ITEM NO.301 COURT NO.4 SECTION PIL-W

S U P R E M E C O U R T O F I N D I A
RECORD OF PROCEEDINGS

SMW (Crl.)No(s).3/2015

IN RE: PRAJWALA LETTER DATED 18.2.2015
VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS

(With appln.(s) for impleadment)

Date : 23-10-2017 This matter was called on for hearing today.

CORAM :
HON'BLE MR. JUSTICE MADAN B. LOKUR
HON'BLE MR. JUSTICE UDAY UMESH LALIT

Ms. N.S. Nappinai, Adv. (A.C.)

For Petitioner(s) Ms. Aparna Bhat, AOR
Mr. Mayank Sapra, Adv.
Ms. Joshita Pai, Adv.

For Respondent(s)
For CBI/MHA Mr. R. Balasubramanian, Adv.
Ms. Gunwant Dara, Adv.
Ms. Sushma Suri, AOR(NP)
Mr. Mukesh Kumar Maroria, AOR(NP)

Yahoo Mr. Samir Ali Khan, AOR
Mr. Sanjay Kumar, Adv.
Mr. Soham Kumar, Adv.

Facebook Ireland Mr. Sidharth Luthra, Sr. Adv.
Ms. Saanjh Purohit, Adv.
Ms. Richa Srivastava, Adv.
Mr. Tejas Chhabra, Adv.
Mr. Nitin Saluja, Adv.
Mr. S. S. Shroff, AOR(NP)

Facebook India Ms. Richa Srivastava, Adv.
Mr. S. S. Shroff, AOR (NP)

Google Mr. Sajan Poovayya, Sr. Adv.
Ms. Ruby Singh Ahuja, Adv.
Mr. Vishal Gehrana, Adv.
Ms. Tahira Karanjawala, Adv.
Mr. Arvind Chari, Adv.
Mr. Priyadarshi Banerjee, Adv.
Mr. Saransh Kumar, Adv.
Mr. Sharvan Sahny, Adv.

Mrs. Manik Karanjawala, Adv.
Mr. Avishkar Singhvi, Adv.
for M/s. Karanjawala & Co.

Microsoft — Mr. V. Giri, Sr. Adv.
Mr. Divyam Agarwal, AOR

WhatsApp — Mr. Kapil Sibal, Sr. Adv.
Mr. Shashank Mishra, Adv.
Mr. Koshy John, Adv.
Mr. Vivek Reddy, Adv.
Mr. Raghav, Adv.
Mr. Ashwin Reddy, Adv.
Mr. Pranav Awasthi, Adv.
Mr. S.S. Shroff, Adv.(NP)

UPON hearing the counsel the Court made the following

O R D E R

On 18th of February, 2015, this Court had received a letter from NGO-Prajwala to the effect that videos of sexual violence were being circulated in abundance.

After hearing learned counsel for the parties, an order was passed on 22nd March, 2017 constituting a Committee to assist and advise this Court on the feasibility of ensuring that videos depicting rape, gang rape and child pornography are not available for circulation, apart from anything else, to protect the identity and reputation of the victims and also because circulation of such videos cannot be in public interest at all.

We had expected the Committee to preferably arrive at a consensus on the possibility of ensuring that objectionable videos pertaining to child pornography, gang rape and rape are not made available on the

internet. For some technical reasons, if that was not possible to explain and detail the reasons why it was not possible.

The Committee was constituted under the Chairmanship of Dr. Ajay Kumar, the then Additional Secretary, Ministry of Electronics and Information Technology. The following persons participated in the deliberations of the Committee:

2. Sh. Arvind Kumar, GC, Cyber Laws and e-Security, MeitY.
3. Dr. Sanjay Bahl, DG, Cert-In;
4. Sh. Rakesh Maheshwari, Scientist G, MeitY;
5. Sh. Sunil Pant, Deputy Secretary, MHA;
6. Sh. Chakit Swarup, Product Manager, Digital India, MHA;
7. Ms. Aparna Bhat, Counsel for the Petitioner;
8. Ms. N.S. Nappinai, Amicus Curiae;
9. Sh. Vikram Langeh, Manager Trust & Safety, Facebook;
10. Dr. Jim Hunt, Software Engineer, Facebook;
11. Sh. Michael Yoon, Policy Manager, Safety & Content, Facebook;
12. Dr. Anthony Surleraux, Child Safety, Google;
13. Dr. Ksenia Duxfield Karyakina, Policy, Google;
14. Ms. Gitanjli Duggal, Legal, Google India;
15. Sh. Robin Fernandes, Grievance Officer, Yahoo;
16. Sh. S. Chandrasekhar, Group Director, Microsoft;
17. Dr. Radhakrishnan Srikanth, Group Program Manager, Microsoft;
18. Sh. Balakrishnan Santhanam, Sr Program Manager, Microsoft;
19. Ms. Keyla Maggessy, Law Enforcement Response Manager, WhatsApp;

20. Ms. Gayle Argon, Legal WhatsApp.

The Committee commenced its proceedings on 5th April, 2017 and met virtually on day to day basis. The Committee also took the advice of the experts who made presentation before the Committee. The experts are:

1. Ms. Susie Hargreaves, CEO and Mr. Fred Langford, Dy. CEO, Internet Watch Foundation (IWF), UK;
2. Professor Venkatesh Babu, IISc. Bengaluru:
3. Mr. John Shehan, NCMEC, USA;
4. Sh. Atul Kabra, Security Expert, FireEye, Bengaluri;

Certain inputs were also received from various other experts being:

1. Dr. Hany Farid, Professor & Chair, Computer Science, Dartmouth College, USA.
2. Dr. Mayank Vatsa, Mayank Vatsa, PhD, Adjunct Associate Professor, West Virginia, USA.
3. Dr. CV Jawqaqhar, Associate Professor, IIIT, Delhi.
4. Prof Dr. Anderson Rocha, Associate Dean, Institute of Computing, UNVIERSITY OF CAMPINAS, SP – BRAZIL.

Presentations and papers were also discussed by the Committee and the following presentations and submissions were made:

1. Presentation by Ms. Aparna Bhat, Advocate for Petitioner/Committee.
2. Presentation by Ms. N.S. Nappinai, Amicus Curiae/Committee Member.
3. Submission by Facebook representatives.
4. Presentation and Submission by Google representatives.
5. Presentation and Submission by Microsoft representatives.
6. Submission by Yahoo representative.
7. Combined industry submission of Google, Yahoo, Microsoft and Yahoo.
8. Presentation by Ministry of Home Affairs representative.
9. Written submission by WhatsApp.
10. Oral Presentation of NCMEC, USA and formal response to written queries.
11. Submission by Internet Watch Foundation (IWF), UK.
12. Presentation of Internet Watch Foundation (IWF), UK.
13. Presentation of Mr. Atul Kabra.

The submissions of learned senior counsel for WhatsApp Inc. were taken into consideration as well as those of the representative of WhatsApp who assisted the Committee. The following persons represented WhatsApp

Inc.:

1. Mr. Matt Jones, Software Engineer;
2. Ms. Keyla Maggessy, Law Enforcement Response Management:
3. Mr. Christian Dowell, Associate General Counsel.

Two members from WhatsApp Inc., viz., Ms. Keyla Maggessy and Ms. Gayle Argon were also co-opted in the Committee.

After a full discussion, a comprehensive report has been submitted to this Court by the Committee in two volumes. The second volume contains the presentations made.

We have gone through the contents of the first volume which deals with various issues that had arisen before the Committee.

All the parties before the Committee agreed on certain recommendations based on proposals made during the deliberations.

Part I of Chapter 7 of first volume of the Report contains the proposals in which the Committee was able to arrive at a consensus while Part II consists of the proposals in which the Committee was not able to arrive at a consensus.

We have been taken through the proposals as well as the recommendations made by the Committee on which there was a consensus.

We may note that Proposal No.9 was actually dropped by the Committee. In other words, there are 11 proposals on which there is agreement between the members of the Committee and one proposal which pertained to WhatsApp Inc. being Proposal No.18 which has been accepted while Proposal No.19 pertaining to WhatsApp Inc. was dropped.

The proposals and the recommendations made on which there is consensus read as follows:

		Proposal	Recommendations
1.	a)	The search engines expand the list of key words which may possibly be used by a user to search for CP content	Government of India may work with the represented companies as well as civil society organizations to suggest expansion of the list of key words for showing CP warning ads/Public service message on search.
	b)	These key words should also be in Indian languages and vernacular search.	The same may be gradually expanded to other Indian languages where applicable.
	c)	These key words should be expanded to cover RGR content.	For RGR, the Government of India may work with the represented companies as well as civil society organisations to suggest the list of key words for RGR warning ads/Public service message.
2.		Creating an administrative mechanism for reporting and	

		maintenance of data in India:	
	a)	Either within the CBI, or under the aegis of the MHA, a cell must be set up to deal with these crimes;	The Committee agrees that there is a need to create a Central Reporting Mechanism (India's hotline portal), as has been done in other countries, like in the U.S. with NCMEC. Further there is a need to strengthen law enforcement in this area. Any person/organization should be able to report any CP and RGR content in India with ease with provision for anonymous reporting. This portal may go for INHOPE membership, as an Indian Hotline.
	b)	A hash bank for RGR content be created (under the charge and control of Ministry of Home Affairs, GoI or through authorities or NGOs authorized by it);	The Committee also agreed that there is a need to develop a centralised agency to maintain and verify the hashes of all known CP and RGR imagery.
	c)	GoI to formulate specific parameters for identifying RGR content to ensure expeditious identification and removal;	Government may look into these for appropriate action expeditiously.
	d)	The hashes so generated must be under the custody of the centralized cell as stated hereinabove who will steps to prosecute, as per the law;	

	e)	A reporting mechanism must be created at a Central level, preferably with the CBI (in view of their role and special access) to also receive information of any CP/RGR content being circulated in the social media or any other platform over the internet;	
	f)	The cell would regularly engage with represented Companies and the NCMEC for updation of technology, technical support etc.	
	g)	Technology similar to Project Arachind crawler technology be availed of, for identifying India – based CP and also to adapt the same for identifying RGR content online;	
	h)	Content hosting platforms (CHPs), Search Engines and GoI to work together in formulating process for proactively verifying, identifying and initiating take down of all CP/RGR content;	
3.		Project CCPWC being a general project to alleviate crimes against women and children, a special focus sub-project to be created within the same foe eliminating CP\RGR to undertake the following:	
	a)	The Online Portal proposed to provide for anonymous reporting of identified CP/RGR;	Government may take action, as appropriate expeditiously.

	b)	A separate hotline to be established for reporting (with the option for caller to remain anonymous) of identified CP/RGR content;	
	c)	GoI to identify and authorize specific authority/entity for receiving Complaints of CP/RGR online and for initiating action thereon within specified timelines; Such authority to have immunity and permission to verify CP/RGR content and to initiate take downs: authority to also have specified processes for immediately intimating respective police stations for registration of FIR and for initiation of prosecutions;	
	d)	A team to be set up for immediately verifying such tips and to issue directions to the service providers/Intermediaries for immediate removal of such identified content;	
	e)	Government of India team/authority to also immediately send communications to concerned police stations for registration of FIR and initiation of prosecutions. In view of the CBIs willingness to take this responsibility it is recommended that matter be handled by CBI and not by local police.	
	f)	Government of India to	

		create tipper list of NGOs. Tips from such sources to be acted upon immediately by GoI authority for take down and initiation of prosecution without delay;	
4.		Creation of infrastructure /Training/Awareness building	
	a)	Government of India to form regulations for reporting of identified CP/RGR Imagery online.	Internet companies should provide technical support and assist in capacity building to the relevant agencies in India including law enforcement and NGOs through a series of trainings on online crime investigations, and trainings on using relevant Internet tools.
	b)	Government of India to ensure that Search Engines other than those already implementing URL blocks for identified CP/RGR content to initiate similar processes.	Internet companies should consider providing support to Indian NGOs to help bring awareness of these issues.
	c)	Government of India or its designated authority/NGOs to be extended permission/immunity for human intervention to identify CP/RGR content;	Government of India may also conduct regular training programme as well as relevant Government training infrastructure to have the latest technology on the subject matter.
	d)	Government of India to allocate funds for	Government of India may also partner with

		training, verification, continuous monitoring and review of personnel involved in such human intervention process for identifying CP/RGR content, in line with those adapted by NCMEC/IWF;	civil society organistaions, research institutes to conduct programme as mentioned in c) above. Premier reserch institutes like IISc must be encourages and supported to have dedicated research programme to undertake these studies.
	e)	GoI/CHPs/Search Engines to involve in creation of awareness amongst users and sensitization programs and capacity building initiatives for judiciary, prosecutors and law enforcement authorities, to mitigate the menace of CP/RGR dissemination;	
	f)	GoI to set up processes for expeditious initiation of prosecution against users for identified CP/RGR content reported by CHPs;	
5.		The solution lies in proactively identifying rogue sites by an independent agency which can identify sites that contains CP and RGR content and blocking these sites. To prevent the circulation of subject imagery, Government can block any additional sites/applications if they do not remove such contents of their own. MHA/designated LEA can be empowered to directly order Indian ISPs through	The members of the Committee were of the opinion that this could be a process that could be considered for suitable implementation in India.

		DoT.	
6.		The Government, through an appropriate agency setup a VPN to receive the NCMEC reports for uploading of CP from India. As conveyed by NCMEC, there were more than one hundred thousand reports belonging to India. Law enforcement agencies should initiate legal action against uploaders.	The Committee agreed that this should be looked into expeditiously.
7.		Removal of known CP/RGR imagery: When imagery is detected as CP/RGR, in addition to preventing subsequent uploads, content hosting platforms (CHP) voluntarily identify, remove and prevent distribution of previously existing content on their platforms.	The Committee agreed to the said proposal.
8.		There is need for greater thrust and emphasis on research & development of Artificial Intelligence (AI)/Deep Learning (DL)/Machine Learning (ML) based techniques for identifying CP/RGR content at the stage of uploading to enable real time filtering. Some specific suggestion in this regard may include as follows:	The Committee recognized the technologies developed by represented companies including PhotoDNA, Video hashing and other techniques for Imagery. However Committee also recognizes the need for much greater collaborative work in the subject area amongst all stakeholders. The Committee also feels that video hashing technique should also mature as has been done for
	a)	Traditional DL/ML techniques, including feature engineering based techniques and other Image processing techniques to be developed for identifying	

		CP/RGR content at the stage of uploading.	hashing techniques for images. Represented companies should further voluntarily collaborate with NCMEC to establish a shared database of CP video hashes similar to the image hashes database that is already used by the industry.
	b)	CHPs to review existing architecture to screen/ verify uploads for CP/RGR content using such AI/DL/ML tools after suitable technologies are developed.	
	c)	AI/DL/ML tools to be tested real time (i.e., upon each upload).	
	d)	Research into above alternatives to be initiated in a time bound manner.	The committee suggested that suitable research be initiated for further development of technologies for identifying CP/RGR imagery.
	e)	CHPs to consider using NCMEC for creating deep learning/machine learning tools, subject to applicable laws, for CP (to avail of the huge data sets repository of NCMEC).	
	f)	Government of India, along with CHPs to enage services of suitable experts for developing deep learning/Machine learning tools for identifying RGR content.	
9.		User Authentication: Create a mechanism where users who seek to upload an image/video, falling within the subject content, using the pre-identified key words, are put to a more rigorous verification process which would have them believe that they would be traced.	The Committee decided to drop this proposal by consensus.

10		Content removal processes/ URL de-indexing process for identified RGR imagery should be as expeditious as removal of CP Imagery.	The represented companies stated that they are continuously working on improving processes for review of content including RGR that is reported to them. The Committee noted the same.
11		Content hosting platforms, social media platforms and search engines will provide links for reporting CP/RGR imagery, as a specific category and the same to be more prominently displayed on their pages.	The represented companies stated that they are continuously working on improving processes for reporting content including CP and RGR that violates their policies or applicable laws. The Committee noted the same.
12	a)	Create a mechanism to ensure that when CP imagery is identified, the CHPs shall preserve and retain such information of the uploader including the identified content to assist law enforcement;	The represented companies are already taking action in this regard. The Committee agrees to Part(a) of proposal.
18		WhatsApp should make further improvement in their reporting process which would enable easier reporting of contents in the App while maintaining the integrity of the contents and metadata available on phone at the time of reporting	There was consensus in the Committee. The Committee recommends that these efforts be taken up at the earlies.
19		Compute the PhotoDNA has, VideoHash at WhatsApp Client on Mobile Handset level, and transmit then to central WhatsApp server for matching with	The Committee agreed not to pursue this proposal.

		CP/RGR Hashes database.	

We expect the parties including the Government of India to abide by the recommendations on which there is consensus and to try and implement them at the earliest.

We make it clear that any information that is based on or is pursuant to the proposals and recommendations to the Government of India will be kept confidential so as not to reveal the technology used by the participating service providers.

The Government of India will prepare a status report on implementation of the recommendations and place it before us in a sealed cover before the next date of hearing.

On the next date of hearing, we will deal with the proposals on which there is no consensus.

List the matter on 11th December, 2017 at 2.00 p.m.

It is made clear that on the next date of hearing also the proceedings will be held in-camera.

(SANJAY KUMAR-I)
AR-CUM-PS

(KAILASH CHANDER)
COURT MASTER