31

COMMITTEE ON SUBORDINATE LEGISLATION

(2012-2013)

(FIFTEENTH LOK SABHA)

THIRTY-FIRST REPORT

ON

(i) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
(ii) The Information Technology (Intermediaries Guidelines) Rules, 2011
(iii) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011
(iv) The Information Technology (Electronic Service Delivery) Rules, 2011

(PRESENTED ON 21.03.2013)

S

E

A

L

LOK SABHA SECRETARIAT

NEW DELHI

March, 2013 /Phalguna,1934 (Saka)

COSL No. 40

PRICE: Rs.

Published under Rule 382 of the Rules of Procedure and Conduct of Business in Lok Sabha (Fourteenth Edition) and printed by the Manager, Government of India Press, Minto Road, New Delhi.

CONTENTS

APPENDICES

COMPOSITION OF THE COMMITTEE ON SUBORDINATE LEGISLATION
(2012-2013)

1. Shri P. Karunakaran — Chairman
2. Shri Praveen Singh Aron
3. Shri Ramen Deka
4. Shri K. Jayaprakash Hegde
5. Dr. Mahesh Joshi
6. Shri Virender Kashyap
7. Dr. Ajay Kumar
8. Shri Narahari Mahto
9. Dr. Thokchom Meinya
10. Shri Gajendra Singh Rajukhedi
11. Dr. Bhola Singh
12. Shri R. Thamaraiselvan
13. Shri Manohar Tirkey
14. Shri Dharmendra Yadav
15. Vacant

SECRETARIAT

1. Shri A. Louis Martin - Joint Secretary
2. Shri S.C. Chaudhary - Director
3. Shri Srinivasulu Gunda - Addl. Director
4. Shri Krishendra Kumar - Under Secretary

I N T R O D U C T I O N

I, the Chairman, Committee on Subordinate Legislation having been authorized by the Committee to submit the report on their behalf, present this Thirty-First Report of the Committee on examination of the following rules :-

(i) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011[GSR 313(E)]
(ii) The Information Technology (Intermediaries Guidelines) Rules, 2011[GSR 314 (E)]
(iii) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011[GSR 315(E)]
(iv) The Information Technology (Electronic Service Delivery) Rules, 2011[GSR 316 (E)]

2. The following Non Governmental Organizations submitted Memoranda to the Committee on the aforesaid rules :-

(i) Society for Knowledge Commons
(ii) Software Freedom Law Centre
(iii) Centre for Internet and Society

3. The Committee heard the views of representatives of "Society for Knowledge Commons" and "Software Freedom Law Centre" on 13 August, 2012 in connection with examination of the subject.

4. The Committee took oral evidence of the representatives of the Ministry of Communications and Information Technology (Department of Electronics and Information Technology) on 20 September, 2012 on the subject.

5. The Committee considered and adopted this Report at their sitting held on 18 March, 2013.

6. The Committee wish to express their thanks to the representatives of the Ministry of Communications and Information Technology [Department of Electronics and Information Technology) who appeared before them and placed their views in connection with examination of the subject. The Committee also wish to thank them for furnishing requisite material on the subject.

7. The Committee also thank (i) Society for Knowledge Commons , (ii) Software Freedom Law Centre and (iii) Centre for Internet and Society for furnishing Memoranda on the subject. The Committee also express their thanks to the representatives of "Society for Knowledge Commons" and "Software Freedom Law Centre" who appeared before the Committee and placed their views on the subject.

8. For facility of reference and convenience, recommendations/observations of the Committee have been printed in thick type in the body of the Report and have also been reproduced in Appendix-I of the Report.

9. The Minutes of the Eighth and the Tenth sittings of the Committee (2011-12) held on 13 August, 2012 and 20 September, 2012 respectively and Minutes of the Fifth sitting of the Committee (2012-13) held on 18 March, 2013 are available in Appendix-II.

P. KARUNAKARAN,
CHAIRMAN,
COMMITTEE ON SUBORDINATE LEGISLATION

New Delhi;
20 March, 2013
29 Phalguna, 1934 (Saka)

REPORT

The Information Technology Act, 2000 was enacted to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternative to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the India Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. The Act was published in GSR No. 27 dated 9 June, 2000. The Act was amended in 2008 and the amended Act came into existence on 5 February, 2009.

2. In exercise of the powers conferred by sections 6A, 43A, 79 and 87 of the Information Technology Amendment Act, 2008 notified on 5 February, 2009, the following rules were notified by the Ministry of Communications and Information Technology [Department of Electronics and Information Technology (DeitY)] on 11 April 2011 and laid on the Table of Lok Sabha on 17 August, 2011:

(i) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
(ii) The Information Technology (Intermediaries Guidelines) Rules, 2011
(iii) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011
(iv) The Information Technology (Electronic Service Delivery) Rules, 2011

3. In the course of examination of the aforesaid Rules a number of infirmities were noticed in the Rules. Written memoranda from three NGOs working in the information technology area *viz*. (i) Society for Knowledge Commons, (ii) Software Freedom Law Center and; (iii) Centre for Internet and Society were received.

Comments of the Department of Electronics and Information Technology (DeitY) were sought on the infirmities.

4. On 13 August, 2012, the Committee had oral hearing of representatives of Society for Knowledge Commons and Software Freedom Law Center.

5. The Committee, thereafter, took evidence of the representatives of the Department of Electronics and Information Technology (DeitY) on 20 September, 2012.

6. The issues examined by the Committee with reference to the aforesaid rules are discussed in the succeeding sections of the report.

A. Definitions of terms

7. Section 79 of the Information Technology Act, 2000 dealing with exemptions from liability of intermediary in certain cases reads as follows:

" (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or 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 purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary".

8. In pursuance of Sections 79 and 87(2) of the Information Technology Act, the Central Government notified the Information Technology (Intermediaries guidelines) Rules, 2011 on 11 April, 2011. Rule 3 of the Information Technology (Intermediaries guidelines) Rules, 2011 deals with due diligence to be observed by the intermediary. Sub rules (1) and (2) of rule 3 read as under:-

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

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

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

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

(c) harm minors in any way;

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

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

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

(g) impersonate another person;

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

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

9. Referring to the aforesaid rules, Software Freedom Law Centre, in their written representation (dated 14.12.2011) submitted to the Committee that the

subject matter of information listed in sub-rule (2) of rule 3 of the intermediaries guidelines 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 Organization further stated that 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..

10. Pleading that the Intermediary guidelines are *ultra-vires* of the Constitution of India, Society for Knowledge Commons, another NGO working in the information technology area in their written representation (dated 16.06.2011) stated as under –

> ''.The list of information that is barred includes information that "is blasphemous", "defamatory", "harassing", "libellous", "invasive of another's privacy", "disparaging", "hateful", "relating or encouraging money laundering or gambling or otherwise unlawful in any manner" etc. This is patently in violation of various Fundamental Rights protected under the Constitution. The Guidelines are therefore vague and ambiguous in that they fail to lay down parameters for deciding what objectionable, disparaging etc and what is not. Further, Intermediaries are required to act as an agency of the government in censoring offending material and may be liable for failure to do the same. The list of offensive information is extremely broad (more so than in Sections 69 and 69A of the IT Act). Supreme Court dicta makes it evident that if any limitation on the exercise of the fundamental rights under Art. 19(1) does not fall within the ambit of Art. 19(2) or is not reasonable and just, it cannot be upheld. The removal of content can thus only be done if it falls under the reasonable restrictions imposed under Art. 19(2) of the Constitution. Hence the broad list of proscribed information provided by the Guidelines, together with the absence of any fair procedure for determining what is offending material ensures that the Guidelines are *ultra vires* the Constitution of India."

11. A representative of the Society for Knowledge Commons who appeared before the Committee on 13.08.12 pointed out that the whole range of expressions given in rule 3(2) (b) is vague and stated as follows -

"….Here, if you look at the IT rules, it has used a whole range of expressions which are not found in Indian law. For instance, it has said 'offensive; if content is offensive to somebody'.

…. It is completely vague. In effect, 'libel' is clearly illegal. I have civil and criminal 'libel' that I can go on. But it is not illegal for me to offend somebody. So there are many such terms which are there which are not drawn from Indian law but it seems to be taken from here and there and just put over there. I would suggest that all that it should be done if you really wanted this provision of private censorship if it is felt necessary then you should have said anything which is against Indian law. That is perfectly legitimate. But to say that it should not be offensive, it should not be disparaging; it should not be harassing.

…..A lot of them are not actually crimes. Blasphemy, for example, is not a defined crime under the IPC. IPC has various provisions regarding creating enmity between classes and so on and so forth. There is no particular punishment under the IPC for blasphemy."

12. Stating further that the words mentioned in rule 3(2) (b) are not defined in the Act or in the rules, the representative of Society for Knowledge Commons submitted before the Committee on 13.08.12 as under -

"Sir, with our limited knowledge, these have not been defined as the Government claims. All that I am saying is that if the Government should have said as per the Indian law, then, it is okay. Then, law and whatever courts had interpreted would have been fine. But if you see 69A, for instance, it says exactly what can be blocked. There, it is very precise. It says sovereignty of India. It says specific things. But when it comes to what the intermediary is supposed to do, it is not defined like 69A. It is defined much more broadly. Though it has two parts of it, 69A was the Parliament Act and it defines it very clearly. But when it came to guidelines – which is what the rules are – then you will see that it has expanded for beyond the Act. 69A is for the Government. The Government will act strictly according to the law but the private parties will act in a much bigger term. That is the problem."

13. A representative of the Software Freedom Law Centre, appearing before the Committee on 13.08.12, expressing the view that the whole range of expression given in rule 3(2) (b) is vague as stated as under: -

" ….phrases like 'grossly harmful', 'harassing', 'offensive', etc. And, these terms are not defined anywhere in the Act; anywhere in the IT Act 2000. So, these are vague terms, specifically what this Committee did not want in the rules. Anybody, who says that some contents are objectionable, he can directly complain to the intermediary, maybe it is Google or Facebook.''

14. In response to a query as to whether the Hon' ble Supreme Court has given judgments about the definitions of these phrases, the representative of Software Freedom Law Centre during the hearing held on 13.08.12 stated as follows:

> "No, it is not defined. For example, something like 'blasphemous', nobody knows what blasphemous is. Of course, there are provisions in IPC, which deal with something which could affect religious feelings, but, nothing which talks about what is blasphemous. Even if there is a decision by the Supreme Court, it should be specific in a rule or an Act. Any term should be defined. It is because that is how the common man comes to know about it. Otherwise, how should he decide?"

15. Enquired whether the word 'blasphemous' has been defined in Section 153 (a) of IPC, the representative of Software Freedom Law Centre during the hearing held on 13.08.12 replied as under:

> "It is not defined; it only talks about an offence. It is said that the 'blasphemous' has been defined in Section 153 (a) of IPC. It is defined nowhere in the Act. It only talks about the offence related to something which could hurt religious feelings. But, when you use a word like blasphemous, in that case they could find it saying that blasphemous is this and it is in such and such Section of the IPC. But, it is not there in the IPC at all. Blasphemous, as a word, is not there in the IPC. It is not there in any statute in India. I have referred to almost all the statutes and I have done a search also. So, these are words, which are not defined in the Act."

16. In response to a query as to whether the words / expressions mentioned in rule 3(2) (b) are defined in the act or the rules made there under, the Secretary, (Deity) deposing before the Committee on 20 09.12 stated as under-

> ''They have been used in the Act, which are in consonance with various sections of IPC, ... We have taken it from various sections of the IPC, etc., and also judgments of the courts. However, they have not been specifically defined as such. ''

17. Elaborating further on the issue, the Secretary, (DeitY) stated as follows -

> "These words have been taken from the different sections of the IT Act itself or from the other accepted laws in India. But the point that there should not be any scope for any vagueness or ambiguities is absolutely correct. We will convey it back to our hon. Minister. This point was also raised in the consultation held in the month of August. So, definitely

our effort will be to make it as crystal clear as possible. There should not be any doubt it. It is rightly pointed out by the hon. Members and we do agree that courts judgements should take it for interpretation but there is nothing like providing a definition upfront. We will convey the suggestions of the hon. Members. "

18. A representative of the DeitY, elaborating further on the issue, during the oral evidence held on 20.09.12 stated as follows –

"The hon. Members have asked about the ambiguous words. Most of the social networking sites which are being accused in this country do not have any operation in India. In fact, they say that they do not have any offices in India. They have Indian subsidiaries. The sites say that the main company and the Indian subsidiaries are not linked together. If we look at the practices and policies of these social networking sites, each of them, whether it is Face Book, Google, You Tube, Yahoo or Twitter or any other sites have exactly used the same words as used in the Rules. These words were given to us by the premier and the major industry association of India. These words have been mentioned verbatim in the policies and guidelines of the social networking sites. So, it was thought that since these words have been used by these sites and the social sites are undertaking the process of deleting and updating content. These social sites understand the process and words ambiguously. Today issue is there only from the foreign websites. All Indian websites have implemented the rules in toto. It is the foreign websites which are raising issues.

... About the definitions, these are the exact words mentioned by the foreign social sites. If one see Article 19(1), the word 'defamation' is there. This was also discussed during the debate in the Rajya Sabha. At best, we can repeat those words which are mentioned in the Article 19 because those words are very well interpreted. We got a very good support in the Rajya Sabha."

19. The Committee observed that there was no definition of the words / expressions either in the act or the rules made there under and also there was no clarification as to whether the definitions of these terms given in relevant acts such as Indian Penal Code, Money laundering Act, etc, are applicable to IT Act/ rules made there under. When enquired from Deity whether they are in favour of making appropriate changes to the Act/ rules to eliminate the scope for misinterpretation / ambiguity, DeitY in a written communication dated 03.12.12 stated that the words such as grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous etc. are used commonly in legal parlance

internationally. All the Internet companies worldwide have mentioned these words in their own terms of use/agreement with the users. According to DeitY these terms therefore, are well understood and interpreted by the Internet companies who are intermediaries. DeitY further stated that their (the intermediaries) terms of use/terms of agreement advise the users not to post content which are of such nature as provided in rule 3(2). For example para 6 of Yahoo! Terms of Service, paras 3, 4 and 5 of Statement of Rights and Responsibilities of Facebook, Content Boundaries of Blogger Content Policy, Content Boundaries and Use of Twitter of Twitter Rules, Community Guidelines of Google Finance. Some of these words such as *grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic* are also defined in the Indian Penal Code (IPC). Some provisions in the IPC also addresses the offences of blasphemous libelous content etc. It may be mentioned that any FIR filed for offences under the Information Technology Act, 2000 also provides analogous provision under IPC. A table showing the sections defining or addressing these words in Indian Law is given below:

Words/ phrases	Sections/Enactments
Grossly harmful/ Harassing/ Hateful/ Disparaging	Various provisions of IPC. Almost all criminal statutes in India have made such components/ elements as part of criminal/guilty mind.
Blasphemous	s. 153A, Chapter XV: Offences relating to religion [ss. 295-298], IPC
Defamatory/ Libelous	Chapter XXI: Defamation [ss. 499-502], IPC
Obscene/ Pornographic/ Paedophilic/ Harms minors in any way	s. 292-294 of IPC, sections 67,67A & 67B of IT Act etc.
Invasive of another's privacy	Right to Privacy [Article 21], Supreme Court laid

	law [Article 141]
Racially, ethnically objectionable	s. 153A IPC
Relating or encouraging money laundering or gambling	Various provisions of the Prevention of Money Laundering Act, 2002
Otherwise unlawful in any manner	Common to all statutes

20. DeitY also informed that Hon'ble Supreme Court and High Courts have interpreted these words in a number of judgements. A list of judgements made by Hon'ble Supreme Court and High Court defining such words is given below:-

(i) Brij Bhusan and another vs the State of Delhi (26.5.1950)
(ii) The State of West Bengal vs Subodh Gopal Bose and others (CA 107/1952)
(iii) Sebastian@Chevithian vs State of Kerala (CA 1368/2008)
(iv) Standard Chartered Bank vs Directorate of Enforcement (2006 4 SCC 278)
(v) Director General of Doordarshan vs Anand Patwardhan (2006 8 SCC 481)

It is stated to be a normal legal practice to draw upon the meaning of such offences from the Indian Penal Code and Code of Criminal Procedure (CrPC). It is not desirable to legally differentiate in the meaning of these words. According to Deity so far no instance has been cited or has been brought to the notice of Government where citing these words have been misinterpreted in the context of Information Technology Act vis-à-vis other Laws. The Secretary Deity, however stated during evidence:-

> "In fact, hon. Minister for Communications held a meeting involving industries, some of the Hon'ble Members of Parliament, media and intermediaries on 3rd August. There, we had detailed discussions and consultations with them. It was also felt there that there is room for improvement of the intermediate guidelines so that there is no ambiguity. Wherever certain ambiguity is there, it should be removed.''

21. In response to a query as to whether any commitment has been given to refine the wordings Deity stated that Hon'ble Minister had convened a Meeting of industry associations, intermediaries, users and other stakeholders on 2nd August, 2012. There was a consensus that the process followed by the Government in framing the rules was fair and transparent.

22. Section 66A of the Information Technology Act, 2000 which provides for punishment for sending offensive messages through communication service, etc, reads as under-

'' Any person who sends, by means of a computer resource or a communication device -

(a) any information that is grossly offensive or has menacing character; or
(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device; or
(c) any electronic mail or electronic mail message for the purpose of the causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such message, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation- For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message. "

23. Section 80 of the Act empowers any police officer not below the rank of 'Inspector' (before amendment of the Act in 2008 it was Deputy Superintendent of Police) or any other officer of the Central Government or a State Government authorized by the Central government in this behalf may enter any public place and search and arrest without any warrant any person found therein who is reasonably

suspected or having committed or of committing or of being about to commit any offence under the act.

24. According to media reports, there have been protests demanding repeal of Section 66A of the Information Technology Act after several instances of reported misuse of the Section - arrest of Jadavpur University professor for circulating a cartoon, cartoonist Aseem Trivedi and arrest of two girls in Maharashtra for criticizing bandh.

25. The Committee note that Rule 3 of the Information Technology (Intermediaries Guidelines) Rules, 2011 requires intermediary to publish rules and regulation etc. for access of the intermediary's computer resource by any person and that such rules should inform the users of the computer resource not to host, display, upload, modify, publish, transmit or share any information that is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, or otherwise unlawful in any manner whatsoever. These terms have, however, not been defined either in the Rules or in the Information Technology Act, 2000. In the representations made to the Committee, some non-governmental organizations pointed out this and other shortcomings. According to the Ministry of Communications and Information Technology (Deptt. of Electronics & Information Technology) these words / terms are dealt within the Indian constitution and also defined in relevant Indian laws such as Indian Penal Code, Cr. PC, Prevention of Money Laundering Act, etc. It has also been stated that these

words have been interpreted by Hon'ble Supreme Court and High Courts in their various judgements. The Committee would draw the attention of the Ministry of Communications and Information Technology (Deptt. of Electronics & Information Technology) to the recent instances of reported misuse of Section 66A of the IT Act due to absence of precise definitions of terms used in the Section. The Committee would suggest that in order to remove ambiguity/misgivings in the minds of the people, the definition of those terms used in different laws should be incorporated at one place in the aforesaid rules for convenience of reference by the intermediaries and general public. In regard to those terms which are not defined in any other statute, these should be defined and incorporated in the rules to ensure that no new category of crimes or offences is created in the process of delegated legislation.

26. As conveyed by the Secretary, Deptt. of Electronics and Information Technology, there is room for improvement of the intermediary guidelines so that there is no ambiguity. The Committee expect the Ministry of Communications and Information Technology to have a fresh look at the Information Technology (Intermediary Guidelines) Rules, 2011 and make such amendments as necessary to ensure that there is no ambiguity in any of the provisions of the said rules.

B. Disablement of information by the Intermediaries

27. Sub rule (4) of rule 3 of the Information Technology (Intermediaries guidelines) Rules, 2011 reads as under:

> '' 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."

28. Contending that the rule is unreasonable, arbitrary and violates fundamental right of freedom of speech, Software Freedom Law Centre in their written representation submitted as under:

> "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."

29. In response to the above observations that the rule does not provide for an opportunity to the user who has posted the content to reply to the complaint and justify his/ her case and as such the rule is violative of the principle of natural justice and also is highly arbitrary, DeitY in a post evidence reply dated 03.12.12 stated as follows-

"The Cyber space is virtual and anonymous. One can post content by any name using private address. Due to these characteristics and the feature of the technology, it is difficult at times to trace the user who posted the content. Moreover, today technology provides to hide the name of the user and its credential by using virtual private network. Such a technology makes it further difficult to identify the user, even the electronic address, called IP address. Nevertheless, the Rule 3(4) provides that Intermediaries, wherever applicable shall work with the user or owner of such information to disable such information that is in contravention to this Rule (2). As per the Rule, it is the responsibility of the Intermediaries to inform the user and work with them to take a decision as to whether infringing content is to be displayed or not. It may be mentioned here that largely the infringing content is posted on servers installed outside India. It is also observed that the foreign intermediaries, on whose server infringing information is posted, do not cooperate with the Government of India to share the information related to user posting such content. Government of India in past cases, following the rules have tried to contact the user. However, due to non-cooperation of the intermediaries to share the information about the user, it is not possible to contact the user posting objectionable content. It is the responsibility of the Intermediary who knows and has details of the user to work with him to take a decision on the disablement of information. In such a situation, the Ministry does not think the rule is violative of natural justice. Particular reference in this regard is invited to Rule 3(5).''

The Rules have been framed in line with international practice as has been mentioned above. The Intermediaries are free to decide to take appropriate action on the complaint received by them. Wherever applicable, they have to work with the user who posted the information. As it is not mandatory for the Intermediaries to disable the information, the rules do not lead to any kind of censorship. The Rules provide a fair balance between the rights of all the three parties – the Intermediary, the user who posted the information and the user about whom the information has been posted. There are complete checks and balances. The Rules follow the international practice of Internet companies and respect the rights of the parties''

30. In regard to the observation that the words 'obtaining knowledge by itself' implies that the intermediaries should be aware of the nature of the content and are required to delete in case in his /her judgment they fall under any of the categories mentioned in rule 3(2) (b) and as such the act amounts to pre-censorship of the content, DeitY stated in a written reply as under:

‘’The words 'obtaining knowledge by itself' do not imply ‘pre-censorship'. Intermediaries are running business and providing content on commercial basis. Revenue is earned from advertisement posted on content. High Courts have stated that intermediaries must install filters. The companies have installed filters worldwide as per laws of those countries e.g. USA, EU etc. No Indian Intermediary ever raised any issue in this regard. Foreign Intermediaries too are following such a practice worldwide. They have notified such practice under their Terms of use/agreement. ‘’

31. According to Software Freedom Law Centre, 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. It also further stated that such a provision of the rules is liable to be misused and is highly unreasonable and arbitrary. In response to this observation, a representative of Department of Electronics and Information Technology stated during evidence: -

“About the adjudicating powers, these websites provide an ‘abuse’ button on their websites. If anybody has any issue, they report to the ‘abuse’ and social sites take action accordingly. They do delete content and they do update content. We do get complaints that social sites have deleted content without any basis of it. This is a worldwide practice. Our rules reflect the practice world wide. The Rule 3(2) which the hon. Chairman had read out, it says that when an actual aggrieved person brings to the notice of the intermediary, the intermediary will act within 36 hours, wherever applicable and work with the owner of the information to get the information deleted. So, social sites has to work with the owner of the information. This whole area of the cyber space is virtual, border-less and anonymous. In the recent case of Assam, where 310 URLs were blocked for public access we have requesting the social sites to give us the details of persons uploading the information so that we can talk to them. They have said that they come under the US laws. The Mutual Legal Assistance Treaty need to be invoked. Most of the time, information is posted in these sites with anonymous name. If there is an anonymous name, invariably such malicious content is posted anonymously and no details are mentioned there. How do we contact the owner of information? How do we identify that this is the person who has uploaded the information? The first thing is the anonymous names and second is that they do not provide information to you. There was a well thought discussion there. But what should we do when there is anonymity? We advise to the social networking sites and if they feel, they can decide it to delete the information on their sites.

32. The Department of Electronics and Information Technology in a subsequent written reply dated 03.12.12 stated as follows -

> "(c) Intermediaries have to follow the framework provided by these rules and this cannot be considered as adjudicating role. It may be pertinent to say all the major intermediaries across the world have a provision of reporting of objectionable information through 'abuse' facility provided on their website. Based on the complaints received under this 'abuse' facility intermediaries worldwide had decided their course of action about the content. The present rules in no way suggest that intermediaries have to do something other than what they have been doing as per their own norms and policies.''

33. Software Freedom Law Centre, in their written representation contended that sub rule (2) of rule 3 violates the fundamental right to freedom of speech and expression guaranteed to citizens and hence unconstitutional and also *ultra vires* of the parent act. The Software Freedom Law Centre further stated:

> "….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.
>
> 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 36hours…..

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 subsection (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 indirect contravention of Section 69 A of the Act and the rules made there under and is hence ultra vires of the Act."

34**.** Society for Knowledge Commons claimed in their written representation that the onus cast on the intermediaries is impractical and unwarranted and submitted as under –

'' The constitutionality of the Guidelines is open to question given that it empowers and obliges Intermediaries to weed out pernicious or objectionable information on the internet. The onus cast on Intermediaries to act as a policeman of the internet is clearly impractical and unwarranted. With the amount of information available on the internet, it is impossible for an Intermediary to ensure that all content made available to users is inoffensive as per the criteria laid down. (For example, gambling is legal in many countries as is advertising for the same, which is fairly common on popular sports related websites, similarly with alcohol related advertising.) The crucial point here is that the Guidelines fail to mandate any sort of judicial role in the process (the closest concession being a requirement of a "lawful order" by an investigative agency prior to enlisting the aid of any Intermediary). The Intermediary is required to make a judgment on the offensive nature of any information and act to take the offending content offline. The Intermediary may also be required to act upon receiving appropriate requests from the public. This is clearly arbitrary and unconstitutional and has tremendous scope for misuse. To be noted that normally if any person is aggrieved by any information being made public, they may seek remedies—including the relief of injunction—from courts of law, under generally applicable civil and criminal law. There is no rational reason for the inapplicability of such provisions even for information posted on the internet.''

35. In response to the above observation, the DeitY in a post-evidence reply dated 03.12.12 informed as follows -

> "The Rule 3(4) clearly states that Intermediaries 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) shall act within 36 hours and wherever applicable work with the user or owner of such information to disable such information that is contravention to this Rule. This does not provide that the intermediaries have to oblige or act as a policeman to remove the information. The Intermediaries have been operating worldwide. They follow such a practice worldwide to entertain the request for disabling the content. All Intermediaries provide 'abuse' button on their website to enable the users to report the infringing content. There is no provision of counter complaint. Recommendation must be there either for counter complaint or some other mechanism.
>
> The contention made by Society for Knowledge Commons is not in order. It may be mentioned here that all the Indian Intermediaries have implemented these Rules and have not raised any issue at any point of time. The issues are being raised by the Software Freedom Law Centre, which is not an intermediary. The organization is an Indian branch of an organization in USA.''

36. Expressing the view that the existing procedure involved in interception, monitoring and blocking will be rendered useless in view of rule 3(4) , Society for Knowledge Commons, submitted as under –

> "….existing procedure involved in interception, monitoring and blocking under Section 69 and 69A will be rendered useless if information can be censored through the offices of an Intermediary. The current Guidelines completely remove the safeguards contained in Section 69 and rules framed there under, and would make Intermediaries answerable to virtually any request from any source accusing any website of breaching these Guidelines – this could seriously hamper the business of any online website. Pertinent to note that all rules framed by the government that could have the effect of abrogating a citizen's fundamental rights must be fair and reasonable. As laid down by the Supreme Court "procedure which deals with the modalities of regulating, restricting or even rejection; a fundamental right falling within Article 21 has to be fair, not foolish, carefully designed to effectuate, not to subvert, the substantive right itself. Thus, understood, "procedure" must rule out anything arbitrary, freakish or bizarre. A valuable constitutional right can be canalised only by canalized processes."

37. Reacting to the aforesaid views, the Department of Electronics and Information Technology in a post evidence reply stated as follows –

> '' The ambit of Sections 69 & 69A of the Information Technology Act is different from the provisions of Section 79. Section 79 provides safe harbour to the Intermediaries provided they follow certain guidelines and due diligence. Section 69 and 69A, on the other hand, empowers the Government to intercept, monitor, decrypt and block the information for public access respectively under specific conditions. The rules for Section 69 and 69A have been notified in detail.''

38. In response to a query as to whether there is no need of any restrictions on hosting, displaying, uploading modifying publishing, transmitting, updating or sharing the information / content as mentioned in rule 3 (2) (b) , a representative of the Society for Knowledge Commons who appeared before the Committee on 13.08.12 replied as given below –

> "No. I would not say that. I would say that the Government or the Parliament in its wisdom under Section 69(A) has made provisions precisely for this class of items. And that 69A is more than adequate to protect the Indian public from such defamatory material or such hate material or similar kinds of material which may be prejudicial to the sovereignty or interest of the Indian nation. So, that is done under 69A and that is adequate. My problem is that when it is expanded that in lieu of safe harbour what I have to do as a Government, now you should do as an intermediary. It is actually outsourcing Government's censorship responsibilities to private parties who certainly should not be censoring the internet on behalf of the Government.
>
> ..... Sir, if you actually go back to the history how the Government's intercepting, monitoring and blocking powers had been looked at by the courts as well, you had the PUCL case in 1997 which laid down various guidelines regarding phone tapping. Based on those, the Government had pronounced various guidelines even for monitoring and blocking of information on the internet under 69A. So, these basically ensure that there is executive responsibility at some level. The Joint Secretary to the Government has to sign off on any blocking request. What happens is when this is moved to the private sphere is that there are no checks and balances at all in the system, which is essentially against the Supreme Court dicta and against the way our Constitutional scheme functions. What we are doing is that we are leaving every sort of adjudication into the hands of the private player. So, who decides whether something is defamatory or not?"

39. Apprehending that sub rule (4) of rule 3 might result in misuse of the rule by the intermediaries leading to restrictions on freedom of speech, a representative of Society for Knowledge Commons, during the personal hearing stated:

> "Also, Sir, if you notice, the Rules state that the intermediary must act even upon by obtaining knowledge by itself or through notice from any affected party. So, that basically opens up the field for any sort of private complaint including, for example, if I am an employee of, say, Google and I am tolling the internet and I come across something that may or may not be illegal, I do not know, but I can block it. Now you can say that the intermediary has knowledge of itself. So, half the functions, for example, of Google are cataloguing search sites. Now, each one of those would actually mean that Google, even before anyone has complained, will have to take the material offline, if, in its own mind, it thinks that it is illegal. So, the point is that again Google have to make the judgment about what is right and what is wrong."

40. Explaining further, the representative stated -

> "...Shri Sibal has said that it does not want pre-censorship but the Rule, the way it is framed, actually talks about pre-censorship by the intermediaries. Though the Government has clarified that it does not intent for pre-censorship, but if you look at the Rules, it really says that you should do things yourself upon obtaining knowledge by itself. Obtaining knowledge by itself is pre-censorship functions. So, it really makes internet actually non-viable if these Rules are really followed strictly. Of course, we always believe that nobody will really follow them strictly but that is not the way the legal process should be set."

41. A representative of Software Freedom Law Centre, apprehending the likelihood of the misuse of the provision during the personal hearing stated as under:

> ''The issue is that anybody, who is aggrieved by some content, he can just complain to the intermediary, maybe to a Facebook or Google. Within 36 hours, they have to act. They need to act under Section 79 to get the legal liability protection, which was granted by the Legislature. If they do not act within 36 hours, they will lose that protection. That exactly is the problem. You are telling that you act, you get the protection, otherwise, you will not. You take down the content, you get the protection, otherwise you will not.
>
> Anybody who is running a business, he is not bothered about the interest of the users. He always tries to minimise his legal risk. What could happen is that perfectly legal content, perfectly valid content could be taken down.

For example, in a legal case the other party is given a chance to be heard. That is in accordance with the common principles of natural justice that the other side should be heard."

42. Regarding the need for a counter complaint mechanism for a proper redressal of such cases and ensuring that all the interests are balanced, the representative of Software Freedom Law Centre, stated during personal hearing as follows:

"Right now, we only have a complaint mechanism. What we need to have is a complaint and a counter-complaint mechanism so that you can file a complaint and provide the person who generated the content an opportunity to file a counter complaint. Anybody who is putting filthy comments or obscene material will definitely not file a counter-complaint. Those contents can be taken out. But the one who is putting the genuine stuff on the internet, will be affected and he will file a counter complaint. It will ensure that all the interests are balanced. I think rules should ensure that all the interests are balanced."

43. When pointed out that 36 hours prescribed for removal of the said content is enough to inflict damage on the innocents, the representative of Software Freedom Law Centre stated as under:

''I understand that. You take down the content. But, at least after that you can inform the user. Nothing prevents you from doing that. My suggestion is that you take down the content in such cases because the contents can be really bad. I do admit that. The hon. Minister also had explained about that during a meeting. I personally understand that there could be contents which could be really bad, which could hurt religious feelings. But, there could be perfectly valid contents which need not be taken down.

There are cases where perfectly valid contents are taken down. A person does not get any chance to respond to it. My only submission is that let the other party be also given a chance. When there is a dispute, when the other person says that my contents are perfectly valid, they are not illegal, let the courts decide..... If you look at the Copyright Amendment Act which has been recently passed, there is a specific provision which says if somebody complains about a copyright infringement, he has to come back with an order within 21 days, if you do not come back with an order from the court within 21 days, the contents will be restored. Let us have a provision like that. How can an intermediary, a private party, decide issues like defamation? It is difficult for even courts to decide what is defamatory and what is libellous.

One more case that I have relates to a journalist in Mumbai who had uncovered a corruption case involving a corporate based on an RTI request. She had put it up on her

bloc, on her website. She got a take down request from a person representing that company. She could not fight this big company and she had to take down the content because she did not have any other recourse. She cannot respond back.

.....My humble submission to the Committee is that when there are rules, it should be done in a well defined manner. The way it is drafted right now is not clear, it is very ambiguous, it is very vague. It should be made sure that there are specific provisions laid down, specific way for a person who is posting the content to respond back.

The issue is that all the intermediaries, for example, somebody like a BSNL or MTNL who is just providing the connection, he also has the same kind of liability. Just because somebody uses a phone to say filthy things, can BSNL or MTNL be held responsible for that? That is the same issue now. Just because MTNL is providing a connection, how can it be held liable for what a person submits on the web? They are just providing the network to the service. Based on the functions of these intermediaries, their legal liabilities should also differ. The due diligence measures that they need to do should also differ. It should be exactly based on the functions that they do.

Then, rules were also issued in 2009, incorporating these Supreme Court guidelines. Now, these rules have gone exactly against the intention of the Legislature, against Section 69 and against the rules issued under Section 69. So, this is against the current Act. It is *ultra vires* of the Act .''

44. Furnishing the data on the acceptance or otherwise of the requests of the Government of India *vis-a- vis* foreign countries for deleting information from social networking sites and also the need for retaining , sub rule (4) of rule 3 a representative of Department of Electronics and Information Technology deposed as under -

"There is a transparency report published. These social sites publish transparency reports..... None of the social networking sites had deleted the information for India more than 30 per cent. We had some 300 requests as against the thousands of requests in USA or Germany..... This is not a situation where India is trying to misuse or trying to regulate information. In other countries, the requests for disablement are much more. The social sites are themselves providing 'abuse' column to delete the information. Most of the content which is malicious is always posted in anonymous name. How do we handle that situation? This is the situation in the country. We have to provide provision for deletion of information. We have asked social sites to work with the user and act within 36 hours. If some malicious content is posted against me, I have a right for redressal. The hon. Member said very clearly. What happens in that case? He has a right to get the information deleted. Ultimately it is social sites who is providing the platform to post the information. Nobody can compel the service provider to have a

right to post his information. If I want to write an article in the newspaper, it is for the editor to accept whether he will allow me to publicise my article. I do not have a right to get my article published in the news paper without the wishes of Editor. In such situations, a provision has been made to enable deletion of the content. Otherwise, the malicious content will never get deleted because the service provider will say that he does not have a right, he cannot do that. How do we handle such a situation? This whole information is anonymous and borderless. Each content is posted from across the border. Today, I can post the content from India using the anonymous connections also. I can buy a so-called virtual private network from some other country, route my access from one country to another country and post the content. I may be posting information in India but the reflection will be shown in some other country. These are the various complications on the issues which the hon. Members have raised. We need to keep the provision and the information published as part of Transparency Report by these agencies itself is a record that they are not honouring the requests from a country like India more than 30 per cent. They have not even honoured many of the court orders. That is the background. They have to act within 36 hours and dispose the grievance within 30 days. We have provided the Rules to post the grievance officer. All the Indian websites have posted the grievance officer by a particular name. The foreign websites have not agreed. In the recent Assam disturbances, they said that they are deleting the information only because they found it objectionable under their guidelines. They have refused to honour our laws. What should we do in such a situation? At least in the international forum we can say that these are the laws and we have to proceed."

45. With regard to the number of requests given to the intermediaries for deleting objectionable content by the Government of India *vis-a-vis* foreign countries Department of Electronics and Information Technology) furnished the following Information –

Google Transparency Report (January- June, 2011)

Country	Content removal requests	% of removal requests fully or partially complied with	Items Requested to be removed
Brazil	224	67%	689
France	9	78%	250
Germany	125	86%	2,405
India	68	51%	358

Italy	36	86%	80
South Korea	88	84%	646
U.K.	65	82%	333
U.S.	92	63%	757

Google Transparency Report (July - Decembr,2011)

Country	Content removal requests	% of removal requests fully or partially complied with	Items requested to be removed
Brazil	194	54%	554
France	31	55%	61
Germany	103	54%	1722
India	101	29%	255
Italy	28	64%	96
South Korea	94	80%	249
U.K.	49	55%	847
U.S.	187	42%	6192

Twitter Transparency Report (1.1.2012- 30.06.2012)

Country	User information requests	Percentage where some or all information produced	Users/ accounts specified
Australia	<10	33%	< 10
Austria	<10	0%	<10

Brazil	<10	0%	<10
Bulgaria	<10	0%	<10
Canada	<11	18%	12
France	<10	0%	<10
Germany	<10	0%	<10
Greece	<10	33%	<10
India	<10	0%	<10
Indonesia	<10	0%	<10
Italy	<10	0%	<10
Japan	98	20%	147
Korea, Republic of	<10	0%	<10
Mexico	<10	0%	<10
Netherlands	<10	75%	<10
Peru	<10	0%	<10
Portugal	<10	0%	<10
Spain	<10	0%	12
Sweden	<10	0%	<10
Switzerland	<10	0%	<10
Turkey	<10	0%	<10
United Kingdom	11	18%	11
United States	679	75%	946

Total	849	63%	1181

Source http://blog.twitter.com/2012/07/twitter-transparency **-** report.html

46. On the issue of disablement of information which is in contravention of sub rule 2 of rule 3, the Secretary, DeitY, deposed before the Committee as under -

> "Actually, they have to decide their course of action within 36 hours and then they have 30 days to deal with the subject"

47. To a query as to whether the above said position is not included in either sub rule 4 or 5 of rule 3, DeitY stated in a post evidence reply stated as under-

> "(i) The Rule 3(4) requires the Intermediaries to act within 36 hours, and wherever applicable, work with users or owner of such information to disable such information that is in contraction of the Sub-rule (2). The Rules clearly says that Intermediaries "shall act". The meaning of the 'act' is to initiate action and decide course of action within 36 hours. The Rule 3(11) provides that the Intermediaries have 30 days to deal with the subject. In fact, period of 30 days was fixed in consultation with industry associations, though users desired a shorter period to be specified in the Rules to deal with the problem."

48. On being enquired about the feasibility of setting up of "Cyber Ombudsman" on the lines of "Banking Ombudsman" to resolve the likely complaints/disputes arising out implementation of Rule 3 (4) of the Information Technology (Intermediary Guidelines) Rules, 2011, the Ministry of Information and Technology vide its letter DIR ID No. 2(4)/2012-CLFE dated 7.12.2012 inter-alia stated that:-

> "There is no provision in the Information Technology Act, 2000 for setting up of the 'Cyber Ombudsman' on the lines of 'Banking Ombudsman' to resolve any issues arising out of implementation of the Act or rules notified therein. The setting up of 'Cyber Ombudsman' would require amendments in the Information Technology Act, 2000. World over the complaints/disputes on hosting and publication of information/content are only adjudicated either through the process of self-regulation by the content hoster and content provider or through the orders of the Courts. The same processes and practices have been followed and provisions provided in the Information Technology Act, 2000 and the rules notified thereunder."

49. The Information Technology (Intermediaries Guidelines, Rule 3) provides a framework for the due diligence to be observed by the Intermediaries. However, as far as the legal enforceability of these guidelines is concerned, replies of the Department of Electronics and Information Technology present a conflicting

picture. In response to a query as to whether the rule 3 (2) exceeds the mandate of the IT Act, the Ministry of Communications and Information Technology have stated that these guidelines are related to due diligence and safeguards and are only of advisory nature and self regulation. Reiterating the same stance in the context of censorship, the Ministry have replied that as it is not mandatory for the Intermediary to disable the information, the rule does not lead to any kind of censorship. Responding to yet another query about disabling of the said information within 36 hours, the Ministry have stated that the rule clearly says that the Intermediary "shall act" and the meaning of the 'act' is to initiate the action and decide the course of action within 36 hours. Hence, it could be seen that it is mandatory on the part of the Intermediary to disable the information, which in Intermediary's view contravenes the laid down rules/regulations. The Committee feel that there is need for clarity on the aforesaid contradictions and if need be, the position may be clarified in the rules particularly on the process for take down of content and there should be safeguards to protect against any abuse during such process

50. The Ministry of Communications and Information Technology (Department of Electronic & Information Technology) have stated that the foreign intermediaries, on whose server infringing information is posted, do not cooperate with the Govt. of India to share the information related to user posting such content. The foreign websites repeatedly refused to honour our laws and with the result, the malicious content posted on their websites is not removed on the pretext that it does not violate the law of their country . The Committee do not expect an expression of helplessness from the Government in this regard and urge the Ministry of Communications and Information Technology to take such steps as deemed necessary to enlist their co-operation.

C. Exceeding the delegated authority.

51. Software Freedom Law Centre in their written representation, contending that rule 3 (4) is *ultra vires* of the Constitution, submitted as under:

" 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 there under. 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."

52. Questioning the constitutionality of the intermediaries' guidelines Society for Knowledge Commons**,** in their written representation on the said guidelines submitted as under –

> '' Further, the constitutionality of the Guidelines may also be called into question on the grounds that they enlarge and expand the scope of the IT Act beyond what was originally

envisaged. The Government is empowered by the IT Act to frame guidelines for the process of due diligence by Intermediaries. The present Guidelines however go well beyond the scope of what could normally be considered "due diligence" and have widened the scope of the IT Act by listing a broad list of information that can be considered unlawful and then requiring Intermediaries to act as a policing agency of the state. It is a settled principle that the conferment of rule-making power by an Act does not enable the rule-making authority to make a rule which travels beyond the scope of the enabling Act or which is inconsistent there with or repugnant thereto. As noted by the Supreme Court, a delegate who has been authorized to make subsidiary rules and regulations has to work within the scope of its authority and cannot widen or constrict the scope of the parent Act or the policy laid down there under. It cannot, in the garb of making rules, legislate on the field covered by the parent Act and has to restrict itself to the mode of implementation of the policy and purpose of the parent Act.

53. In response to a query as to why no elaborate procedure for disabling the said information is not specified similar to the procedure prescribed for blocking under section 69A for the purposes mentioned therein , DeitY, in a written reply stated as under-

"This provision requires intermediary to initiate action for disablement of objectionable content. The requestor or affected person has to clearly mention the content or the exact webpage link/URL for disablement of objectionable content.

Therefore, the Intermediary certainly is notified by the affected person about the exact webpage link for disablement of objectionable content. It may also be mentioned here that the Rule 3(4) also states that the affected person has to report the matter in writing or through email signed with electronic signature and the Intermediary where applicable, work with user or owner of such information that is contravention to the rules.

It may be noted that the provisons of section 69A and those of section 79 operate in different environment and conditions. The section 69A provides power to the Govt. to block the information under five specific conditions namely – (i) in the interest of sovereignty and integrity of India, (ii) defence of India, (iii) security of the State, (iv) friendly relations with foreign states or (v) public order or for preventing incitement to the commission of any cognizable offence relating to above.

The Section 79 on the other hand is of generic nature under which any affected person can lodge a complaint and request intermediaries to remove the objectionable

content from their website. Intermediary under this section has the right to take action where applicable. Therefore the two sections operate and apply in different conditions.''

54. Contending that the provisions of sub rule (4) of rule 3 of the Information Technology (Intermediaries Guidelines) Rules, 2011 go beyond the mandate of the IT Act, 2000, a representative of the Society for Knowledge Commons who appeared before the Committee stated as follows -

" Mr. Chairman, first of all, the reason that we have raised issues with the IT Rules is that we believe that it goes beyond what the IT Act intended. If you look at the IT Act, the provision of Section 79, which is called safe harbour provisions, came for intermediaries because intermediaries are precisely those who do not participate in creating content on the internet. That means, if I look at an intermediary, the intermediary is an Internet Service Provider who brings connectivity to internet. It could be search engines like Google or it could be blogspot.com where a number of people post their views. They neither publish nor edit nor create information directly. They are essentially pipes which bring information which somebody else has created to us as consumers. So, effectively they are a link between the creator of the information and the user of the information and they are called intermediaries. It is just like the newspaperwala who gives us the newspaper in the morning every day. He is not responsible for the content.

When the intermediary, who is an Internet Service Provider or it is a company like Google or Yahoo, obviously they are much larger in size.

So, if you look at the purpose of information as published, whether it is a newspaper or it is internet, it should be treated similarly. That means if there is freedom of speech for a newspaper, what I post on the internet, I am liable as if I posted information like any author of an article in the newspaper. The publisher, if the person who is running the website is moderating, editing the material, looking at what is being published, taking a decision whether it should or should not be published, then he or she is also responsible for the material and content being published. But those who are acting just as passive pipes, they should not be responsible for fulfilling certain functions, which are my responsibilities as a user. My responsibility is the creator of the content. So, the creator of the content, like newspaper articles, like authors have responsibilities, that responsibility cannot go to intermediary….

…..So, on that the Parliament took cognizance and passed essentially the safe harbour provision in the IT Act to protect the intermediaries from these kinds of lawsuits because without this protection it is accepted that intermediaries cannot be in business. So if you accept that today internet is importing for the economy of a country and everybody accepts that then obviously intermediaries who are performing a very vital role in bringing the internet to us, there could be that specific safe harbour provision which Parliament, in its wisdom, has passed.

Now, what the IT Rules do in effect is take the safe harbour provision which was created to protect the intermediaries and say that you will get the safe harbour protection provided you yourself perform certain censorship functions. Now, effectively it means that the intermediary is now being used to censor content and a task for which there is no provision in Indian law that he should do this exercise. This censorship function is either an Executive/Government function or a court function. Therefore, extending this to private censorship means that I have no redress as a user if the intermediary is supposed to perform this function.

So, I think in terms of the basic intent of the Parliament's Act of providing safe harbour and using the safe harbour for private censorship, I think, the rules have ostensibly expanded what its real task is. Legally, the subordinate legislation cannot create new rights or liabilities. I think it went beyond by creating certain scope for intermediary rules, created certain specific provisions which were not envisaged under the Act of the Parliament. So, I think, there is basically a constitutional issue involved here."

55. The Department of Electronics and Information Technology (DeitY), in post evidence reply to a query on the above mentioned observation / opinion stated as under:

''The Information Technology (Intermediaries Guidelines) Rules, 2011 primarily provide a framework for the due diligence to be observed by the Intermediaries. It is pertinent to mention that Rule 3(1) states "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" and Rule 3(2) provides that "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 **……..**". These Rules are only of advisory nature and self-regulation.

Sub-section 2(C) of Section 79 of the Information Technology Act, 2000 provides that "The Intermediaries observe due diligence while discharging their duties under this Act and also observe such other guidelines as the Central Government prescribed in this behalf." The

Rules have been prescribed strictly within the ambit of the principal Act. The rules intend to promote self-regulation by the end users and the intermediaries, and are not in the nature of regulation by the Government. The guidelines are related to due diligence and safeguards and are only of advisory nature and self-regulation. The Rules have been framed under Section 79. The Sections 67C, 69A and 69B deal with entirely different situations and should not be linked with Section 79. The contentions made by Software Freedom Law Centre in their written representations, are, therefore, not correct.''

56. The Ministry has also informed in a written reply that "rules under Section 79 in particular have undergone scrutiny by High Courts in the country. Based on the Rules, the courts have given reliefs to a number of individuals and organizations in the country. No provision of the Rules notified under Sections 43A and 79 of the IT Act, 2000 have been held ultra vires."

Right to terminate the access or user rights of the users to the computer resources of the intermediary

57. Sub Rule (5) of Rule 3 of the Information Technology (Intermediaries Guidelines) Rules, 2011 reads as under –

> ''(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."

58. Software Freedom Law Centre in their written representation on the above rule, stated as under:

> "1. The rule is arbitrary
>
> …. 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….."

59. Society for Knowledge Commons in their written representation stated that current guidelines completely remove the safeguards contained in section 69 of the Information Technology Act, 2000 and rules framed there under, and would make intermediaries answerable to virtually any request from any source accusing any website of breaching these guidelines hampering the business of any online website.

60. The DeitY in a written reply regarding the above mentioned point stated as under-

"Society for Knowledge Commons, an NGO appears to have misinterpreted the provisions of Sub Rule (5) of Rule 3. The provisions included in Sub-rule (5) of Rule 3 are identical to the provisions included by Internet mega companies in their terms of use/agreement. As has been said earlier, the attempt of Govt. of India has been to harmonize the guidelines and procedure for due diligence with those prevailing internationally and being implemented by the Internet mega companies. This provision of Sub-rule (5) of Rule 3 has been designed accordingly.

Accordingly, it may be pointed out that Section 69 provides safeguards for very specific type of information viz. that affecting the interests 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 these or for investigation of any offence. It may be noted that all the Internet mega intermediaries in their terms and conditions for the users retain the right to terminate the access and uses of their computer resource and remove non-compliant information.''

D. Cost of Operations and Sustainability of Small companies

61. Rule 3 of Information Technology (Guidelines for Cyber Café) Rules, 2011 which requires the registration of Cyber cafe reads as under:

> ''Agency for registration of cyber café.— (1) All cyber cafes shall be registered with a unique registration number with an agency called as registration agency as notified by the Appropriate Government in this regard. The broad terms of registration shall include:
>
> (i) name of establishment;
>
> (ii) address with contact details including email address;
>
> (iii) whether individual or partnership or sole proprietorship or society or company;
>
> (iv) date of incorporation;
>
> (v) name of owner/partner/propertier/director;
>
> (vi) whether registered or not (if yes, copy of registration with Registrar of Firms or Registrar of Companies or Societies); and
>
> (vii) type of service to be provided from cyber café
>
> Registration of cyber café may be followed up with a physical visit by an officer from the registration agency.
>
> (2) The details of registration of cyber café shall be published on the website of the registration agency.
>
> (3) The Appropriate Government shall make an endeavour to set up on-line registration facility to enable cyber café to register on-line.
>
> (4) The detailed process of registration to be mandatorily followed by each Registration Agency notified by the Appropriate Government shall be separately notified under these rules by the central Government"

62. In response to a query as to whether such a registration requirement for cyber cafes will have adverse impact on the internet penetration in non-metro cities and rural areas , DeitY, in a written reply stated as follows –

> "A number of cases in the past have been observed where the miscreants and terrorists use Cyber Cafes for posting/sending emails or posting any information which is detrimental to the peace & harmony and sovereignty of the country. The police officials struggle to

find the evidence in such cases, as a result of which almost all the States have framed regulations therein requiring Cyber Cafes to be registered with certain agencies in the State Govt. so that bonafide of the Cyber Café could be ascertained and information could be obtained from them as and when needed. Every state has followed different procedure for registration of the Cyber Cafes. Some states are registering Cyber Cafes under the Police Act and some are registering under Companies Act. There is no uniform process followed in this regard across the country. As a result of which the Central agencies find it difficult to investigate such cases. Similarly State Govt. has difficulty when investigating cases relating to law and order which has origin in different States. The Cyber Café rules were framed with the objective to streamline and harmonize the process across the country so that Cyber Cafes will clearly identifiable across the country.

The registration process has been simplified. Any person intending to set up a Cyber Café will have to fill a form in a prescribed format, based on which the Cyber Café will be registered. The process is simple and does not involve any inspection at the time of granting registration of Cyber Café. The process has been prescribed in a simplistic manner so that it does not harm growth of Internet penetration in India. The whole position can be monitored and corrective steps can be taken after sometime if the rules are found to impeding the growth of Internet business in India. In any way, Cyber Cafés are required to follow certain procedural aspects and register their establishment under the Shop and Establishment Act/Companies Act as the case may be"

63. Rule 5 Information Technology (Guidelines for Cyber Café) Rules, 2011 which prescribes maintenance of the log register containing the details of the users reads as under-

"5. Log Register.— (1) After the identity of the user and any person accompanied with him has been established as per sub-rule (1) of rule 4, the Cyber Café shall record and maintain the required information of each user as well as accompanying person, if any, in the log register for a minimum period of one year.

(2) The Cyber Café may maintain an online version of the log register. Such online version of log register shall be authenticated by using digital or electronic signature. The log register shall contain at least the following details of the user, namely :

(i) Name

(ii) Address

(iii) Gender

(iv) Contact Number

(v) Type and detail of identification document

(vi) Date

(vii) Computer terminal identification

(viii) Log in Time

(ix) Log out Time

(3) Cyber Café shall prepare a monthly report of the log register showing date wise details on the usage of the computer resource and submit a hard and soft copy of the same to the person or agency as directed by the registration agency by the 5th day of next month.

(4) The cyber café owner shall be responsible for storing and maintaining backups of following log records for each access or login by any user of its computer resource for at least one year:-

(i) History of websites accessed using computer resource at cyber café;

(ii) Logs of proxy server installed at cyber café.

Cyber Café may refer to "Guidelines for auditing and logging – CISG-2008-01"prepared and updated from time to time by Indian Computer Emergency Response Team (CERT-In) for any assistance related to logs. This document is available at www.cert-in.org.in

(5) Cyber café shall ensure that log register is not altered and maintained in a secure manner for a period of at least one year.

64. Expressing apprehension that many small internet companies may not be in a position to comply with the proposed rules as it involves extra cost and likely adverse impact on the sustainability of operations of these small companies, a representative of Society for Knowledge Commons appearing before the Committee on 13.08.12 stated as under –

"....in economic terms, the freedom of the internet is such that if I put onerous duties on intermediaries, Indian intermediaries will not be able to do it because they will be small, they will be start-ups. Only companies of the size of Google and Yahoo may be able to do it.

They have the ability to do that if they want. If we put legal duties on them, they can at least spend money. So, they may find material of different kinds like automated searching. If you look at the material that comes, today in one minute 60 hours of You Tube videos are put up, probably in something like 200 languages. It is humanly impossible for people to really go through that and find out what is

offensive; what is blasphemous; and what is harassing and so on. If you insist Google does this then the Google will put some automated search words, search things and so on and by virtue of which it will spend may be 100 million dollars but considering that it gets about a revenue of 14 billion dollars for advertisements it may still be able to do it. But anybody who wants to put up something like this cannot really do it. So, what effectively we will do is we will allow the internet intermediaries to be only large and big players no small company giving small service. For instance, if I put a news blog on the website – I am an intermediary by virtue if I allow people to post comments – comments are what actually drive sites, the discussion, debate that is what people come to site for. If I have to monitor comments, I cannot automatedly monitor it. I cannot employ people to monitor all the comments so effectively I disable comments, which means, the news website then has much less value then somebody who sets up that website say in Thailand or somewhere else and, therefore, allows free comment and so on.

I think, in business terms for India there is a case for making internet much more free; allowing freedom of the internet and in any case under Indian law that is the intent of what 19(2) is that restrict very lightly what is Freedom of Expression. Yes, Freedom of Expression needs to be restricted if it is hate speech, if it is pedophelia and so on. Apart from this very strict classification, which the Supreme Court has also pinioned on, I think, rest of it should be left open and this should not be private censorship of intermediaries should not come in into play.

So, I think, the Parliament had done a legislation which was in intent, absolutely correct. It allowed the safe harbour provision; it had the provision under 69(A) for even censorship. If there is an emergency measure to immediately act the Executive is allowed to act immediately. All these provisions are well thought out and given. But 79 through rules what has been done is expansion of the safe harbour to private censorship, making it vague and, therefore, creating a regime, in which, then the intermediary will tend to take down any objection that is given, and, therefore, destroying the ability of the internet today to be a vibrant forum for democratic exchanges. I think, this is not the intent of the Parliament's Act and rules have been framed without adequate application of mind. This is what, at least, as a Committee, you do recommend to the Government to relook at this internet rules, the intermediary guidelines, then, I think, it will be doing enormous benefit.''

65. Sub rules (2), (3) & (5) of rule 4 and rule 5 of the said rules prescribes the maintenance of records of the user identification, installation of cameras for photographing the users , maintenance of the log book etc, for a period of one year. In response to a query as to whether such measures increase the cost of operations of

the Cyber Cafes resulting in adverse impact on their operations on sustainable basis and also whether police are empowered to search the Cyber Cafes, the representative of Department of Electronics and Information Technology during the evidence held on 20.09.12 stated as follows -

> "There is no clause in the rules which provides that the police can search. The rules make registration necessary. He need not visit any authority for registration. On-line registration can be done. Afterwards, the officer of the Government can visit that place. Only registration is there. This aspect of keeping the records for one year has been debated. Again, we have had consultations with all the associations. The police agencies are very emphatic about it because it takes time to get the collection of evidence which has to be produced. They have to keep an authorised person to enter it. A number of cases happen. Many of the things happen only from the cyber café. They are not able to trace the person who enters, who uses the system. So, it is precisely for the police requirement, security requirement that we have to prescribe the data. In any way, the cyber cafes are of the kind of firms, companies or individual people. They have to make records ready for the Sales Tax, VAT or Income-tax purposes. They have to maintain the records for seven years or three years depending upon whether they are dealing with VAT or Income-Tax. This is only for one year that one has to maintain the records. Today, the whole data is to be maintained for one year in a small disc which does not cost much. Software is available in the market. He has to maintain a small disc costing Rs.5000/- There is a small, hard disc in the computer. This hard disc is costing Rs.5000-7000 depending on the capacity. He can maintain the data there. We can certainly help them if there is any issue - how to do that. But it does not need much time because today storage system costs this much amount only. This is a requirement because records have to be produced in the court. So, it is maintained only for one year. This is in line with the Telecom licensing policy where the service provider has to maintain the data for a certain period.''

66. When pointed out that adherence to the rules may increase the cost of setting up, operation, and maintenance / compliance cost of cyber cafes and this may reportedly have adverse impact on the growth of Cyber Cafes and also the penetration of internet in the country, DeitY in post evidence reply stated as follows-

> ''The provisions have been made in the Rules for Cyber Cafes in creating a balance between the requirement of Law Enforcement Agencies, users interest, cost and growth of Cyber Cafes and there is growth in penetration of Internet in the country.''
>
> The Department (DeitY) keeps on interacting with associations in the area to monitor the impact of rules. So far no adverse impact of the rules on Cyber Café has been brought to the notice of DeitY. No Cyber Café also has reported any difficulty in compliance of the rules.''

67. The Committee are of the view that cost involved in complying with the aforementioned rules for maintenance of log register, keeping record of user identification documents, maintenance of record of staff for a year, installation of web camera is bare minimum to have any adverse impact on the penetration of internet especially in rural areas in the country. The Committee agree with the Government that these rules balance the interests of stakeholders - law enforcement agencies, internet users and Cyber Cafes.

E. Need for amending the rule for protecting the Privacy of the net users in Cyber Cafes

68. Sub rule (2) of rule 6 of Information Technology (Guidelines for Cyber Café) Rules, 2011, prescribes that the screen of all computers installed other than in Partitions or Cubicles shall face 'outward' *i.e.* they shall face the common open space of the Cyber café.

69. As per Rule 6(5) of the Information Technology (Guidelines for Cyber Cafe) Rules, 2011, Cyber Cafes are required to be equipped with a commercially available safety or filtering software so as to avoid as far as possible access to the websites relating to pornography including child pornography or obscene information.

70. In this regard, Society for Knowledge Commons in their written representation expressed the following view:

> ''these rules appear impractical given that (a) they would allow every computer screen to be seen by a bystander thereby invading the privacy and security of every user (b) may pose practical problems for small cyber cafes, (C) filtering software is far from perfect and tends to censor a lot of necessary, useful, and completely inoffensive material (for example medical information may be censored as pornography)"

71. In response to the above observation of the NGO, DeitY in a written reply dated 03.12.12 stated as under-

> ''Installation of filtering software is not mandatory. The Rules uses the word "may" and hence installation of safety or filtering software is optional. An analogy can be drawn in that child pornography is a serious offence in all the countries. All the intermediaries operating internationally deploy the software to filter child pornography images and information. The deployment of such a software is mandatory in USA and EU. The issue raised by Society for Knowledge Commons can certainly considered to be analogous to the issue of handling child pornography on the internet. The filtering of child pornography is complete and would certainly be affecting the medical information pertaining to child as mentioned by the Society for Knowledge Commons''

72. According to sub rule (2) of Rule 6 of Information Technology (Guidelines for Cyber Café) Rules, 2011, screens of the computers installed other than in partitions and cubicles should face open space of the cyber café. Such an arrangement would obviously allow every computer screen to be seen by bystander thereby invading privacy and security of every user. The Committee, would suggest that the sub-rule (2) of Rule 6 be modified suitably to ensure that privacy of the users is not intruded for legitimate purposes.

F. Constitution of Cyber Regulations Advisory Committee (CRAC)

73. Section 88 of the Information Technology Act, 2000 provides for constitution of Cyber Regulations Advisory Committee (CRAC) to advise the Central Government either generally as regards any rules or for any other purpose connected with the Act and the Controller in framing the regulation under the Act. The CRAC among others shall consist of members representing the interests principally affected or having special knowledge of the subject matter.

74. In response to queries as to whether CRAC has been constituted and whether the Government have got any advice from CRAC, the Secretary , Department of Electronics and Information Technology, deposed before the Committee as under:

> "First of all, I would like to say about the Cyber Advisory Committee. It was provided under the Act. It was constituted but it is a fact that it has not met very frequently and the intention is to reconstitute it at this point of time. We will make it functional and able to give positive suggestions for improvement of these rules."

75. Adding further, the Secretary stated as under:

> "... But on 3rd of August, it was also pointed out about the need to reconstitute this Committee. It was in principle decided."

76. Giving details of the CRAC, a representative of Department of Electronics and Information Technology stated as follows:

> "The Cyber Advisory Committee was constituted when the main Act was enacted on 17th October, 2000. The hon. Minister is the Chairman and all industry associations are members, apart from some key Ministries like MHA, Ministry of Finance, Ministry of I & B and DoT. This Committee did meet when we were making regulation at that point of a time in 2000. It had two meetings in the year 2000 and 2001. Thereafter, no meeting was held primarily because the rules and regulations were not formed. The Act was then amended in 2008 and notified in 2009."

77. Adding further, the representative stated as under-

'' When we talk about these rules, we had been consulting these rules with the Industry Associations and other stakeholders for more than a year. It is a difficult subject. We have been consulting each and every stakeholder through every means. We ask them to give us an approach paper on how the rules are to be framed. We studied the practices which major social networking sites follow in their own countries. Thereafter, we had framed the rules and those draft rules were put on the website.

It was put for more than three months and the comments were obtained. We revised the draft. The revised draft was also sent to the key industry association which deals with this subject. They had agreed to it and only then we went ahead notifying Rules. The members of the Advisory Committee, are the same key industry associations to whom we have sent draft Rules. So, it was the view that we have obtained in writing from the associations and we got the confirmation and they okayed the rules, there may not be need of convening meeting of Advisory Committee. The other Ministries also participated in that. It was thought that we can straightaway go and notify the rules. That was the basic intent because all consultation process was done. Now this Committee is in the process of revising it and certainly we will hold their views. This is a subject which needs to be updated regularly. Technology is changing very fast and a lot more needs to be done. Certainly we will be consulting the Advisory Committee. I have given the reason as to why we did not convene the Advisory Committee specifically because all the members were consulted not once but three times in the process of one and a half years."

78. In this regard, in a post evidence reply the Department of Electronics and Information Technology stated as follows -

"The Cyber Regulation Advisory Committee has been reconstituted. The meeting of the Cyber Regulation Advisory Committee with the convenience of Chairman and other Members has been held on 29.11.12."

79. Section 88 (1) of the Information Technology Act requires constitution of Cyber Regulations Advisory Committee (CRAC) to advise the Central Government either generally as regards any rules or for any other purpose connected with the Act. The Committee are distressed to note that though the Cyber Regulation Advisory Committee (CRAC) was constituted when the IT Act was enacted in the year 2000, it met only twice, once in the year 2000 and then in 2001 and thereafter, no

meeting was held. The CRAC has since been reconstituted after the matter has been taken up by this Committee. The Committee would impress upon the Ministry of Information Technology (Department of Electronics & Information Technology) to make the CRAC functional and benefit from its advice particularly in the context of having a fresh look at the rules and amendment of rules recommended in this report.

80. The CRAC reportedly consists of the Minister of Communications and Information Technology, members drawn from the Industry Associations and key Ministries of the Government. It is not clear from the information furnished by the Department whether, in the reconstituted CRAC, there are members representing the interests of principally affected or having special knowledge of the subject matter as expressly stipulated in Section 88(2) of the IT Act. The Committee hope that this requirement has been met in the composition of the CRAC. The Committee would like to be informed of the position in this regard.

G. Delay in framing of Rules.

81. Section 70A of the IT Act empowers the Central Government to designate any organization of the Government as national nodal agency in respect of Critical Information Infrastructure Protection. Section 70 B of the Act empowers the Government to appoint an agency of the Government to be called Indian Computer Emergency Response Team (ICERT) to serve as the national agency for performing the functions mentioned therein in the areas of cyber security which includes *inter- alia* coordination of cyber incidents response activities. The aforesaid section of the Amendment Act, 2008 came into effect on 5 February, 2009. The manner of performing functions and duties of the Critical Information Infrastructure Protection Agency in terms of Section 70 A (3) and salary and allowances and terms and conditions of the Director General and other officers and employees of Indian Computer Emergency Response Team in terms of Section 70 (B) (3) are required to be prescribed. In response to a query as to whether the rules required to be notified under section 70 A (3) &70 B (3) have been notified, the Department of Electronics and Information Technology vide their written communication dated 3.12.12 stated as follows-

> "Draft of rules under section 70A and 70B have been prepared. Notes for Cabinet Committee on Security for approval of draft rules for these two sections have been circulated to concerned Ministries/Departments for comments. The comments from Ministries/Departments are awaited."

82. The Committee are constrained to note that the rules required to be framed under sections 70A (3) and 70 B (3) of the IT Act regarding the manner of performing functions and duties of "Critical Information Infrastructure Protection Agency" and terms and conditions of employees of "Indian Computer Emergency Response Team" have not been framed even three and half years after notification of the Act in February, 2009. The Committee have emphasized time and again that rules should invariably be notified within six months after the notification of the Act. The delay by the Department of Electronics and Information Technology in notification of the Rules even after lapse of such long period reflects lack of seriousness of the Ministry in fully implementing all provisions of the IT Act. The

Committee require the Ministry of Information Technology to take urgent steps to ensure that rules in this regard are finalized and notified without any further delay.

P. KARUNAKARAN,
CHAIRMAN,
COMMITTEE ON SUBORDINATE LEGISLATION

New Delhi;
March, 2013
Phalguna, 1934 (Saka)

APPENDIX –I

(Vide Para 7 of the Introduction of the Report)

SUMMARY OF RECOMMENDATIONS MADE IN THE THIRTY- FIRST REPORT OF THE COMMITTEE ON SUBORDINATE LEGISLATION

(FIFTEENTH LOK SABHA)

Sl. No.	Reference to Para No. in the Report	Summary of Recommendations
1	2	3
A.	25	**Definitions of terms** **The Committee note that Rule 3 of the Information Technology (Intermediaries Guidelines) Rules, 2011 requires intermediary to publish rules and regulation etc. for access of the intermediary's computer resource by any person and that such rules should inform the users of the computer resource not to host, display, upload, modify, publish, transmit or share any information that is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, or otherwise unlawful in any manner whatsoever. These terms have, however, not been defined either in the Rules or in the Information Technology Act, 2000. In the representations made to the Committee, some non-governmental organizations pointed out this and other shortcomings. According to the Ministry of Communications and Information Technology (Deptt. of Electronics & Information Technology) these words / terms are dealt within the Indian constitution and also defined in relevant Indian laws such as Indian Penal Code, Cr. PC, Prevention of Money Laundering Act, etc. It has also been stated that**

	26	**these words have been interpreted by Hon'ble Supreme Court and High Courts in their various judgements. The Committee would draw the attention of the Ministry of Communications and Information Technology (Deptt. of Electronics & Information Technology) to the recent instances of reported misuse of Section 66A of the IT Act due to absence of precise definitions of terms used in the Section. The Committee would, suggest that in order to remove ambiguity/misgivings in the minds of the people, the definition of those terms used in different laws should be incorporated at one place in the aforesaid rules for convenience of reference by the intermediaries and general public. In regard to those terms which are not defined in any other statute, these should be defined and incorporated in the rules to ensure that no new category of crimes or offences is created in the process of delegated legislation.** **As conveyed by the Secretary, Deptt. of Electronics and Information Technology, there is room for improvement of the intermediary guidelines so that there is no ambiguity. The Committee expect the Ministry of Communications and Information Technology to have a fresh look at the Information Technology (Intermediary Guidelines) Rules, 2011 and make such amendments as necessary to ensure that there is no ambiguity in any of the provisions of the said rules.**
B.	**49**	**<u>Disablement of information by the Intermediaries</u> The Information Technology (Intermediaries Guidelines, Rule 3) provides a framework for the due diligence to be observed by the Intermediaries. However, as far as the legal enforceability of these guidelines is concerned, replies of the Department of Electronics and Information Technology present a conflicting picture. In response to a query as to whether the rule 3 (2) exceeds the mandate of the IT Act, the Ministry of Communications and Information Technology have stated that these guidelines are related to**

		due diligence and safeguards and are only of advisory nature and self regulation. Reiterating the same stance in the context of censorship, the Ministry have replied that as it is not mandatory for the Intermediary to disable the information, the rule does not lead to any kind of censorship. Responding to yet another query about disabling of the said information within 36 hours, the Ministry have stated that the rule clearly says that the Intermediary "shall act" and the meaning of the 'act' is to initiate the action and decide the course of action within 36 hours. Hence, it could be seen that it is mandatory on the part of the Intermediary to disable the information, which in Intermediary's view contravenes the laid down rules/regulations. The Committee feel that there is need for clarity on the aforesaid contradictions and if need be, the position may be clarified in the rules particularly on the process for take down of content and there should be safeguards to protect against any abuse during such process.
	50	**The Ministry of Communications and Information Technology (Department of Electronic & Information Technology) have stated that the foreign intermediaries, on whose server infringing information is posted, do not cooperate with the Govt. of India to share the information related to user posting such content. The foreign websites repeatedly refused to honour our laws and with the result, the malicious content posted on their websites is not removed on the pretext that it does not violate the law of their country . The Committee do not expect an expression of helplessness from the Government in this regard and urge the Ministry of Communications and Information Technology to take such steps as deemed necessary to enlist their co-operation.**

D	**67**	**<u>Cost of Operations and Sustainability of Small companies</u> The Committee are of the view that cost involved in complying with the aforementioned rules for maintenance of log register, keeping record of user identification documents, maintenance of record of staff for a year, installation of web camera is bare minimum to have any adverse impact on the penetration of internet especially in rural areas in the country. The Committee agree with the Government that these rules balance the interests of stakeholders - law enforcement agencies, internet users and Cyber Cafes.**
E	**72**	**<u>Need for amending the rule for protecting the Privacy of the net users in Cyber Cafes</u> According to sub rule (2) of Rule 6 of Information Technology (Guidelines for Cyber Café) Rules, 2011, screens of the computers installed other than in partitions and cubicles should face open space of the cyber café. Such an arrangement would obviously allow every computer screen to be seen by bystander thereby invading privacy and security of every user. The Committee, would suggest that the sub-rule (2) of Rule 6 be modified suitably to ensure that privacy of the users is not intruded for legitimate purposes.**
F	**79**	**<u>Constitution of Cyber Regulations Advisory Committee (CRAC)</u> Section 88 (1) of the Information Technology Act requires constitution of Cyber Regulations Advisory Committee (CRAC) to advise the Central Government either generally as regards any rules or for any other purpose connected with the Act. The Committee are distressed to note that though the Cyber Regulation Advisory Committee (CRAC) was constituted when the IT Act was enacted in the year 2000, it**

		met only twice, once in the year 2000 and then in 2001 and thereafter, no meeting was held. The CRAC has since been reconstituted after the matter has been taken up by this Committee. The Committee would impress upon the Ministry of Communications and Information Technology (Department of Electronics & Information Technology) to make the CRAC functional and benefit from its advice particularly in the context of having a fresh look at the rules and amendment of rules recommended in this report.
	80	**The CRAC reportedly consists of the Minister of Communications and Information Technology, members drawn from the Industry Associations and key Ministries of the Government. It is not clear from the information furnished by the Department whether, in the reconstituted CRAC, there are members representing the interests of principally affected or having special knowledge of the subject matter as expressly stipulated in Section 88(2) of the IT Act. The Committee hope that this requirement has been met in the composition of the CRAC. The Committee would like to be informed of the position in this regard.**
G		**<u>Delay in framing of Rules</u>**
	82	**The Committee are constrained to note that the rules required to be framed under sections 70A (3) and 70 B (3) of the IT Act regarding the manner of performing functions and duties of "Critical Information Infrastructure Protection Agency" and terms and conditions of employees of "Indian Computer Emergency Response Team" have not been framed even three and half years after notification of the Act in February, 2009. The Committee have emphasized time and again that rules should invariably be notified within six months after the notification of the Act. The delay by the Department of Electronics and Information Technology in notification of the Rules even after lapse of**

		such long period reflects lack of seriousness of the Ministry in fully implementing all provisions of the IT Act. The Committee require the Ministry of Information Technology to take urgent steps to ensure that rules in this regard are finalized and notified without any further delay.

APPENDIX – II

(Vide Para 8 of the Introduction of the Report)

MINUTES OF THE EIGHTH SITTING OF THE COMMITTEE ON SUBORDINATE LEGISLATION (2011-2012)

_____

The Eighth sitting of the Committee held on Monday, the 13th August, 2012 from 1500 to 1605 hours in Committee Room 'E'. Parliament House Annexe, New Delhi.

PRESENT

1. Shri P. Karunakaran — Chairman

MEMBERS

LOK SABHA

2. Shri Kalyan Banerjee
3. Shri Ramen Deka
4. Shri Mahesh Joshi
5. Shri Virendra Kashyap
6. Dr. Thokchom Meinya
7. Shri Gajendra Singh Rajukhedi
8. Dr. Bhola Singh
9. Shri Vijay Bahadur Singh
10. Shri A.K.S. Vijayan

SECRETARIAT

1. Shri S.C. Chaudhary - Director
2. Shri Srinivasulu Gunda - Additional Director
3. Shri Krishendra Kumar - Under Secretary

2. At the outset, the Chairman welcomed the Members of the Committee

3. Thereafter, representatives of 'The Society for Knowledge Commons' were called in. The following persons were present:

1 Shri Prabir Purkayastha – Chairperson, Society for Knowledge Commons

2. Shri Rishab Bailey - Member, Society for Knowledge Commons

4. The Committee heard their views on (i) 'the Information Technology (Intermediary Guidelines) Rules, 2011', and; (ii) 'the Information Technology (Guidelines for Cyber Cafes) Rules, 2011'.

The witnesses then withdrew.

5. Thereafter, representatives of the 'Software Freedom Law Centre' were called in. The following persons were present:-

1. Shri Prasanth Sugathan – Counsel, Software Freedom Law Centre

2. Ms. Amrita Jayaram – Counsel, Software Freedom Law Centre

6. The Committee heard their views on 'the Information Technology (Intermediary Guidelines) Rules, 2011'.

7. The witnesses then withdrew.

8. A verbatim record of the sitting has been kept.

The Committee then adjourned.

MINUTES OF THE TENTH SITTING OF THE COMMITTEE ON SUBORDINATE LEGISLATION (2011-2012)

_____

The Tenth sitting of the Committee held on Thursday, the 20th September, 2012 from 1500 to 1610 hours in Room No. 53, Parliament House, New Delhi.

PRESENT

1. Shri P. Karunakaran — Chairman

MEMBERS

LOK SABHA

2. Shri Kalyan Banerjee
3. Shri E.T. Mohammed Basheer
4. Shri Mahesh Joshi
5. Dr. Thokchom Meinya
6. Shri Gajendra Singh Rajukhedi
7. Dr. Bhola Singh
8. Shri Vijay Bahadur Singh

SECRETARIAT

1. Shri S.C. Chaudhary - Director
2. Shri Srinivasulu Gunda - Additional Director
3. Shri Krishendra Kumar - Under Secretary

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(DEPARTMENT OF ELECTRONICS AND INFORMATION TECHNOLOGY)

1	Shri J. Satyanarayanan	-	Secretary
2.	Dr. Gulshan Rai	-	Addl. Secretary, DG, CERT-In
3.	Shri Rajiv Gauba	-	Additional Secretary
4.	Dr. Rajendra Kumar	-	Joint Secretary
5.	Shri. V.L. Kanta Rao	-	COO, Negd. DIT

MINISTRY OF LAW & JUSTICE (LEGISLATIVE DEPARTMENT)

Dr. S.D. Singh	-	Joint Secretary and Legislative Counsel

2. At the outset, the Chairman welcomed the Members of the Committee and the representatives of the Department of Electronics and Information Technology and drew the attention of the witnesses to Direction 55 (1) of Directions by the Speaker, Lok Sabha regarding confidentiality of the proceedings of the sitting of the Committee.

3. The representatives of Department of Electronics and Information Technology made a Power Point presentation on the salient features of the following rules framed in pursuance of Information Technology Act, 2000:

(i) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ;

(ii)

(iii) The Information Technology (Intermediaries guidelines) Rules, 2011;

(iv) The Information Technology (Guidelines for Cyber Café) Rules, 2011;

(v) The information Technology (Electronic Service Delivery) Rules, 2011.

4. The Committee, thereafter, held discussion with the representatives of the Department of Electronics & Information Technology on the above mentioned rules.

5. The Chairmen then asked the representatives of the Department of Electronics & Information Technology to furnish written replies to those points which could not be answered during the discussion.

6. The witnesses then withdrew.

7. As the term of the Committee would be expiring on 22.9.2012, the Chairman thanked the members for their active participation during the deliberations of the Committee.

The Committee then adjourned.

MINUTES OF THE FIFTH SITTING OF THE COMMITTEE ON SUBORDINATE LEGISLATION (2012-2013)

_____

The Fifth sitting of the Committee was held on Monday, the 18th March, 2013 from 1500 to 1535 hours in Chairman's Room No. 143, Parliament House, New Delhi.

PRESENT

1. Shri P. Karunakaran — Chairman

MEMBERS

2. Dr. Mahesh Joshi
3. Shri Virender Kashyap
4. Dr. Ajay Kumar
5 Dr. Thokchom Meinya
6. Dr. Bhola Singh

SECRETARIAT

1. Shri A Louis Martin - Joint Secretary
2. Shri S.C. Chaudhary - Director
3. Shri Krishendra Kumar - Under Secretary

2. At the outset, the Chairman welcomed the members to the sitting of the Committee (2012-13).

3. The Committee, thereafter, considered the Draft Report of Committee on Subordinate Legislation on examination of the following rules:-

(i) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

(ii) The Information Technology (Intermediaries Guidelines) Rules, 2011

(iii) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011

(iv) The Information Technology (Electronic Service Delivery) Rules, 2011

4. The Committee adopted the aforesaid Report without any modification. The Committee also authorized the Chairman to present the same to the House after factual verification.

The Committee then adjourned.