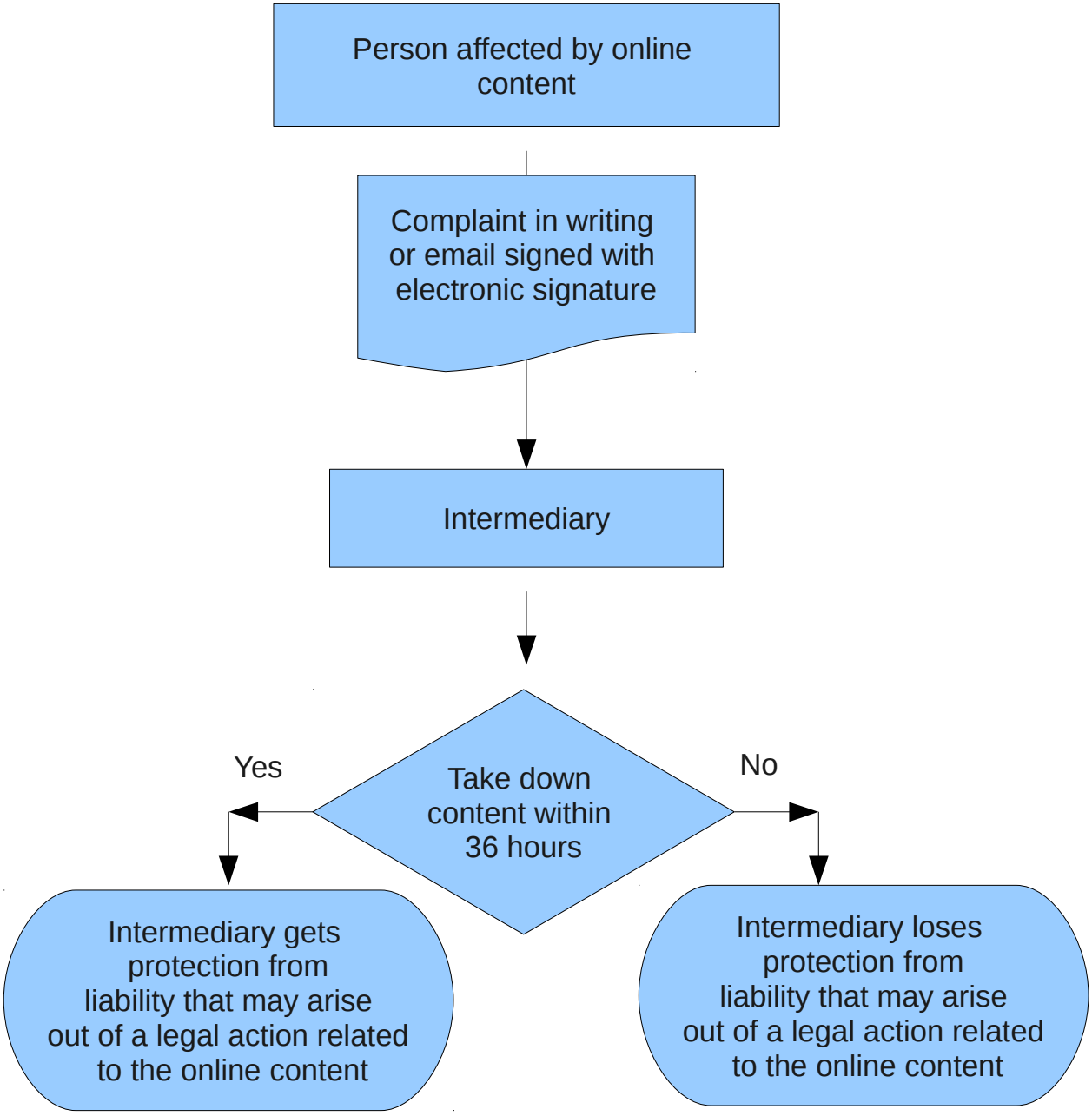
The broad list of unlawful content includes information that is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever. These words are too ambiguous and result in broad interpretation. (Please refer to page 13 for definition of these terms).

Now, any person aggrieved by any content on the internet can ask the intermediaries to take down such content. Intermediaries are obliged to remove access to such content within a period of 36 hours from the time of receipt of the complaint. The rules do not provide for the creator of the content to respond to this complaint. In fact, the rules do not even provide for the intermediaries to inform the user who posted the content regarding the complaint. The intermediaries that do not comply with take-down notice loses the protection from any legal liability that could arise over user content.

The rules also deal with government's power to access user information from the intermediary and the power of the intermediary to disconnect user access. The Rules mandate that intermediaries have to co-operate with government agencies and provide information to them for the purpose of verification of identity, or for prevention, detection, investigation, prosecution etc when a request has been made by the agency in writing. The Intermediary also has to inform the user that in case of violation of any rules and regulations, user agreement or privacy policy; the intermediary shall

terminate the access to its service.

These rules, although titled as guidelines for intermediaries, in effect result in restricting the users by controlling their use of the services offered by intermediaries.



Users and the Chilling effect

These intermediary rules result in placing the onus on intermediaries to restrict content posted on the internet. As intermediaries run the risk of losing their safe harbour protection if content is not removed on receiving a complaint, they will err on the side of caution and this will result in removal of perfectly legal content. Thus, the rules curtail the freedom of the users to express their opinions which ultimately fails the purpose of having an interactive website as such platforms are aimed at allowing users to voice their opinion and to write anything that is in their mind. Also there are certain kinds of websites like online forums and product/service rating sites where the major purpose of running that website is to provide a platform to the user to express his view on a particular issue. Introduction of such guidelines will not only curtail the online freedom, but also defeat the purpose of having websites like blogs, social networking sites and online forums.

The rules empower the Government agencies to obtain information of users from intermediaries. This power granted to the Government agencies do not have any system of checks and balances to safeguard the interests of users.

The rules also mandate the intermediaries to inform the users that their services can be terminated if they violate the terms of service. This provision could have far serious consequences than the three strikes legislation that has been introduced in countries like France, South Korea and Taiwan.

The Intermediary rules, in short, affect the right to freedom of speech and expression of the users by deciding what is acceptable content, affects the right to privacy of individuals by providing for a mechanism to access user information from intermediaries without any safeguards, and could even restrict their ability to access these services by arbitrarily disconnecting them.

Industry and the rules

These rules will have a major effect on internet enterprises based out of India as well as those targeting India. Let us consider effects of the rules on major enterprise verticals:

Internet Service Providers (ISPs)

ISPs come under the definition of intermediaries and these rules apply to them. ISPs do not have any control over the content which is posted on the internet by a user as the ISPs only provide a conduit or a pipe for a user to connect to the internet. ISP cannot in anyway modify or delete content that has been posted on a web-page as the access to that completely rests in the hand of the user who has posted the content or the website/web-page host. Making an ISP liable for content is like making a telephone operator liable for any conversation that occurred on a phone line.

Moreover, take-down notices, if sent to ISPs, could result in taking down of entire websites instead of the individual pages that has the alleged illegal content, as the ISPs may not be able to restrict access to individual pages.

A major issue is that ISPs could end up receiving many requests from Government agencies for user information and since the rules do not have any safeguards for protecting the privacy of the users, this could expose the private transactions of users. This could in turn create problems for the ISPs as they will have to allocate infrastructure and resources to respond to innumerable data monitoring requests.

Domain registrars and web hosts

Web hosts and domain registrars based out of India will be the ones who will be affected the most as they might often have to remove access to domains in response to take-down requests. This will result in customers often moving to hosts based out of other countries.

Interactive websites and social networking

The guidelines are skewed entirely against the creator of the content. The rules also do not place any burden on the complainant to produce evidence in support of the complaint and also do not provide for any penalty on sending frivolous complaints. The rules could soon result in intermediaries being flooded with complaints burdening them with the task of examining these. Also there are certain kinds of websites like online forums and service rating sites like 'Trip advisor' where the major purpose of running that website is to provide a platform to the user to express his view. Frivolous complaints could make the operation of such sites unviable. It is estimated that

there are 140 million tweets posted on twitter per day, 250 million photos are uploaded per day on Facebook and 48 hours of video are uploaded every minute on on Youtube. Frivolous take-down requests would make their operation extremely difficult.

Understanding the ambiguous terms used in the Rules

The Information Technology (Intermediaries Guidelines) Rules, 2011 are replete with numerous words that are ambiguous and have not been defined in the rules or the parent Act. Most words are not defined in any Indian statute for that matter. This list looks at some of these words and try to decipher their meaning. These meanings are given to show the ambiguous nature of the words and should not be taken as a definitive legal interpretation of the words or phrases.

Harm Minors in any way:

The term has not been explained under the Information Technology Act, 2000. However, the closest meaning which can be derived for this term can be found in Section 2(2)(a) of Young Persons (Harmful Publications) Act, 1956 which defines harmful publication as -

"harmful publication" as "means any book, magazine, pamphlet, leaflet, newspaper or other like publication which consists of stories told with the aid of pictures or without the aid of pictures or wholly in pictures, being stories portraying wholly or mainly-
(i) the commission of offences; or
(ii) acts of violence or cruelty ; or
(iii) incidents of a repulsive or horrible nature;
in such a way that the publication as a whole would tend to corrupt a young person into whose hands it might fall, whether by inciting or encouraging him to commit offences or acts of violence or cruelty or in any other manner whatsoever"

Harassing:

The term harassing has not been defined under Information Technology Act, 2000 and it is difficult to comprehend as to what type of content would be termed as harassing.

Blasphemous:

The term Blasphemous has not been defined under the Information Technology Act, 2000. The closest definition that we can refer to is from Indian Penal Code under Section 295 (A) and that is -

295A. Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs.— Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of[citizens of India],[by words, either spoken or written, or by signs or by visible representations or otherwise], insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to[three years], or with fine, or with both.

Defamatory:

A defamatory statement or a publication would be that which affects the reputation of a person. Defamation is defined under Section 499 of Indian Penal Code.

499. Defamation.-- Whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.

Obscene:

Obscene as a general term would mean a written material, gesture or an action designed to incite lust or depravity.

Section 292 of Indian Penal Code, 1860 defines “obscene”

292 Sale, etc., of obscene books, etc. –

For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting representation, figure or any other object, shall be deemed to be ***obscene*** *if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.]*

Section 67 on Information Technology Act, 2000 lists the following provision for publication of

information which is obscene as an offence.

67. Publishing of information which is obscene in electronic form.
Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeal to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Pornographic:
Pornographic material is the material that depicts erotic behaviour and is intended to cause sexual excitement. The term 'Pornographic' has not been defined under Information Technology Act, 2000. However, reference can be drawn about 'Pornography' and 'Pornographic material' from Section 67A of the Act which says

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Paedophilic:
Paedophilia is sexual perversion in which children are the preferred sexual object. The term 'paedophilic' has not been defined in the Information Technology Act, 2000 which again makes the rules acting as guidelines for intermediaries very ambiguous. However, Section 67B of the Information Technology Act, 2000 deals with this offence, although it does not use the term

'paedophilia'.

67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more hildren for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Libellous:

A defamatory statement in a published form is called a Libel. For more information on what constitutes a defamatory statement please refer to the definition of Defamation which has been

mentioned above.

Hateful:

Hateful is any act or gesture that is full of hatred against any person or object. The term hateful has not been defined anywhere under the Information Technology Act, 2000.

Racially/ethnically objectionable:

Information Technology Act, 2000 is silent on this term as well. However for a better understanding Section 153A of the Indian Penal Code can be referred.

153A. Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.

(1) Whoever

(a) By words, either spoken or written, or by signs or by visible representations or otherwise, promotes or attempts to promote, on grounds of religion, race, place or birth, residence, language, caste or community or any other ground whatsoever, disharmony or feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities, or

(b) Commits any act which is prejudicial to the maintenance of harmony between different religious, racial, language or regional groups or castes or communities, and which disturbs or is likely to disturb the public tranquillity, 2[or]

(c) Organizes any exercise, movement, drill or other similar activity intending that the participants in such activity shall use or be trained to use criminal force or violence of knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, or participates in such activity intending to use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, against any religious, racial, language or regional group or caste or community and such activity for any reason whatsoever causes or is likely to cause fear or alarm or a feeling of insecurity amongst members of such religious, racial, language or regional group or caste or community,

Shall be punished with imprisonment which may extend to three years, or with fine, or with both.

Disparaging:

Disparaging would constitute commission of an act which lowers the rank or reputation of the other person. The Information Technology Act, 2000 does not provide definition or explanation of disparaging which burdens us with some doubts regarding what will fall under the term disparaging with reference to the IT Rules.

As per Black's Law Dictionary Disparagement is -

1. *A derogatory comparison of one thing with another*
2. *The act or an instance of castigating or detracting from the reputation of, esp. unfairly or untruthfully*
3. *A false and injurious statement that discredits or detracts from the reputation of another's character, property, product or business.*
4. *Reproach, disgrace or indignity.*

Relating or encouraging money laundering or gambling:

Money laundering is the act of covering up of illegal sources of money to make it look like it came from legal sources. Section 3 of the Prevention of Money Laundering Act, 2002 defines offence of money laundering as under:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering."

Impersonation:

Impersonation means imitation of other persons behaviour, habits, traits and their features in order to look like them. Section 66D of the Information Technology Act,2000 deals with punishment recommended for the offence of Impersonation.

As per S.66D of the Act, whoever, by means of any communication device or computer resource

cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Privacy:

Privacy is a very wide term denoting confidentiality for information relating to oneself and his family and this has been recognised by the Hon'ble Supreme Court to be an integral part of “right to life and personal liberty” granted under Art. 21 of the Constitution of India. However the definition of “privacy” as provided in Information Technology Act, 2000 is very narrow. The use of word privacy in the rules is very ambiguous in relation with as to what exactly would be covered under the term 'privacy'.

As per Section 66E of the Information Technology Act,2000 the term privacy has been restricted to the images of private areas of a person.

66E Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both Explanation.- For the purposes of this section–

(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) “publishes” means reproduction in the printed or electronic form and making it available for public;

(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that–

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

But,if we look at Article 21 of the Constitution of India as interpreted in R. Rajagopal v. State of T.N. popularly known as "Auto Shanker case" , the Supreme Court has expressly held

" the "right to privacy", or the right to be let alone is guaranteed by Article 21 of the Constitution. A citizen has a right to safeguard that privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right of the person concerned and would be liable in action for damages. However, position might differ if he voluntarily puts into controversy or voluntarily invites or raises a controversy."

Thus, the Information Technology (Intermediaries guidelines) Rules, 2011 has given a broad list of content considered to be unlawful, that are replete with ambiguous terms.

A legal analysis of the Information Technology (Intermediaries guidelines) Rules, 2011

The Government has notified on April 13, 2011 the Information Technology (Intermediaries guidelines) Rules, 2011 prescribing guidelines to be observed by the intermediaries. The rules were issued in exercise of the powers conferred by clause (zg) of subsection (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (Act 21 of 2000) . The provisions of the new rules are unconstitutional as they affect the right to freedom of speech and expression as well as right to privacy of citizens, are arbitrary being violative of Art. 14 of the Constitution of India and are ultra vires of the parent act.

Section 79 of the Act provides the intermediaries protection from liability arising out of user generated content. This is in line with the position followed in countries like the US and members of the European Union. The Digital Millennium Copyright Act and the Communications Decency Act in the US and the Directive on Electronic Commerce in the EU provides protection to intermediaries from liability arising out of content posted by users of services provided by intermediaries.

S. 79 of the Act mandates the intermediary to observe due diligence while discharging its duties under the Act and to observe such other guidelines as prescribed by the Central government in this behalf. The Central Government is thus conferred with powers to prescribe guidelines relating to duties to be discharged by the intermediaries. However while issuing this sub-ordinate legislation, the central government has acted beyond its powers provided under the Act and expanded and amended the provisions of the Act.

The provisions of the rules that are unconstitutional or ultravires of the parent act are listed below:

A. Sub-rule (2) of Rule 3

Sub-rule (2) of Rule 3 mandates intermediaries to place restrictions on the kind of content that a user can post by enumerating a broad list of information. Sub-rule (2) of Rule 3 mandates users not to host information included in a broad list that includes information that 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.

1. The rule is arbitrary

The subject matter of information listed in sub-rule (2) of rule 3 including words like blasphemous, grossly harmful, harassing, invasive of another's privacy, racially, ethnically objectionable, disparaging, belongs to another person and harm minors in any way, is highly subjective and is not defined either in the rules or in the Act, or in any statute for that matter. The rule by including such ambiguous terms results in wide interpretation of the subject matter, and hence, the rule is highly unreasonable and arbitrary and violative of Art.14 of the Constitution of India.

2. The rule is violative of freedom of speech and expression

Clause (2) of Article 19 permits the state to make laws mandating reasonable restrictions on the exercise of the right conferred by Art. 19(1)(a) in the interests 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. Thus, any restrictions that can be made on the right of citizens to freedom of speech and expression can only be within the ambit of clause (2) of Article 19.

Clause (i) of sub-rule (2) of Rule 3 has listed the reasonable restrictions to freedom of speech permissible under Article 19(2) of the Constitution of India. Apart from clause (i) of sub-rule (2) of rule 3, all the clauses attempt to impose restrictions that are not reasonable on the right to freedom of expression of the user. The Hon'ble Supreme Court has held in *Express Newspapers (Private) Ltd. and Anr. Vs. The Union of India (UOI) and Ors., AIR 1958 SC 578* that if any limitation on the exercise of the fundamental right under Art. 19(1)(a) does not fall within the four corners of Art. 19(2) it cannot be upheld.

3. The rule is ultra vires of the parent act.

Central Government obtains the source of power to issue these rules from the provisions of the Information Technology Act, 2000. The rule making power has to be strictly confined to the

boundaries specified as per the Act and cannot result in expanding the scope of the Act. Chapter XII of the Information Technology Act, 2000 (as amended) provides exemption from liability of intermediaries in certain cases. This exemption is subject to certain conditions to be observed by the intermediaries. The Government obtains the source of power to issue these rules from two provisions of the Act :

> S.79 (2) (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.
>
> S.87 (2) (zg) - the guidelines to be observed by the intermediaries under sub-section (2) of section 79

Thus the rule making power of the Central Government is limited to prescribing other guidelines in this behalf**.** These guidelines can only be related to "due diligence" to be observed by the intermediary while discharging its duties under the Act.

The duties of an intermediary under the Act are restricted to the following:

1. Under S. 67C of the Act intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
2. Under S. 69. of the Act relating to power to issue directions for interception or monitoring or decryption of any information through any computer resource the subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1) extend all facilities and technical assistance to—

   (*a*) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

   (*b*) intercept, monitor, or decrypt the information, as the case may be; or

   (*c*) provide information stored in computer resource.
3. Under S. 69A of the Act relating to blocking public access of any information through any computer resource the intermediary has to comply with the direction issued by the government in this regard.
4. Under S. 69B of the Act relating to monitoring and collecting traffic data or information

> through any computer resource for cyber security the intermediary or any person in-charge or the computer resource shall, when called upon by the agency authorised, provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

The government can prescribe guidelines only on behalf of the above duties of the intermediaries. But these rules have widened the scope of the Act by legislating on information that can be posted by a user and listing a broad category of information that can be considered as unlawful and this is not in any way connected to the duties to be discharged by the intermediaries under the Act. Sub-rule (2) and (4) of Rule 3 of the intermediary rules go beyond controlling intermediaries and result in controlling the users who post content.

The Hon'ble Supreme Court has held in *State of Karnataka and Anr. Vs. Ganesh Kamath and Ors. (1983)2 SCC 40* that:

> "it is a well settled principle of interpretation of statutes 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".

The Hon'ble Supreme Court has held in *Agricultural Market Committee Vs. Shalimar Chemical Works Ltd. (1997)5 SCC 516* that:

> "The delegate which 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 Act or the policy laid down thereunder. It cannot, in the garb of making Rules, legislate on the field covered by the Act and has to restrict itself to the mode of implementation of the policy and purpose of the Act."

In view of the law as laid down in the aforementioned judgments, the Central Government has acted beyond its powers vested by the Information Technology Act, 2000 in framing the new IT rules.

B. Sub-rule (4) of rule 3

1. The rule is unreasonable and arbitrary

Sub-rule (4) of rule 3 that mandates that the intermediary, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours to disable such information that is in contravention of sub-rule (2), does not provide for an opportunity to the user who has posted the content to reply to the complaint and to justify his case. The rule that mandates the intermediary to disable the content without providing an opportunity of hearing to the user who posted the content is violative of the principles of natural justice and is highly arbitrary.

This provision results in taking down of content without any involvement of the government or its agency and this will lead to a private censorship mechanism without any checks and safeguards. Such a provision is highly unreasonable and arbitrary.

Sub-rule (4) of rule 3 results in endowing an adjudicating role to the intermediary in deciding questions of fact and law, which can only be done by a competent court. Such a provision of the rules is liable to be misused and is highly unreasonable and arbitrary.

2. The rule violates the fundamental right to freedom of speech and expression guaranteed to citizens and is unconstitutional

Sub-rule (4) of rule 3 of the intermediary rules mandates that 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). The subject matter of unlawful information listed in sub-rule (2) of rule 3 is highly subjective and could result in wide interpretation. Sub-rule (2) of rule 3 has provisions that are beyond reasonable restrictions that can be laid down as per Article 19(2) of the Constitution of India. The rules place a burden on the intermediaries to decide on the lawful nature of the content as a pre-condition for exemption from liability. The

intermediaries, on receiving a complaint, to ensure that they continue to receive the protection offered by Section 79 of the Act, will be forced to disable access to the content posted by a user. Under the rules, any person who is critical of an article or a blog post can raise a complaint with an intermediary, and this will result in removal of the content by the intermediary. Thus, the direct effect of the rules will be strict censoring of content posted on-line by users. The rules will have a direct effect on the fundamental right of freedom of speech and expression guaranteed under Article 19(1) of the Constitution of India. Article 19(1) of the Constitution of India guarantees all citizens the right to freedom of speech and expression.

3. The rule is ultra vires of the parent act and is invalid

Clause (b) of sub-section 3 of Section 79 of the Information technology Act, 2000 mandates the intermediary 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, to disable access to the material. The rule has in effect amended this provision by providing for any affected person to submit a request to the intermediary to take down content and mandating the intermediary to comply within a period of 36 hours. This provision that results in taking down of content without any involvement of the government or its agency will result in a private censorship mechanism without any checks and safeguards.

Section 69A of the Information technology Act, 2000 provides that when the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, 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, it may subject to the provisions of sub-section (2) of Section 69A, for reasons to be recorded in writing by order, direct any agency of the Government or intermediary to block for access by the public any information generated, transmitted, received or stored in any computer resource. The legislature has thus spelt out a specific procedure for blocking access to information. The Central Government has notified the rules providing for safeguards for such blocking of access called the Information technology (Procedure and safeguards for blocking for access of information by public) Rules, 2009. The rules

lay down the procedure and safeguards for blocking of access of any information that comes under the scope of sub-section (1) of section 69 A. Sub-rule (4) of rule 3 of the intermediary rules is in direct contravention of Section 69 A of the Act and the rules made thereunder and is hence ultra vires of the Act.

C. Sub-rule (5) of Rule 3

1. The rule is arbitrary

Sub-rule (5) of rule 3 mandates the intermediary to inform 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 rights of the users to the computer resource of Intermediary and remove non-compliant information. This provision will result in termination of services to a user on posting of any content which the intermediary deems as unlawful. This provision does not provide for any checks and balances for use of this power to terminate the access of a user. Such a power mandated to be exercised by the intermediary is highly unreasonable and arbitrary.

2. The rule violates the right to freedom of speech and expression

The right to freedom of speech and expression guaranteed by the constitution includes the right to receive information. Article 19 of the Universal Declaration of Human Rights states that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". The disconnection of the service by an intermediary will affect the right of a citizen to receive information and this is a violation of the fundamental right under Article 19(1) of the Constitution of India. The Hon'ble Supreme Court has held in *The Secretary, Ministry of Information & Broadcasting v Cricket Association Of Bengal, 1995 AIR SC 1236* that:

> The freedom of speech and expression includes right to acquire information and to disseminate it. Freedom of speech and expression is necessary, for self expression

> which is an important means of free conscience and self fulfillment. It enables people to contribute to debates of social and moral issues. It is the best way to find a truest model of anything, since it is only through it, that the widest possible range of ideas can circulate. It is the only vehicle of political discourse so essential to democracy. Equally important is the role it plays in facilitating artistic and scholarly endeavours of all sorts. The right to communicate, therefore, includes right to communicate through any media that is available whether print or electronic or audio-visual such as advertisement, movie, article, speech etc. That is why freedom of speech and expression includes freedom of the press. The freedom of the press in terms includes right to circulate and also to determine the volume of such circulation. This freedom includes the freedom to communicate or circulate one's opinion without interference to as large a population in the country as well as abroad as impossible to reach."

In *Tata Press Ltd. Vs. Mahanagar Telephone Nigam Limited and Ors (1995)5 SCC 139*, the Hon'ble Supreme Court held that:

> "Article 19(1)(a) not only guarantees freedom of speech and expression, it also protects the rights of an individual to listen, read and receive the said speech".

Sub-rule (5) of rule 3 by providing for terminating access to the services of an intermediary without laying down any procedures and safeguards, results in violation of a citizen's right to freedom of speech and expression.

D. Sub-rule (7) of Rule 3

1. The rule violates right to privacy of citizens

Sub-rule (7) of rule 3 mandates the intermediary, when required by lawful order, to provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The requirement for lawful order is modified while

mandating that 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 stating clearly the purpose of seeking such information or any such assistance. The requirement of giving information about users by the intermediary on a mere written request from an agency could have serious implications on the right to privacy of citizens. Right to privacy as a component of Article 21 of the Constitution of India, which guarantees for "right to life and personal liberty" has been recognised by the Hon'ble Supreme Court in *Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148* and *R. Raj Gopal v. State of Tamil Nadu,(1994) 6 SCC 632.* This right can be curtailed only by a procedure established by law and cannot be done arbitrarily. The Hon'ble Supreme Court of India in *People's Union of Civil Liberties (PUCL)Vs. Union of India (UOI) and Anr., (1997)1 SCC 301*, while deliberating on the issue of tapping of telephone conversation held that "Telephone-Tapping is a serious invasion of an individual's privacy" and prescribed guidelines for that. The rules by providing for information to be provided by intermediaries on a written request will result in wire-tapping of the internet without any legal safeguards whatsoever.

2. The rule is ultra-vires of the parent act.

Sub-rule (7) of rule 3 mandates the intermediary, when required by lawful order, to provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. Section 69 of the Information Technology Act, 2000 deals with the power to issue directions for interception or monitoring or decryption of any information through any computer resource. Sub-section (2) of Section 69 provides for procedures and safeguards subject to which such interception or monitoring may be carried out. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were notified by the Government to provide for such safeguards and procedures. These rules enshrine the guidelines prescribed by the Hon'ble Supreme Court in *People's Union of Civil Liberties (PUCL)Vs. Union of India (UOI) and Anr., (1997)1 SCC 301.* These rules mandate that such interception or monitoring of information can be carried out by an order by an order issued by a competent authority. The competent authority to issue such an order under these rules is the Secretary in the Ministry of Home Affairs, in case of Central Government or

the Secretary in charge of the Home Department, in case of a State Government or Union Territory. Sub-rule (7) of rule 3 that mandates an intermediary to provide information does not have any such safeguards and is in violation of the provisions of the Act and the rules issued thereunder.

The Information Technology (Intermediaries guidelines) Rules, 2011.

G.S.R (E).— In exercise of the powers conferred by clause (zg) of sub- section (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely: —

1. Short title and commencement.— (1) These rules may be called the Information Technology (Intermediaries guidelines) Rules, 2011.

(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,— (j) “Act” means the Information Technology Act, 2000 (21 of 2000);

(k) “Communication link” means a connection between a hypertext or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which could be another document or another website or graphical element.

(l) “Computer resource” means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;
(m) “Cyber security incident” means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(n) “Data” means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(o) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;

(p) “Indian Computer Emergency Response Team” means the Indian Computer Emergency Response Team appointed under sub section (1) of section 70(B) of the Act;

(q) “Information” means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(r) “Intermediary” means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(s) “User” means any person who access or avail any computer resource of intermediary for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views

and includes other persons jointly participating in using the computer resource of an intermediary.

(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. Due diligence to be observed by intermediary.— 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 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 hosting, 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 rights 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 stating 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.

[No. 11(3)/2011-CLFE]
(N. Ravi Shanker)
Joint Secretary to the Government of India

Clarification by Ministry of Communications & Information Technology

11-May-2011 16:36 IST

Exemption from Liability for Hosting Third Party Information: Diligence to be Observed under Intermediary Guidelines Rules

The attention of Government has been drawn to news items in a section of media on certain aspects of the Rules notified under Section 79 pertaining to liability of intermediaries under the Information Technology Act, 2000. These items have raised two broad issues. One is that words used in Rules for objectionable content are broad and could be interpreted subjectively. Secondly, there is an apprehension that the Rules enable the Government to regulate content in a highly subjective and possibly arbitrary manner.

The Department of Information Technology (DIT), Ministry of Communications & IT has clarified that the Intermediaries Guidelines Rules, 2011 prescribe that due diligence need to be observed by the Intermediaries to enjoy exemption from liability for hosting any third party information under Section 79 of the Information Technology Act, 2000. These due diligence practices are the best practices followed internationally by well-known mega corporations operating on the Internet.

The terms specified in the Rules are in accordance with the terms used by most of the Intermediaries as part of their existing practices, policies and terms of service which they have published on their website. In case any issue arises concerning the interpretation of the terms used by the Intermediary, which is not agreed to by the user or affected person, the same can only be adjudicated by a Court of Law. The Government or any of its agencies have no power to intervene or even interpret. DIT has reiterated that there is no intention of the Government to acquire regulatory jurisdiction over content under these Rules. It has categorically said that these rules do not provide for any regulation or control of content by the Government.

The Government adopted a very transparent process for formulation of the Rules under the Information Technology Act. The draft Rules were published on the Department of Information

Technology website for comments and were widely covered by the media. None of the Industry Associations and other stakeholders objected to the formulation which is now being cited in some section of media.

The Government has been forward looking to create a conducive environment for the Internet medium to catapult itself onto a different plane with the evolution of the Internet. The Government remains fully committed to freedom of speech and expression and the citizen's rights in this regard.
SP/AS