* **IN THE HIGH COURT OF DELHI AT NEW DELHI**

Date of decision: 26th APRIL, 2023

IN THE MATTER OF:

\+ **W.P.(CRL) 1505/2021 & CRL.M.As. 12645/2021 & 811/2022**

MRS X ..... Petitioner

Through: Mr. Sanjeev Mahajan, Mr.Sachin Tandan, Advocates

versus

UNION OF INDIA AND ORS ..... Respondents

Through: Mr. Anurag Ahluwalia, CGSC with Mr. Gursihar Preet Singh, Mr. Danish Faraz Khan, Advocate for UOI.

Ms. Nandita Rao, ASC for the State with Mr. Amit Peshwani, Ms. Aaliya Waziri, Advocates and Inspector Kusum Dangi, IFSO Cyber Cell, Dwarka.

Mr. Arvind Nigam, Sr. Advocate along with Ms. Mamta Rani Jha, Ms. Shruttima Ehersa, Mr. Rohan Ahuja, Mr. Vatsalya Vishal & Ms. Riya Gupta, Advocates for R-3/Google LLC.

Mr. Jayant Mehta, Sr. Advocate with Ms. Anushka Sharda, Mr. Madhav Khosla, Ms. Moha Paranjpe, Advocates for Respondent No. 4 (Microsoft).

Mr. Debopriyo Moulik and Ms. Shweta Chabbra, Advocates for R-10

Mr. Saurabh Kripal, Sr. Advocate

(*Amicus Curiae*) with Ms. Tanima Gaur, Mr. Sidhant Kumar, Ms. Manyaa Chandok, Ms. Vidhi Udayshankar, Advocates

CORAM:
HON'BLE MR. JUSTICE SUBRAMONIUM PRASAD

JUDGMENT

1. The instant writ petition has been filed under Article 226 of the Constitution of India, 1950, read with Section 482 of the Code of Criminal Procedure (*hereinafter referred to as "Cr.P.C."*) seeking, in a nutshell, the blocking of certain sites exhibiting intimate images of the Petitioner herein, and for registration of a First Information Report (FIR) arising out of the complaint dated 03.08.2021 made by the Petitioner to Lajpat Nagar Police Station, New Delhi.

GENESIS OF THE MATTER

2. At the outset, this Court deems it appropriate to refer to the Petitioner as "Mrs. X" in consonance with the directions rendered by the Hon'ble Supreme Court in Nipun Saxena v. Union of India, **(2019) 2 SCC 703**, whereby it was observed that in a patriarchal society like India, survivors/victims of sexual violence of any nature are forced to undergo ostracization for no fault of their own. Therefore, to prevent hostile discrimination or harassment of the survivor/victim in the future, this Court believes it to be prudent to refer to the Petitioner herein as "Mrs. X".

3. Having stated the above, the facts, in brief, leading to the instant petition are stated as under:

a) It is stated that the Petitioner is a married woman with a nine-year-old son. In December 2019, she became acquainted with one Mr. Richesh Manav Singhal who approached her through social media and introduced himself as a British Chartered Accountant. It is stated that in February 2020, the Petitioner shared her personal contact number with Mr. Singhal, and over a period of time, the Petitioner became close to Mr. Singhal.

b) In July 2020, it is stated that as the Petitioner was living with her son at a rented accommodation in Gurugram on account of her job and financial constraints. Mr. Singhal took advantage of the absence of the Petitioner's family members, came over to her place and forced himself upon her. He allegedly not only clicked explicit pictures of the Petitioner, but also transferred to himself from the mobile phone of the Petitioner explicit pictures that the Petitioner had taken of herself for the purpose of sharing them with her husband.

c) It is stated that Mr. Singhal involved the minor son of the Petitioner in various sexual acts as well. Consequently, the Petitioner lodged a complaint against Mr. Singhal at the Lajpat Nagar Police Station, and on the basis of the same, a Zero FIR was registered with the investigation thereafter being transferred to Gurugram. It is stated that on multiple occasions, Mr. Singhal threatened the Petitioner that he would leak her sexually explicit photographs on various pornographic websites and that he would kill her son if she did not pay huge amounts of money to him. Consequently, the Petitioner was extorted into

paying lakhs of money to Mr. Singhal, along with handing him all her jewellery.

d) It is stated that as the funds of the Petitioner had depleted and she was unable to pay any more money to Mr. Singhal, he followed through on his threats and leaked the Petitioner's explicit images on various pornographic websites without the consent or permission of the Petitioner. This led to the Petitioner addressing a complaint dated 03.08.2021 against Mr. Singhal to the SHO at Police Station Lajpat Nagar recording the new offences. The said complaint notes that Mr. Singhal had made a YouTube channel in the Petitioner's name, and has been posting her explicit videos and photographs on a daily basis.

e) Despite the Petitioner having approached the Grievance Cells of Respondents No. 3 to 6, i.e. Google LLC, Microsoft India Pvt. Ltd. (later replaced by Microsoft Ireland Operations Ltd. which is the entity managing its search engine, Bing), YouTube.com and Vimeo.com, as well as having placed multiple complaints on cybercrime.gov.in, the explicit images of the Petitioner were not taken down.

f) Aggrieved by the failure in the redressal processes available to her, the Petitioner herein has approached this Court by way of the instant writ petition for directions to the Respondents for removal of all her non-consensual intimate images on the internet.

4. During the course of hearing of the instant writ petition, *vide* Order dated 11.08.2021, Respondent No.5 was deleted from the array of parties,

and this Court directed for impleadment of the concerned Police Station at Gurugram. *Vide* Order dated 07.09.2021, this Court informed Mr. Anurag Ahluwalia, appearing for the Union of India, Ms. Mamta Jha, learned Counsel appearing for Google LLC and YouTube, that the instant matter was not adversarial in nature and that full cooperation was expected on their part in removal of the objectionable content pertaining to the Petitioner herein with the same being done before the next date of hearing.

5. Status Reports dated 28.08.2021 and 14.09.2021were filed on behalf of Respondent No.2, i.e. Government of NCT of Delhi (GNCTD) with regard to the Uniform Resource Locator (URLs) being blocked/removed. The Status Report dated 14.09.2021 noted that all possible efforts were being made to get the remaining active URL/links blocked/removed through the concerned intermediaries. A Status Report dated 16.09.2021 was filed on behalf of Respondent No.1, i.e. Union of India. Relevant portions of the said Status Report recording the jurisdiction of the Delhi Police over matters of the instant nature have been reproduced as under:

> *"3. That the Ministry of Home Affairs has launched Cybercrime Reporting Portal (www.cybercrime.gov.in) a central platform, to facilitate the victims/complainants to report all types of cybercrime complaints online.*
>
> *4. That this portal allows citizens to lodge complaints pertaining to online Child Pornography (CP) - Child Sexually Abuse Material of sexually explicit contents such as Rape/Gang Rape (CP/RGR) content other cybercrimes. The citizens have an option of reporting complaints anonymously when the complainants do not want to disclose their identity. They can also report the complaints as a registered user to track the status of complaint at various stages.*

5. That the Government has also made a Toll free Helpline number (155260) functional to help the citizens to lodge their complaint on the Portal.

6. That the complaint reported by a citizen on the cybercrime reporting portal (www.cybercrime.gov.in) is routed automatically to the concerned Law Enforcement Agency and appears in the inbox of the concerned State/UT Nodal Officer for assigning it to the concerned authority or Police Station for taking further action as per the laid down law and procedure.

7. That the Ministry of Home Affairs has designated the National Crime Record Bureau as Central Nodal Agency to manage technical & operational functions of the online cybercrime reporting portal and its associated work.

8. That Delhi Police is the Law Enforcement Agency in the instant case and they were asked to take further necessary action to get the URLs mentioned in para 18 of WP blocked.

9. That the Delhi Police is the agency to whom the subject complaint is routed through the portal and has the jurisdiction to take action; hence the actionable information / status of blocking of all relevant URLs must be available with Delhi Police. In order to avoid repetition of facts before the Hon'ble Court, the Delhi Police being a respondent in this matter may file the same.

10. That considering the nature of subject issue and the material facts submitted through this Affidavit, the Hon'ble Court may graciously be pleased to accepts the averments made above and may consider to take response of the LEA i.e. Delhi Police as 'Police' and 'Public Order' being States subjects the issues raised by the Petitioners are primarily related to the

> *detection, investigation & prosecution, which are done as per the provisions of law."*

6. Thereafter, an Additional Affidavit dated 21.09.2021 was filed on behalf of the Petitioner noting that the offending material was consistently being reproduced and re-uploaded. On 06.10.2021, this Court was informed by learned Counsel appearing for Google LLC that though all the offending material had been removed from YouTube and the URLs which had been specifically supplied were de-indexed by Google, it did not mean that it could not be found on the internet through other search engines and that merely directing only the search engines to de-index the links would not be an adequate solution.

7. Due to the complexity in the nature of the matter and the fact that consistent Orders of this Court were being frustrated, *vide* Order dated 06.10.2021, this Court deemed it appropriate to appoint Mr. Saurabh Kirpal, learned Senior Counsel, as *Amicus Curiae*, to assist this Court on the position of law and the extent to which this Court can issue directions to intermediaries in such matters so as to protect the rights of the Petitioner and other similarly situated individuals *vis-à-vis* the duties of the intermediaries as well as the right to free speech. Accordingly, the scope of the instant Writ Petition under Article 226 has been expanded, and any directions that will be rendered will be limited to search engines, MEITY and Delhi Police.

8. A Short Affidavit dated 22.12.2021 was filed on behalf of Respondent No.1 in the instant matter, stating that the Ministry of Electronics and Information Technology (MEITY) is the custodian of the Information Technology Act, 2000 (*hereinafter referred to as* "IT Act"). The Short Affidavit delineates the objective and relevant provisions of the said Act as well as the Information Technology (Intermediary Guidelines and Digital

Media Ethics Code) Rules, 2021 (*hereinafter referred to as the* "IT Rules"). It notes that the IT Rules not only focus on the enhanced safety of women and children, but that it also provides for statutory timelines for grievance redressal and content takedown. The Short Affidavit, thereafter, goes on to note that the prayer of the Petitioner seeking delinking/de-tagging/de-referencing/de-indexing the name of the Petitioner would adversely affect the freedom of speech and expression of other individuals having the same name as the Petitioner or a similar name. The paragraphs of the Short Affidavit stating the aforesaid are as follows:

> *"5. It is submitted that the Ministry of Electronics and Information Technology (hereinafter referred to as "MEITY") is the custodian of the Information Technology Act, 2000 (hereinafter referred to as "IT Act, 2000") and Rules framed thereunder.*
>
> *6. It is submitted that the IT Act, 2000 contains provisions under Sections 66E, 67 and 67A, under Chapter XI thereof for violation of bodily privacy, publishing or transmitting obscene material and publishing or transmitting sexually explicit material in electronic form respectively. It is further submitted that Section 67B of the IT Act, 2000 provides for punishing the publishing or transmitting of material depicting children in sexually explicit act in electronic form.*
>
> *7. It is submitted that Section 79 of the IT Act, 2000 contains safe harbor provisions for intermediaries as defined under Section 2(1)(w) thereof. It is further submitted that the intermediaries must inter alia observe due diligence guidelines as prescribed by the Central Government to ensure exemption from liability. It is further submitted that to ensure open, safe, trusted and accountable Internet, the answering Respondent has notified the Information Technology (Intermediary Guidelines and Digital*

Media Ethics Code) Rules, 2021 (hereinafter "IT Rules, 2021") on 25.02.2021. It is further submitted that the Part II of the IT Rules, 2021 have been framed under Section 79 of IT Act, 2000, which relates to due diligence to be observed by an intermediary. A copy of IT Rules 2021 is annexed herewith and marked as Annexure RA-1.

8. It is submitted that the answering Respondent has recently published a Frequently Asked Questions (FAQs) communicating the intent of the IT Rules, 2021 in simple and easy to understand language for all its stakeholders. A copy of the Frequently Asked Questions is annexed herewith and marked as Annexure RA-2.

9. It is submitted that as stated hereinabove, the legislative intent the IT Rules, 2021 is to ensure open, safe, trusted and accountable Internet. It is further submitted that the IT Rules, 2021 prescribe the due diligence to be followed by all intermediaries as well as the additional due diligence to be followed by significant social media intermediaries (SSMI), i.e., the intermediaries having registered user base of 50 lacs or more in India.

10. It is submitted that the IT Rules, 2021 have been framed to provide for increased user safety, i.e., the intermediaries t to respond to the direct requests by the affected individuals for content takedown in specific cases of content relating to breach of bodily privacy, impersonation, morphed imagery of the concerned individual in order to address the immediate need to prevent harm and emotional distress, particularly in instances of revenge porn and other similar instances.

11. It is submitted that, as stated above, the IT Rules, 2021 have a clear objective of enhancing online safety of users, particularly women and children. It is further submitted that various provisions of the IT

Rules, 2021 focus on enhanced safety of women and children. It is further submitted that these include:

> *"1. Specific inclusion of certain requirements to be explicitly conveyed in terms and conditions [Rule 3(l)(b)].*
> *2. Reporting by the aggrieved individual in respect of revenge porn and similar content breaching physical privacy and taking action within 24 hours for content removal [Rule 3(2)(b)].*
> *3. Enhanced grievance redressal mechanism by intermediaries [Rule 3(2)(a)].*
> *4. Additional provision for SSMI to appoint a Resident Grievance Officer, a Chief Compliance Officer and a nodal contact person, all to be residents in India; and a physical contact address of the significant social media intermediary to be in India [Rule 4(1) and 4(5)].*
> *5. The Rules also have provisions that intermediary shall cooperate with Law Enforcement Agencies (LEA) to identify the first originator of information related to rape and child sexual abuse material (CSAM) imagery for prosecution [Rule 4(2)].*
> *6. The significant social media intermediaries shall endeavor to deploy technology-based measures to identify any imagery of child sexual abuse, rape etc. whether real or simulated in accordance with the safeguards in the Rules [Rule 4(4)].*

12. It is submitted that the IT Rules, 2021 provide for the following statutory timelines for grievance redressal and content takedown:

> *1. Grievance Redressal; 24 hours for acknowledgement and 15 days for disposal [Rule 3(2)].*

> *2. Information takedown from platform upon actual knowledge based on court order or notice from appropriate government authorised by law: 36 hours [Rule 3(1)(d)]*
> *3. Providing information on a lawful request: 72 hours [Rule 3(1)(j)]*
> *4. Removal of revenge porn (sexual extortion/non-consensual porn publication/sexual act or conduct involving impersonation, etc.) and other similar content: 24 hours [Rule 3(2)(b)].*
>
> *13. It is submitted that in the present Petition, the grievance(s) of the Petitioner falls under Rule 3(2)(b) of the IT Rules, 2021 and accordingly, the Petitioner has an efficacious remedy to approach the intermediary directly or through any person on her behalf including law enforcement agencies for removal of URLs containing offending content.*
>
> *14. It is submitted that the Petitioner's Prayer in clause (B) seeking delinking/de-tagging/de-referencing/de-indexing the name of the Petitioner from the search engines would adversely affect on the freedom of expression and speech of other individuals having the same or similar name as that of the Petitioner.*
>
> *15. It is submitted that the Rule 3(2)(b) of the IT Rules, 2021 empower the Petitioner to seek removal of the content by submitting the information/URLs to the intermediaries, who are obligated to remove such content within 24 hours"*

9. *Vide* Status Report dated 16.03.2022, this Court was apprised of the fact that the accused Richesh Manav Singhal and one Shweta Chhabra had been arrested after an investigation at their residence which lead to the discovery of more than 83,000 explicit pictures, including that of the Petitioner herein, on one of the laptops at their residence. It was further

found that the accused was involved in multiple other cases. Relevant portion of the Status Report reads as under:

> *"Further, on the basis of information, early morning of 8.3.2022, the officer investigating the case, visited C-2400, Suite No. 103 Sushant Lok, Gurugram, Haryana. Richesh Manav Singhal and Shweta found present on the above mentioned address. They were joined the investigation and after interrogation both were arrested in this case. A total Cash of Rs 23,99,182/-, jewellery articles, 17 mobile and 4 laptops belong to the accused persons were taken in police possession as per seizure memo. The laptop and mobile phones recovered from the accused are being forensically examined. A large number (more than 83,000) of objectionable photographs of various girls including the nude photographs of the petitioner Mrs. X have been found in one of the laptops. Further forensic examination of the laptops and mobile phones arc going on. It has been found tha, the accused Richesh Manav Singhal is previously also involved in several cases viz*
>
> *1.) FIR No. 448/2016, U/s 66 A, 354D/506/509 IPC, PS Mukherjee Nagar*
>
> *2) FIR No. 1161/15, U/s 354/354(A), 354B, 509 IPC, PS Vasant Kunj North.*
>
> *3) FIR No. 355/15, U/s 376/323/506 IPC, PS Malviya Nagar,*
>
> *4.) FIR No. 206/2017, U/s 354D/509 IPC PS Timarpur,*
>
> *5.) FIR No. 185/21, U/s 376,506 IPC, 8/10 POCSO Act PS Sector 56, Gurugram.*
>
> *Both accused persons namely Richesh Manav Singhal and Shweta Chhabra are on PC remand. The Investigation is still going on. The undersigned is ready to abide the directions passed by Hon'ble Court"*

10. The Writ Petition, therefore, becomes infructuous. However, to ensure that the victims like the Petitioner herein are not forced to approach the authorities/intermediaries including the search engine repeatedly for removal of any offending content, this Court has proceeded further so that appropriate directions may be issued.

11. *Vide* Order dated 22.03.2022, this Court issued the following directions to Respondent No.3, i.e. Google LLC, and Respondent No.4, i.e. Microsoft India:

> *"1. The search engines i.e. respondent No.3/Google LLC and respondent No.4/Microsoft India Pvt. Ltd. are directed to file an affidavit stating the technologies they possess, to ensure that the material which has been directed to be removed by the competent authority/court does not re-appear on the internet after the same has been brought down, which could force the complainant to repeatedly go to the law enforcing agencies/court for the very same order. It is also directed to disclose as to whether such a material can be removed without any reference to specific URLs.*
>
> *2. The said affidavit be filed within three weeks from today. A copy of the same be supplied to the learned amicus curiae."*

12. After the Judgement was reserved in the instant matter, the learned *Amicus Curiae* sought to place on record the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022by way of CRL.M.A. No. 22861/2022. The same was allowed *vide* Order dated 20.12.2022.

13. Non-Consensual Intimate Images (NCII) refers broadly to sexual content that is distributed without the consent of those who are being

depicted in the said content. This content may or may not be taken with the consent of the individual involved, however, its dissemination is largely meant to be non-consensual and comes under the larger umbrella of cyber-harassment. Such distribution, more colloquially known by the term "revenge porn", causes psychological damage to the victim and subjects them to social ostracization and humiliation that can seriously impact the mental health of the victim. This Court will, however, refrain from using the term "revenge porn" as it is merely a subset of NCII and NCII encompasses a larger number of scenarios in which such content may be distributed. The individual whose images are shared without their consent are perceived by the public to be *deserving* of the violation of their privacy and bodily integrity. Further, the same level of gravity that is attached to a crime like molestation/sexual harassment is not assigned to NCII abuse as the public in general finds it difficult to conceptualize its negative impact on account of the fact that the victim's physical person remains unharmed. However, what such conceptualization tends to ignore is that victims of NCII abuse face significant life disruptions, such as loss of job, being turned away by their families, etc, which in turn radically affects their mental health. In a 2013, a self-selected study conducted by the Cyber Civil Rights Initiative on Non-consensual Pornography (NCP), it was found that 93% of NCII abuse victims suffer significant social distress, 51% experience suicidal thoughts, and 82% experience social or occupational impairment.

14. With an increasing number of cases of NCII abuse in a simultaneously advancing digital community as well as keeping in mind that we are currently living in the digital age where accessibility to internet is becoming easier which is in turn leading to diverse and new forms of violence being perpetuated, this Court deems it necessary to conduct the

following exercise and analyse NCII abuse through the prism of the IT Act and the Rules thereunder, as well as to carve out the roles that intermediaries, more specifically search engines, play in not only its distribution, but in its prevention as well.

NCII *vis-à-vis* the IT Act and the IT Rules

15. While NCII in itself has not been explicitly defined either in the IT Act or the Rules thereunder, Rule 3(2)(b) of the IT Rules, which lays down the grievance redressal mechanism that is to be followed by an intermediary, more or less defines NCII as any content which *prima facie* exposes the private area of any individual/shows such individual in full or partial nudity/shows or depicts such individual in any sexual act or conduct/is in the nature of impersonation in an electronic form, including artificially morphed images. The provision has been reproduced as under:

> *"**3(2)(b)**. The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, **in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual,** take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it."*
> (emphasis supplied)

16. However, the aforementioned definition does not mention the lack of consent in either producing the content or in dissemination of the content.

Further, Rule 3(2)(b) is not a charging offence. It is only under Section 66E of the IT Act that violation of privacy of an individual is punished with imprisonment which may extend to three years or with fine not exceeding two lakhs, or with both. Section 66E has been reproduced as under:

> *"**66E**. Punishment for violation of privacy.–Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.*
>
> *Explanation.–For the purposes of this section–*
>
> *(a) ―transmit means to electronically send a visual image with the intent that it be viewed by a person or persons;*
>
> *(b) ―capture, with respect to an image, means to videotape, photograph, film or record by any means;*
>
> *(c) ―private area means the naked or undergarment clad genitals, public area, buttocks or female breast:*
>
> *(d) ―publishes means reproduction in the printed or electronic form and making it available for public;*
>
> *(e) ―under circumstances violating privacy‖ means circumstances in which a person can have a reasonable expectation that–*
>
> *(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or*

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

17. Explanation (a) to Section 66E clarifies that the term "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons; Explanation (d) states that the term "publishes" means reproduction in the printed or electronic form and making it available for public; and Explanation (e) notes that "under circumstances violating privacy" means circumstances in which persons have a *reasonable expectation* that they may disrobe in privacy or that any part of their private area would not be visible to the public, regardless of whether they are in a public or private place.

18. Further, Section 67 of the IT Act provides punishment for publishing or transmitting of obscene material in electronic form, and the said provision is as follows:

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

***67A**. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.–*

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

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

Whoever,–

> *(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or*
>
> *(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or*
>
> *(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in*

a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–

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

(ii) which is kept or used for bona fide heritage or religious purposes.
Explanation–For the purposes of this section, ―children means a person who has not completed the age of 18 years.

***67C**. Preservation and retention of information by intermediaries.–(1) 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) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.]"*

Role of intermediaries in removal of NCII *vis-à-vis* IT Act and IT Rules

19. NCII's presence on the internet can be traced to "originators" who are responsible for uploading and publishing the content, and NCII's spread and its continued existence on the internet can be attributed to "intermediaries" that facilitate its flow and provide other users access to it. Before venturing into the role that intermediaries play in removal of offending content from the internet, it is imperative to reproduce the relevant provisions from the IT Act and the IT Rules for ease of comprehension.

20. Section 2(1)(o) of the IT Act defines "data" to mean information processed in a computer system or network in any form, including media. Section 2(1)(v) of the IT Act defines "information" to include data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche, and Section 2(1)(w) of the IT Act defines "intermediary", with respect to any particular electronic records, to mean any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service

providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes. Section 2(1)(f) of the IT Rules defines "communication link" to mean a connection between a hypertext or graphical element, and one or more items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which can be another electronic record or another website or application or graphical element.

21. Section 69A of the IT Act enlists the power of the Central Government to issue directions for blocking for public access of any information through any computer resource. Section 69A(3) notes that any intermediary who fails to comply with the direction under Section 69A(1) shall be punished with imprisonment for a term which may be extended to seven years and also be liable to a fine. The same has been reproduced as follows:

> *"**69A**. Power to issue directions for blocking for public access of any information through any computer resource.–*
>
> *(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section*
>
> *(2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or*

> *cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource. (2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.*
>
> *(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine."*

22. An intermediary is exempted from incurring any liability in certain cases under Section 79 of the IT Act, which is known as the "safe harbour provision". This provision states that an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. The intermediary in question is required to observe due diligence while discharging his duties under the Act and to also observe such other guidelines as the Central Government may prescribe in his behalf. Section 79(3) states that the protection under Section 79 lapses and does not apply if the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act, or if upon receiving "actual knowledge", or if the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner 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. Section 79 of the IT Act is as under:

*"**79**. Exemption from liability of intermediary in certain cases.–*

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-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."*

23. With respect to the IT Rules, Rule 3 of the IT Rules assumes significance as it lays down due diligence that must be exercised by intermediaries and the grievance redressal mechanism that is to be employed by an intermediary. At this juncture, it is stated that the IT Rules have been amended by way of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 (*hereinafter referred to as the* "2022 Amendment Rules"). This Court will, thus, refer to the amended Rule 3. Rule 3(1)(b) stipulates that the intermediary shall inform its rules and regulations, privacy policy and user agreement to the user in English or any language specified in the Eight Schedule to the Constitution in the language of his choice and shall make *reasonable efforts* to cause the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that, *inter alia*, belongs to

another person and to which the user does not have any right, or is obscene, pornographic, paedophilic, invasive of another's privacy including bodily privacy, insulting or harassing on the basis of gender, etc. It is pertinent to note that prior to the amendment, the intermediary was merely required to *inform* the user to not host, display, upload, modify, publish, transmit, store, update or share the said content, but the amendment increases the burden on the intermediary.

24. First proviso to Rule 3(1)(d) enlists that in the case of any prohibited information as mentioned in Rule 3(1)(d), the intermediary is required to remove or disable access to that information, as early as possible, but in no case later than thirty-six hours from the receipt of the Court order or on being notified by the Appropriate Government or its agency, as the case may be. Furthermore, Section 3(1)(m) has been inserted in the 2022 Amendment Rules to state that the intermediary shall take all reasonable measures to ensure accessibility of its services to users along with reasonable expectation of due diligence, privacy and transparency, and the newly inserted Section 3(1)(n) states that the intermediary shall respect all the rights accorded to the citizens under the Constitution, including in Articles 14, 19 and 21.

25. Apart from knowledge of the offending information being supplied by way of a Court order or an order of the Appropriate Government or its agency, the IT Rules under Rule 3(2) introduces a detailed and time-bound grievance redressal mechanism to a user or a victim to approach the intermediary directly by making a complaint with regard to the violation of the provisions of Rule 3 to the Grievance Officer who is then supposed to acknowledge the complaint within twenty-four hours and then dispose of the same within a period of fifteen days from the date of its receipt. The 2022 Amendment Rules have added a proviso to Rule 3(2)(a)(i) which states that

if the complaint is in the nature of request for removal of information or communication link relating to Rule 3(1)(b), except sub-clauses (i), (iv) and (ix), the intermediary shall act upon the same as expeditiously as possible and resolve it within seventy-two hours of such reporting.

26. Under Rule 3(2)(b) and Rule 3(2)(c), within twenty-fours from receipt of complaint made by an individual or on their behalf in relation to content which is *prima facie* in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in nature of impersonation in an electronic form, including artificially morphed images of such individual, the intermediary is required to take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it. Further, the intermediary is also required to implement a mechanism for the receipt of complaints under Rule 3(2)(b) which may enable the individual or person to provide details, as may be necessary, in relation to such content or communication link.

27. Rule 3 of the IT Rules has been reproduced as follows:

> *"3. (1) Due diligence by an intermediary: An intermediary, including social media intermediary and significant social media intermediary, shall observe the following due diligence while discharging its duties, namely:—*
>
> > *(a) the intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the rules and regulations, privacy policy and user agreement in English or any language specified in the Eighth Schedule to the Constitution for access or usage of its computer resource by any person in the language of his choice and ensure compliance of the same;*

(b) the intermediary shall inform its rules and regulations, privacy policy and user agreement to the user in English or any language specified in the Eighth Schedule to the Constitution in the language of his choice and shall make reasonable efforts to cause the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that,—

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

(ii) is obscene, pornographic, paedophilic, invasive of another's privacy including bodily privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or promoting enmity between different groups on the grounds of religion or caste with the intent to incite violence;

(iii) is harmful to child;

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

(v) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature;

(vi) impersonates another person;

(vii) 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 cognisable offence, or prevents investigation of any offence, or is insulting other nation;

(viii) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;

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

(c) an intermediary shall periodically inform its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be;

(d) an intermediary, on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information

which is prohibited under any law for the time being in force:

> *Provided that any notification made by the Appropriate Government or its agency in relation to any information which is prohibited under any law for the time being in force shall be issued by an authorised agency, as may be notified by the Appropriate Government:*
>
> *Provided further that if any such information is hosted, stored or published, the intermediary shall remove or disable access to that information, as early as possible, but in no case later than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency, as the case may be:*
>
> *Provided also that the removal or disabling of access to any information, data or communication link within the categories of information specified under this clause, under clause (b) on a voluntary basis, or on the basis of grievances received under sub-rule (2) by such intermediary, shall not amount to a violation of the conditions of clauses (a) or (b) of sub-section (2) of section 79 of the Act;*

(e) the temporary or transient or intermediate storage of information automatically by an intermediary in a computer resource within its control as an intrinsic feature of that computer resource, involving no exercise of any human, automated or algorithmic editorial control for onward transmission or communication to another computer resource shall not amount to

hosting, storing or publishing any information referred to under clause (d);

(f) the intermediary shall periodically, and at least once in a year, inform its users in English or any language specified in the Eighth Schedule to the Constitution in the language of his choice of its rules and regulations, privacy policy or user agreement or any change in the rules and regulations, privacy policy or user agreement, as the case may be;

(g) where upon receiving actual knowledge under clause (d), on a voluntary basis on violation of clause (b), or on the basis of grievances received under sub-rule (2), any information has been removed or access to which has been disabled, the intermediary shall, without vitiating the evidence in any manner, preserve such information and associated records for one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by Government agencies who are lawfully authorised;

(h) where an intermediary collects information from a user for registration on the computer resource, it shall retain his information for a period of one hundred and eighty days after any cancellation or withdrawal of his registration, as the case may be;

(i) the intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011;

(j) the intermediary shall, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents:

> *Provided that any such order shall be in writing stating clearly the purpose of seeking information or assistance, as the case may be;*

(k) the intermediary shall not knowingly deploy or install or modify technical configuration of computer resource or become party to any act that may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:

> *Provided that the intermediary may develop, produce, distribute or employ technological means for the purpose of performing the acts of securing the computer resource and information contained therein;*

(l) the intermediary shall report cyber security incidents and share related information with the Indian Computer Emergency Response Team in accordance with the policies and procedures as mentioned in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

(m) the intermediary shall take all reasonable measures to ensure accessibility of its services to users along with reasonable expectation of due diligence, privacy and transparency;

(n) the intermediary shall respect all the rights accorded to the citizens under the Constitution, including in the articles 14, 19 and 21.

(2) Grievance redressal mechanism of intermediary:

(a)The intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the name of the Grievance Officer and his contact details as well as mechanism by which a user or a victim may make complaint against violation of the provisions of this rule or any other matters pertaining to the computer resources made available by it, and the Grievance Officer shall –

(i) acknowledge the complaint within twenty-four hours and resolve such complaint within a period of fifteen days from the date of its receipt:

Provided that the complaint in the nature of request for removal of information or communication link relating to clause (b) of sub-rule (1) of rule 3, except sub-clauses (i),(iv) and (ix), shall be acted upon as expeditiously as possible and shall be resolved within seventy-two hours of such reporting;

Provided further that appropriate safeguards may be developed by the

> *intermediary to avoid any misuse by users;*
>
> *(ii) receive and acknowledge any order, notice or direction issued by the Appropriate Government, any competent authority or a court of competent jurisdiction.*
>
> *(b) The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it:*
>
> *(c) The intermediary shall implement a mechanism for the receipt of complaints under clause (b) of this sub-rule which may enable the individual or person to provide details, as may be necessary, in relation to such content or communication link."*

28. Rule 7 of the IT Rules categorically states that if any intermediary fails to observe the rules, the safe harbour protection provided to the intermediary under Section 79 of the IT Act will stand vitiated and the intermediary shall stand liable for prosecution under any law for the time being in force, including the IT Act and the Indian Penal Code, 1860.

29. Having reproduced the relevant provisions of the IT Act and IT Rules, we may now proceed with the role of the intermediaries. As can be discerned from the definition of "intermediaries" as provided by Section 2(1)(w), amongst various entities, search engines also fall under the category of intermediaries. A working paper on "Tackling the Dissemination and Redistribution of NCII" by Centre for Communication Governance (CCG) at National Law University, Delhi**,** observes that recognition of heterogeneity in intermediary functionality is necessary to ensure proper regulation of online content. The paper espouses that due to the heterogenous nature of intermediaries, mandating a single approach for removal of NCII content might prove to be ineffective. While espousing this viewpoint, the paper defines four different types of intermediaries:

> *"**ISPs**: connect their subscribers to the internet by supplying telecommunications facilities and equipment such as modems and last-mile connectivity. ISPs do not ordinarily filter or examine the data that is transmitted on their networks, nor can they interfere with the content by altering or removing the content they transmit. Thus, it is impractical to require ISPs to monitor and detect unlawful content. However, since they control their subscribers' access to the internet, they can block certain locations (URLs) on the internet if directed by a government or court order. This effectively prevents any of the ISPs' subscribers from accessing the URL. This may be particularly useful when websites refuse to remove unlawful content.*
>
> ***Websites hosting third-party content**: While some websites host their own content (eg, a news website), other websites allow third parties (eg, ordinary users) to upload content on their website. The latter type of website is an "intermediary" as it is hosting third-party content. Websites may host thousands of pieces of third-party content, and may not always be aware*

that they are hosting NCII. However, a user may complain directly to a website (identifying NCII content). Because websites host the third-party content, unlike ISPs, they have the ability to remove any unlawful content at source. Removal at source is preferable to blocking by ISPs, as it ensures the deletion of the content for every user on the internet, irrespective of which ISP they use or which country they attempt to access the content from.

***Social media platforms**: are similar to websites hosting third-party content but may be distinguished by their size and efforts to curate the content their users see (and don't see). The Intermediary Guidelines recognises that social media platforms with more than five million subscribers in India (termed 'significant social media companies' or "SSMIs") are subject to heightened obligations vis-à-vis unlawful content. Like websites (but unlike ISPs and search engines), SSMIs have control over third-party content on their platforms and can remove content at source if necessary. Further, SSMIs proactively detect unlawful content (including NCII) voluntarily because it is in their commercial interests to keep their platforms free of such*

***Search engines**: do not themselves store and transmit content but allow users to locate and visit content. Search engines 'crawl' web-pages across the internet, extracting key-words and metadata to identify the type of content on these pages. Search engines then 'index' the extracted data to make it accessible for future use. When a user submits a query, the search engine matches the query against pages in its index that likely have content useful to the user's query and displays them. Because search engines do not themselves host the content (such as NCII) on these pages, they cannot take down or remove unlawful content on websites. For the same reason, search engines cannot proactively detect unlawful content*

> ***like SSMIs. However, they can 'de-index' (remove from the search engine's index) specific URLs. Once a webpage is de-indexed, traffic to the page can be expected to decline, as new users who do not know the page's exact URL are unlikely to find the page given the billions of webpages on the internet.****"*
>
> **(**emphasis supplied**)**

30. Thus, while search engines do not themselves store and transmit content, they allow users to locate and visit content; basically, it enables individuals to find relevant webpages already available on the internet. Using the key-words provided by the user, a software known as *"crawlers"* is employed to scour the internet for the content that is being searched for and this process of crawling retrieves material in a matter of micro-seconds that is most relevant to the user. The material that is retrieved is stored and organized in an index which is a database of the content that has been discovered, which can then later be retrieved when searched for by a user. Search engines further rank the content in their order of relevance in a bid to solve the user's query at the earliest. It is relevant to note that as search engines do not host content *per se*, they cannot take down the content available on a third-party platform, such as websites. However, they can de-index specific URLs that can render the said content impossible to find due to the billions of webpages available on the internet and, consequently, reduce traffic to the said website significantly.

31. Search engines, however, cannot be categorised as social media intermediaries [Rule 2(1)(w)] or even significant social media intermediaries (SSMIs) [Rule 2(1)(v)] as they do not enable online interaction between two or more users, and they do not allow the users to create, upload, share, disseminate, modify or access information using its services. Thus, social

media platforms such as Facebook, Twitter, and Instagram may qualify as SSMIs, however, a search engine such as Google Search will not. This has further been clarified in FAQ 12 issued by MEITY on Part III of the IT Rules. By not falling under the ambit of SSMIs, search engines can, thus, be categorised solely as intermediaries, and their obligations are only limited to Rule 3 which is applicable to *all* intermediaries and not Rule 4 of the IT Rules which provides for additional due diligence that must be observed by SSMIs.

32. Being an intermediary simpliciter, as has been stated above, search engines are obligated to observe due diligence while discharging its duties under Rule 3, including making *reasonable efforts* to cause the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that is invasive of another's privacy, including bodily privacy, and violates any law for the time being in force. Rule 3(1)(d) states that on receiving actual knowledge in the form of a Court order or on being notified by the Appropriate Government or its agency under Section 79(3)(b), the search engine is required to not allow such offending content to continue on its platform, and it shall remove or disable access to that information as early as possible, but not later than thirty-six hours. For information received through the grievance redressal mechanism under Rule 3(2), the search engine is required to remove the offending content as expeditiously as possible and resolve the complaint within seventy-two hours of reporting. If the information is relating to content which is *prima facie* in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in nature of impersonation in an electronic form, including artificially morphed

images of such individual, the search engine is required to take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it. A mechanism for reporting such content by the user/victim is also to be devised by the intermediary in question under Rule 3(2)(c).

33. Pertinently, violation of any of this will lead to the safe harbour protection under Section 79 being taken away, as stated in Rule 7.Section 79, which recognises the principle of secondary liability and protects intermediaries from being held liable for content that is generated by third-parties, is not absolute in nature. It is incumbent upon intermediaries to duly discharge their obligations in order to avail this protection, and any lapse in following the IT Rules [as per Section 79(2)(c) and Rule 7] can lead to the protection accorded to it being taken away and paving the way for easy prosecution for the intermediaries.

CONTENTIONS OF THE PARTIES

Submissions on behalf of the *Amicus Curiae*

34. Mr. Saurabh Kirpal, learned *Amicus Curiae*, has provided a short note pursuant to the Order of this Court dated 08.11.2021 whereby this assistance was sought, and the following submissions have been advanced by him:

a. The applicable law obliges the intermediaries in question to take down offending content not limited to specific URLs provided to it by the users, but to remove all offending content from the platform under Section 79(3)(b) of the IT Act. He states that this safe

harbour provision under Section 79is only available to intermediaries as long as they perform their legal obligations under Section 79(3)(b).

b. Section 79(3)(b) stipulates that the obligation bestowed upon the intermediary extends beyond taking down the content in particular URLs and includes content that is found to be unlawful by a judicial order. Any limitation would render the statute and its purpose to be otiose, and thus, cannot be accepted.

c. Rule 3 of the IT Rules mandates removal of content by intermediaries, with Rule 3(1)(b) enlisting the content that is considered unlawful, including content that belongs to another person and to which the user does not have any right, and content that is invasive of another's privacy (including bodily privacy). Rule 3(1)(d) mandates the intermediary to remove unlawful content within thirty-six hours of receiving actual knowledge of a Court order or an order by a competent authority. Apart from a Court order or an order by a competent authority, Rule 3(2)(b) requires intermediaries to take down content within twenty-four hours of receiving a complaint in relation to the offending content.

d. The ratio of Shreya Singhal v. Union of India (supra) with regard to "actual knowledge" being construed as communication of Court order to the intermediaries is not applicable in the instant case as herein, the Court has already adjudicated upon the unlawfulness of the content, and that Rule 3(2)(b) which provides for a grievance

redressal mechanism available to the users was not before the Supreme Court in the said case.

e. The decision of this Court in X v. Union of India (supra) in a similar matter had already directed the Respondent-intermediaries therein to remove the content within twenty-four hours as per Rule 3(2)(b) of the IT Rules as well as to endeavour to employ pro-active monitoring by using automated tools, to identify and remove or disable access to any content which is "exactly identical" to the offending content that is subject matter of the Court order. It was also observed by this Court that for the Order of the Court to be effective in India, the content would have to be blocked by the intermediary
globally.

f. The judgment of the Supreme Court in Sabu Mathew George v. Union of India, **(2018) 3 SCC 229,**was relied upon to state that in the matter therein, the Supreme Court had directed search engines to delete advertisements pertaining to pre-natal sex determination within thirty-six hours of being informed of the same. The Order dated 16.02.2017 in the matter therein was passed to make search engines responsive to Indian law.

g. Respondent intermediaries are multi-billion dollar entities which possess vast technological and economic resources to develop the requisite tools for removal of NCII content. Moreover, there are existing tools for prevention of copyright infringement and child

pornography which can be deployed to reduce NCII abuse. The relevant portion of the Short Note recording the same has been reproduced as under:

> *"21. The legal obligation to remove unlawful content in its entirety and not just an obligation to remove URLs having been established, the tools available to comply with such obligation are an important consideration. Respondent Intermediaries are multi-billion dollar international conglomerates, possessing vast technological and economic resources to develop the tools and address the concerns raised in the present proceedings. It is a matter of public record, and as per the policies of the Respondent Intermediaries, that content detection tools are used for various purposes including preventing Intellectual Property Right (IPR) infringement and child pornography. The methods or tools presently used can be principally divided into (I.) Audio-Video Blocking; (II.) Image to Code Conversion; and (III.) Keyword Search.*
>
> *I. Audio-Video Blocking*
>
> *22. Respondent No.5/ YouTube, which is primarily an audio-video platform, regulates the content it hosts for, inter alia, copyright infringement. In order to ensure that no such infringement takes place. Respondent No.5/ YouTube deploys its 'Content ID' system. Under this system, the content provided by copyright owners is by an automated system compared to all videos hosted on the platform. This system is used by copyright owners to identify infringing content and require the platform to enforce its take down [Ref. Annexure G, Pg. 346],*
>
> *23. This mechanism is used to flag and identify videos that violate copyright laws. Smart technology is used to*

identify audio recordings in uploaded videos that infringe an individual's copyright [Ref. Annexure G, Pg. 348). Once these videos and audios are flagged by Respondent No.5/ YouTube, it has an option of, inter alia, blocking the content worldwide or in some countries/ regions [Ref. Annexure G, Pg. 348]. Therefore, tools for identifying objectionable content in audio-video form and blocking its access exist with Respondent No.5/ YouTube.

True copy of Respondent No.5/ YouTube's Content ID System is annexed herewith as ANNEXURE G [Pg. 346 to 348].

24. Additionally, Respondent No.5/ YouTube's 'CSAI (Child Sexual Abuse Imagery) Match' is its proprietary technology for combating CSAI Match content online. This technology allows it to identify known CSAI content in a sea of innocent content. When a match of CSAI content is found, it is then flagged for reporting in accordance with local laws and regulations [Ref. Annexure H, Pg. 349].

True copy of Respondent No.5/ YouTube's CSAI Match Policy is annexed herewith as ANNEXURE H [Pg. 349 to 353].

25. Given the existence of technology to identify specific videos throughout the platform, the same can be deployed to identify the video in question in the captioned matter. Technology similar to the aforesaid can be used, wherein Respondent No.5/ YouTube and other audio-video based intermediaries that host the content in question can identify and flag it, and then block access to the content worldwide to ensure that the content becomes unavailable on these platforms.

II. Image to Code Conversion

26. Respondent No.3/ Google, in its policy against Child Sexual Abuse Material ('CSAM') states that it deploys technology with the help of AI to ensure no such material is accessible on the internet [Ref. Annexure I, Pg. 355]. Respondent No.3/ Google uses technology to deter, detect, and remove CSAM from its platforms. This includes automated detection and human review to detect, remove, and report CSAM on its platforms. It deploys hash matching, including Respondent No.5/ YouTube's CSAM Match, to detect known CSAM.

27. Respondent No.3/ Google identifies and reports CSAM with, inter alia, hash-matching technology, which creates a 'hash' code, or unique digital fingerprint, for an image or a video so it can be compared with hashes of known CSAM. When it finds CSAM, it reports it to the National Center for Missing and Exploited Children ('NCMEC'), which liaises with law enforcement agencies around the world Respondent No.3/ Google identifies new CSAM it may create a hash code of the content and add it to its internal repository. Hashing technology allows Respondent No.3/ Google to find previously identified CSAM by comparing it to the repository and remove it from the platform [Ref. Annexure I, Pg. 355].

True copy of Respondent No.3/ Google's CSAM Policy is annexed herewith as ANNEXURE I [Pg. 354 to 364].

28. This technology is also applied to video content. Respondent No.5/ YouTube's CSAM Match 'Fingerprinter' has the ability to create a Fingerprint file of the video, a digital ID that uniquely represents the content of the video file. This is then compared with Respondent No.5/ YouTube's Fingerprint repository. The repository contains Fingerprints of known abusive content detected by Respondent No.5/ YouTube and Respondent No.3/ Google. Once the content is reviewed and identified as objectionable, the same is

eligible to be removed in accordance with local laws and regulations [Ref. Annexure, Pg. 353].

29. This technology, which is already being used to identify and remove CSAM content online, can be used to identify the images and/ or videos in the captioned matter, using the same identification algorithm. Once the content is identified, the same can be removed from all platforms to ensure that it becomes inaccessible to all individuals.

30. Additionally, Respondent No.3/ Google also deploys pattern and face recognition tools to recognize the common patterns of shapes and colors that make up the digital image of a face [Ref. Annexure J, Pg. 365]. Therefore, since Respondent No.3/ Google possesses technology to detect images based on their pattern, the same technology can be used to detect the images of the Petitioner in the captioned matter, in order to flag and remove them from the internet.

True copy of Respondent No.3/ Google's Pattern Recognition Policy is annexed herewith as ANNEXURE J [Pg. 365 to 366].

III. Keyword Searches

31. Respondent No.3/ Google, as a search engine functions in three steps; Firstly, it continually searches the web with automated programs called crawlers. Crawling is a discovery process whereby Respondent No.3/ Google uses technology (crawlers) to find new and updated web pages on the internet. Once new web pages are discovered, the crawlers follow links provided on those discovered web pages to find new URLs. This process is continued till all new URLs are discovered. Secondly, once any new or updated URL is found. Respondent No.3/ Google adds it to its index, which is a massive database of discovered URLs. This step is called indexing. Thirdly, when a search is

conducted subsequently on the search engine, URLs are then retrieved from this index based on the terms searched for, location, user preferences etc., and the best matches are displayed [Ref. Annexure K, Pg. 367, 369]. Essentially, when a user searches on Respondent No.3/ Google, they are not searching the live web. Instead, they search Respondent No.3/ Google's index of the web, which it regularly updates through crawling and indexing. Therefore, Respondent No.3/ Google, by its very nature and architecture, has the ability to detect and block content that is adjudicated to be unlawful and subject to takedown. True copy of 'How Google Search Works' available on developers.google.com is annexed herewith as ANNEXURE K [Pg. 367 to 372].

32. Respondent No.3/ Google, as a matter of policy, deploys tools to restrict search of certain keywords on its search engine. It blocks search results that lead to child sexual abuse imagery or material that appears to sexually victimize, endanger, or otherwise exploit children. Respondent No.3/ Google constantly updates its algorithms to combat these evolving threats and applies extra protections to searches that it understands are seeking CSAM content. It filters out explicit sexual results if the search query seems to be seeking CSAM, and for queries seeking adult explicit content, the search will not return imagery that includes children, to break the association between children and sexual content. In many countries (including India), users who enter queries clearly related to CSAM are shown a prominent warning that child sexual abuse imagery is illegal, with information on how to report this content [Ref. Annexure L, Pg. 373]. . True copy of Respondent No.3/ Google's Policy on Keyword Search is annexed herewith as ANNEXURE L [Pg. 373].

33. Additionally, the Hon'ble Supreme Court of India in the case of Sabu Mathew George v. Union of India

(2017) 2 SCC 516(2) propounded the 'doctrine of auto block', wherein intermediaries were directed to block a proposed list of words from search results on their platforms [Ref. Annexure M, Pg. 381, Para 9, Pg. 382 Para 10]. The Court held that when such words are searched on search engines, the results shall be 'auto blocked' with a warning and nothing would be reflected on the internet, since it is prohibited under the laws in force. The relevant portion of the judgment is reproduced below;

> *"9. Mr Ranjit Kumar, learned Solicitor General at this juncture would submit that he has been apprised today only about the proposed list of words" in respect of which when commands are given, there will be "auto block" with a warning and nothing would be reflected in the internet, as it is prohibited in India. We think it appropriate to reproduce the said "proposed list of words". It reads as under;*
>
> *****
>
> *10. At this juncture, Mr C.A. Sundaram, Mr K.V. Viswanathan, learned Senior Counsel, Mr Anupam Lai Das, learned counsel appearing for Google India, Microsoft Corporation (1) (P) Ltd. and Yahoo! India, respectively, have submitted that apart from the aforesaid words, if anyone. taking recourse to any kind of ingenuity, feeds certain words and something that is prohibited under the Act comes into existence, the "principle of auto block" shall—be immediately applied and it shall not be shown. The learned counsel appearing for the search engines/intermediaries have submitted that they can only do this when it is brought to their notice,— considered opinion, they are under obligation to see that the—doctrine of auto block" is applied within a reasonable period of time. It is difficult to accept the submission that once it is brought to their notice , they will do the needful. It need not be*

> *overemphasised that it has to be an in-house procedure/method to be introduced by the Companies, and we do so direct.'" (emphasis supplied)*
>
> *True copy of the order dated 19.09.2016 passed by the Hon'ble Supreme Court in Sabu Mathew George v Union of India (2017) 2 SCC 516(2) is annexed herewith as ANNEXURE M [Pg. 374 to 387].*
>
> *34. In the present matter, take down orders of this Hon'ble Court may specify key words such as name of the victim appearing in the impugned URL. Intermediaries must proactively thereafter take down content contained in different URLs that is similar or identical to the impugned URL, and block search results bearing such keywords, in light of Respondent No.3/ Google's keyword search policy and the decision of the Hon'ble Supreme Court in the case of Sabu Mathew George (supra).”*

Submissions on behalf of Google LLC

35. Mr. Arvind Nigam, learned Senior Counsel appearing for Google LLC and YouTube, i.e. Respondent Nos.3 and 5, has made the following submissions:

a. At the outset, all possible actions have been taken by Google to ensure that the offending content does not remain on its index with re-uploads being disabled and errant channels on YouTube being removed. Google Search, the search engine of Google LCC, does not host or publish or have any control over any content, and it merely indexes content made available by third-parties on their websites/platforms. It has specifically been excluded from the

definition of an "originator" under Section 2(1)(za) of the IT Act which is the person that generates the data being transmitted. It is similar to a library catalogue which has no information of its own, but merely points to the location of a particular book on a shelf. Further, unlike Google's text-based search results, image-based search results are more difficult to identify and retrieve, and it involves complex software algorithms that use information about an image as well as other information to match images to a user's queries in an automated manner. Thus, it is futile to render directions only to search engines and not to third-party websites which are the primary sources of NCII content.

b. As Section 2(1)(f) of the IT Rules consciously defines a communication link as a URL or a hyperlink, and when the same is read harmoniously with Section 79 of the IT Act, it indicates the legislative intent to ensure URL specific reporting. Reliance has been placed on Shreya Singhal v. Union of India (supra) to submit that the Supreme Court has held that intermediaries cannot be arbiters and are not expected to adjudicate on third-parties' rights. It is only upon receiving actual knowledge that a Court order has been passed asking it to expeditiously remove or disable access to certain links that the intermediary must do so. Further, even the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the grounds specifically laid down in Article 19(2) of the Constitution of India, 1950.

c. It has never been the intention of the Legislature to task

intermediaries with policing and monitoring of content under the garb of "due diligence", and that Rule 3(1)(d) affirms that an intermediary ought to take down content only upon receipt of the Court order or order from government agency. This has been clarified by the Executive *vide* FAQs dated 01.11.2021 whereby it is stated that the communication between the authorities to the intermediary should contain "platform specific identified URLs" and "justification and evidence". Thus, Orders for disablement of content have to be *qua* specific URLs and intermediaries are not expected to proactively sift through unlimited content to determine its legitimacy; their role must be neutral and not reactive [Refer to Muskan Jattana v. Union of India, **W.P.(Crl.) 956 of 2021**and Vandana Pal v. Union of India, **W.P.(Crl.) 1669/2021**]. Further, proactive monitoring would lead to the intermediary losing immunity/safe harbour protection provided under Section 79. Moreover, this Court in Anchit Chawla v. Google India, **W.P.(C) 13921/2018**, has recognised that Orders only against search engines are futile, and directions need to be passed against actual publishers to ensure holistic removal of content. Allowing intermediaries to apply its own mind to adjudge the legitimacy of online content will lead to chilling free speech, over-blocking as well as circumventing the fundamental right of online speech of third-parties. It would also undermine the right to privacy of users, which has been recognized by the Supreme Court, whose personal or sensitive personal data/information would be interfered with, and it would go against various decisions of the Supreme Court where blanket orders or pre-censorship of content was held to be illegal.

d. Reliance upon Sabu Mathew George v. Union of India (supra) is misplaced as the directions therein were rendered to "Google Ads" which is completely different from Google Search. Furthermore, directions were rendered for constitution of a Nodal Agency to report the content to the intermediaries who were then obligated to act upon the same. Even Order dated 13.04.2017 in the said matter observes that there ought to be no curtailment of access to information and knowledge, and that a balance has to be struck. Moreover, other Judgements of the Supreme Court, such as Anuradha Bhasin v. Union of India, **(2020) 3 SCC 637**, have categorically observed that any direction that restricts speech over the internet has to be proportionate and the least restrictive measure needs to be employed.

e. The IT Rules provide for a specific grievance redressal mechanism for reporting *prima facie* sexually explicit content under Rule 3(2). Rule 3(2)(c) clarifies that the mechanism for receipt of complaints requires provision of details *qua* specific communication links. Thus, directing the intermediaries to proactively filter and remove content is outside the purview of the IT Rules and entails casting of additional or exceptional onus on the intermediaries. The difference in obligations of an intermediary, which is what a search engine is, and a significant social media intermediary (SSMI) whose duties are enumerated under Rule 4 demonstrates that absence of proactive filtering on the part of an intermediary was a well-deliberated decision taken by the Legislature. Even Rule 4 does not

cast any mandatory obligation upon an SSMI to deploy automated tools and only an endeavour is to be made towards adopting any measures.

f. Application of tools to remove content has been discussed by the Supreme Court in In Re: Prajwala Letter dated 18.02.2015 Videos of Sexual Violence and Recommendations, **S.M.W. (Crl.) No. 3 of 2015**, but this has been limited to Child Sexual Abuse Material (CSAM). India has entered into an Memorandum of Understanding (MoU) with the National Centre for Missing and Exploited Children (NCMEC) for effectively combating the menace of CSAM content with reports being sent to the National Crime Records Bureau (NCRB) and the Ministry of Home Affairs. For the purposes of preventing CSAM content, automated flagging through hash-matching and Artificial Intelligence (AI)-based tools enables Google to act quickly and accurately to enforce its policies and rules. However, while cognition by an AI/ML (Artificial Intelligence/Machine Learning) tool of an image on the theme of "explicit content with a child subject" is useful to combat CSAM, a similar determination of "explicit content with an adult female subject" may not prove to be useful in any manner in identifying NCII. The factor of "consent" which is an essential ingredient for categorization of NCII cannot be detected by automated tools.

g. Other automated tools such as pattern recognition or AV matching are deployed for limited purposes and, thus, they cannot be applied indiscriminately to content of third-parties on any other

websites without any consent or permission. They have extreme technological limitations and adverse repercussions, especially on the exercise of free speech. As they cannot effectively distinguish between content and they operate in an "all or nothing" framework, there exists the possibility that they may end up jeopardizing and removing legitimate and genuine content.

h. Unlike CSAM which is patently and universally illegal, NCII content is dependent on the context in which it has been taken or shared. Despite Google's best efforts to prevent the content from re-appearing, many such content can be easily modified and thus, evades detection. The index that is cultivated by the search engines is only a "keyword on the page" + URL. The computer cannot qualitatively review this information to decide whether this pertains to the concerned subject or not. Any mandate to review such content will devastate the efficacy of platforms and cripple delivery of services online. There is also no obligation under law to put any filters *qua* search engines.

i. Reporting mechanisms *qua* Google Search have been provided by way of an Affidavit and the same has been reproduced as under:

> *"30. I say that the support pages and reporting mechanisms qua Google Search are briefly encapsulated hereinbelow, for ready reference of this Hon'ble Court:*

i. Google search engine provides a detailed mechanism with respect to Non-Consensual Explicit Images (NCEI), which is explained and can be accessed at the URL https://support.google.com/websearch/answer/6302812?hl=en;

ii. The specific reporting mechanism is available at the URL https://support.google.com/websearch/troubleshooter/9685456#ts=28 89054%2C2889099, so that the relevant team can review and take necessary action as per the applicable policies. This also includes reporting content for "doxing", i.e. the act of publishing the contact details of a person, with intent to harm;

iii. Pertinently, in addition to the aforesaid, users in India may use the webform available URL at the publicly https://support.google.com/legal/contact/lr_idmec for seeking removal of nudity or graphic sexual content about an individual, and upon request, Google may de-index these URLs thereby removing such content from Google search results. This is in accordance to Rule 3(2)(b) of IT Rules 2021.A

iv. Additionally, the specific help centre article for seeking removal of personal information is publicly available the URL https://support.google.com/websearch/answer/3143948;

v. Since Google requires specific URLs to identify any content, it also provides a detailed support page on identifying and reporting specific URLS. which is available at Regn. 1 https://support.google.com/webmasters/answer/63758

vi. Further, users/webmasters can also seek re-crawling of webpages, if the content thereon has changed. To this end, Google provides a webform for expeditious removal of outdated information, publicly available at the URL https://search.google.com/search-console/remove-outdated- content;

However, it is reiterated that search engines can only de-index search results, whereas only the webmasters have control on the content published on their webpages and can remove it. For this reason, any person willing to No content removed at the source should request such removal to the relevant webmaster. This is explained by Google at the support page at the URL https://support.google.com/websearch/answer/9109, which also indicates how to contact the webmaster and request a change.

31. I say that, with specific reference to India, Google has also created a dedicated web form for government agencies, including Law Enforcement Agencies (LEA), to report content that may be unlawful, which is actioned upon on priority. The same is freely and publicly available at the URL https://support.google.com/legal/contact/lr_gov_india and is routinely used by LEAs across India to report content. Copies of the aforesaid webforms are annexed herewith as Annexure R-5 (Colly).”

j. With regard to YouTube, its policies on CSAM are broad and any content related to sexual exploitation of minors is removed immediately. A combination of people and ML is deployed to detect problematic content at scale for detecting, reviewing, and removing

content that violates Community Guidelines. Individual reporting can be done anonymously by users who have come across potentially offensive content. A Trusted Flagger Program has also been developed that provides tools to individuals, government agencies and Non-Governmental Organizations (NGOs) for notifying YouTube of content that violates the Community Guidelines. Additionally, there are reviewer teams that remove content that violates the policies as well as age-restrict content that is not appropriate for all audiences. Further, automated flagging systems also exist to help identify and remove spam automatically as well as to monitor re-uploads of already flagged content. If it is determined by the users that the reported content is violative of the Community Guidelines, then it is immediately removed and a notice is sent to the uploader. All users are required to comply with all applicable laws.

k. Video-hashing technology is deployed to prevent re-uploads of identical copies of video content that has been removed for violation of Community Guidelines. This technology converts a particular video into an alphanumeric hash value which functions as a mathematically precise fingerprint of the original video. This allows the platform to prevent re-uploads of the violative content. AI/ML tools also exist which allows Google to prevent content that violates its Community Guidelines or Terms of Service from being widely viewed, or viewed at all, before it is removed. The Affidavit filed on behalf of Google states that *"through the application of these sophisticated technological tools, it has been possible to ensure that*

about 42% of all content removed are removed prior to the same being viewed even for a single time".

l. Google has also come up with Content Safety API (Application Programming Interface) which has been delineated in its Affidavit as follows:

> *"**17**. It is stated that Google is actively working on AI and ML research to solve issues pertaining to child safety to prevent the uploading of CSAM content on its platforms. Google recognises that detecting known CSAM images only addresses part of the problem. While the industry was effectively combating the spread of known images, a solution was needed to address the new CSAM that predators continue to generate, so as to increase the chances of helping minors still being victimised. With this in mind, Google recently announced Content Safety API (Application Programming Interface), a mechanism for sharing groundbreaking technology with NGOs and other industry partners, that allows for the prioritisation of review of content likely to contain abuse -- thus enabling those who use it to better review, report, and takedown content that may include previously unseen CSAM. This technology uses cutting-edge artificial intelligence (AI) that significantly advances Google's existing technologies to dramatically improve how service providers, NGOs, and other technology companies review such content at scale. By using deep neural networks for image classification, Google can now assist reviewers sorting through many images by prioritising the content most likely to contain abuse. This new technology keeps up with offenders by targeting abuse content that may not have been seen before. Quick identification of the new images means that children who are being sexually abused today are much more likely to be identified and protected from further abuse."*

Submissions on behalf of Microsoft

36. Mr. Jayant Mehta, learned Senior Counsel appearing on behalf of Microsoft Ireland Operations Ltd., i.e. Respondent No. 4, has made the following submissions:

a. A dedicated webform is available for reporting NCII and any member of the public may use this webform for requesting the removal of a nude or sexually explicit image or video of themselves that may have been shared without their consent. However, Bing (www.bing.com), which is the search engine that is operated by Respondent No.4, does not currently possess any technology for automatically finding and deleting NCII, and can only remove the content globally upon receiving notice of its existence. Further, Bing is not a content-hosting platform and has no control over the information published on third-party web pages. It becomes incumbent upon the user/victim to work with webpage owners to remove the content from the internet in its entirety.

b. Though the technology for image scanning exists, its implementation for the purpose of automatically finding and de-indexing NCII depends on development of a cryptographic database, interoperability standards, and Application Programme Interfaces (APIs) which can be used to identify duplication of NCII. Microsoft is currently working with a cross-industry coalition of tech

companies to put in place processes and standards for deployment of such technology that would be beneficial to user safety.

c. The IT Rules notified on 25.02.2021 were framed pursuant to directions of the Supreme Court, and they are a product of a lengthy and thorough consultative process between all stakeholders which took into account the requirement of balancing of issues of public safety with technological advancement that has been achieved by tech companies as of date. Certain key events that led to the enactment of the IT Rules were a Rajya Sabha Motion dated 26.07.2018 on "Misuse of Social Media Platforms and Spreading of Fake News" wherein the Minister for MEITY conveyed to the Upper House the need for a stronger legal framework to make social media platforms accountable under the law, and directions of the Supreme Court in In Re: Prajwala Letter dated 18.02.2015 Videos of Sexual Violence and Recommendations, **S.M.W. (Crl.) No. 3 of 2015**, as per which the Government of India had been directed to consult with intermediaries like Google, Microsoft, and WhatsApp, to formulate guidelines pertaining to circulation child pornography, rape and gang bang videos.

d. During the public consultation regarding the IT Rules, comments and counter comments were invited, and it was observed that deployment of automated filtering of content would have harmful effects as it could lead to removal of legitimate content. Further, requiring intermediaries to filter content would amount to excessive and unreasonable restriction on the fundamental right to

freedom of speech and expression. The decision to, thus, not incorporate auto-filtering/auto-moderation by intermediaries, was a deliberate and informed decision that was taken after weighing all pros and cons. Additionally, Rule 3(9) of the Draft Rules which were released on 24.12.2018 had provided for the intermediary to deploy technology-based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling access to unlawful information or content. However, this Rule was deleted post the consultative process, and pro-active filtering of any form is limited to Significant Social Media Intermediaries (SSMIs) as under Rule 4(4) of the IT Rules. Further, this Rule limits the obligation to actively filter to an *"endeavour"* to employ such measures, and is non-binding in nature.

e. Courts should refrain from interfering with rules and regulations that are framed by the Government, and the same has been reiterated by the Supreme Court time and again in various judgements such as Federation of Railway Officers Association v. Union of India, **(2003) 4 SCC 289** and Dr. Ashwini Kumar v. Union of India, **(2020) 13 SCC 585**. Further, interference cannot be made in a vacuum and only on the basis of the desirability of solutions.

f. Reliance has been placed on MySpace Inc. v. Supercassettes Industries Ltd., **2016 SCC OnLine Del 6382** to submit that the safe harbour protection under Section 79 of the IT Act demonstrates that the Parliament was mindful of the diligence that can be carried out by the intermediary. However, obligating intermediaries with

identifying infringing content from the non-infringing one would lead to impeding free speech and privatized censorship. Further, it would lead to the intermediary in question being liable for contempt of Court for not being able to comply with an Order that is impossible to perform. Thus, intermediaries may only remove content once it receives specific instances of the same and should refrain from doing so proactively.

Submissions on behalf of MEITY

37. Mr. Anurag Ahluwalia, learned CGSC, has advanced the following submissions of behalf of MEITY:

a. Section 79 of the IT Act contains safe harbour provisions for intermediaries as defined under Section 2(1)(w) and these intermediaries must observe due diligence guidelines as prescribed by the Central Government to ensure exemption from liability. The IT Rules enumerates the due diligence that must be observed by all intermediaries, including social media intermediaries and SSMIs. These Rules have been framed for increased user safety as they now allow users/victims to directly approach the intermediaries for requests pertaining to content takedown in specific cases relating to breach of bodily privacy, impersonation, morphed imagery of the concerned individual so as to prevent harm and emotional distress, particularly in instances of revenge porn. Statutory timelines have also been provided for grievance redressal and content takedown. The relevant portion from the Short Affidavit filed on behalf of MEITY is as follows:

"11. It is submitted that, as stated above, the IT Rules, 2021have a clear objective of enhancing online safety of users particularly women and children. It is further submitted that various provisions of the IT Rules, 2021 focus on enhanced safety of women and children. It is further submitted that these include:

1. Specific inclusion of certain requirements to be explicitly conveyed in terms and conditions [Rule 3(l)(b)].

2. Reporting by the aggrieved individual in respect of revenge porn and similar content breaching physical privacy and taking action within 24 hours for content removal [Rule 3(2)(b)].

3. Enhanced grievance redressal mechanism by intermediaries[Rule 3(2)(a)].

4. Additional provision for SSMI to appoint a Resident Grievance Officer, a Chief Compliance Officer and a nodal contact person, all to be residents in India; and a physical contact address of the significant social media intermediary to be in India [Rule 4(1)and 4(5)].

5. The Rules also have provisions that intermediary shall cooperate with Law Enforcement Agencies (LEA) to identify the first originator of information related to rape and child sexual abuse material (CSAM) imagery for prosecution [Rule 4(2)].

6. The significant social media intermediaries shall endeavor to deploy technology-based measures to identify any imagery of child sexual abuse, rape etc. whether real or simulated in accordance with the safeguards in the Rules [Rule 4(4)].

12. It is submitted that the IT Rules, 2021 provide for the following statutory timelines for grievance redressal and content takedown:

1. Grievance Redressal; 24 hours for acknowledgement and 15days for disposal [Rule 3(2)].

2. Information takedown from platform upon actual knowledge based on court order or notice from appropriate government authorised by law: 36 hours [Rule 3(1)(d)].

3. Providing information on a lawful request: hours 72 [Rule 3(1)(j)].

4. Removal of revenge porn (sexual extortion/non-consensual porn publication/sexual act or conduct involving impersonation, etc.) and other similar content: 24 hours [Rule 3(2)(b)]"

b. Though the grievance of the Petitioner falls under Rule 3(2)(b) of the IT Rules and the intermediary is obligated to remove the offending content within twenty-four hours, any proactive monitoring and removal of content will adversely affect the freedom of speech and expression of other individuals having the same or similar name as that of the Petitioner.

Submissions on behalf of Delhi Police

38. Ms. Nandita Rao, learned ASC (Criminal) for GNCTD, has advanced the following suggestions on behalf of Delhi Police. The same has been reproduced as under:

"1. Steps being taken by Delhi Police to monitor and prosecute offences against women and children on the internet

(a)www.cybercrime.gov.in portal has an inbuilt feature mechanism that automatically assists the victim/ complainant to send her complaint to the concerned PS/ unit as per her residence.

(b)District Cyber Police Stations have been established in each district and the same have dedicated NCMEC (National Centre for missing and exploited Children) / CP RGR (Child Pornography- Rape Gang Rape) Cell for handling the cyber issue related to women and children.

(c)A dedicated helpline, is functioning round the clock to help the victim of cyber-crimes.

(d)District Cyber Cells (DCC) have been replaced with the District Cyber Police Stations. The contact details of each District Cyber Police Station IS available on cybercelldelhi.in, Tatpar Delhi Police and other websites of Delhi Police."

ANALYSIS AND CONCLUSIONS

39. With the advent of the internet, its increasing access to the world at large, its ubiquity as well as with its all-encompassing nature and lack of borders, the dissemination of unlawful content by any individual can done with ease and without expeditious detection of the source of the same. As our virtual identities steadily gain more importance and space, the immortality of the internet raises questions on its impact on one's right to privacy and right to be forgotten. The internet never forgets, and once such content is uploaded, it becomes exceptionally difficult to control its spread.

In cases like these, the Court must appreciate that the matter is not adversarial in nature with no right or wrong, and the directions/guidelines are not such that there is an element of impossibility in its implementation, thereby frustrating the entire exercise; the aim of this exercise is to ensure that the victim of NCII dissemination does not have to undergo any further distress. Any solution that is provided must be deliberate and proportional, and should not be akin to a remedy that is worse than the disease. This Court cannot burn the house to roast the pig [Refer to decision of Supreme Court of United States in Reno v. American Civil Liberties Union, **521 US 244**].

40. As has been discussed above, intermediaries are granted protection and are not amenable to the principle of secondary liability on account of Section 79 of the IT Act. The principle of secondary liability denotes the legal responsibility that must be discharged by an entity for the actions of another. Section 79 exempts an intermediary from incurring this liability, and the rationale behind the same is that the fundamental rights of the users and the free flow of information on the internet must remain intact. However, once an intermediary, upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that an unlawful act is being committed by way of any information, data or communication link residing in or connected to a computer resource controlled by the intermediary, fails to remove or disable access to the said material, then Section 79(1) shall not apply. It is only under these exceptional circumstances that the principle of secondary liability is activated, and, despite NCII abuse being perpetuated by a third-party user and causing harm to a stranger, the intermediary becomes liable for the conduct of the third-party user. Further, the IT Rules also devise a mechanism for the user/victim to directly approach intermediaries for removal of NCII content without

having to obtain a Court order. Therefore, apart from making its own *reasonable efforts* in not publishing offending content, intermediaries can be requested to takedown offending content after being informed by a Court order or by an order of the appropriate Government or by the user themselves.

NCII and Right to Privacy

41. The Court order or order of the appropriate Government or its agency has to be in pursuance of the infringement of any law for the time being in force. In the instant case, not only does uploading of NCII lead to a clear violation of the provisions of the IT Act and IT Rules, it is also a violation of the right to privacy which is a sacrosanct aspect of Article 21 of the Constitution of India as held by a 9-Judge Bench of the Supreme Court in K.S. Puttaswamy v. Union of India, **(2017) 10 SCC 1**. In the said Judgement, the Supreme Court observed that privacy has distinct connotations, including decisional autonomy which comprehends intimate personal choices and informational control which empowers an individual to retain control over information pertaining to the individual. It would be appropriate at this juncture to reproduce the relevant paragraphs describing the various aspects of privacy:

> *"**248**. Privacy has distinct connotations including (i) spatial control; (ii) decisional autonomy; and (iii) informational control. [Bhairav Acharya, "The Four Parts of Privacy in India", Economic & Political Weekly (2015), Vol. 50 Issue 22, at p. 32.] Spatial*

control denotes the creation of private spaces. Decisional autonomy comprehends intimate personal choices such as those governing reproduction as well as choices expressed in public such as faith or modes of dress. Informational control empowers the individual to use privacy as a shield to retain personal control over information pertaining to the person. With regard to informational privacy, it has been stated that:

> *"... perhaps the most convincing conception is proposed by Helen Nissenbaum who argues that privacy is the expectation that information about a person will be treated appropriately. This theory of "contextual integrity" believes people do not want to control their information or become inaccessible as much as they want their information to be treated in accordance with their expectation (Nissenbaum 2004, 2010, 2011)". [Bhairav Acharya, "The Four Parts of Privacy in India", Economic & Political Weekly (2015), Vol. 50 Issue 22, at p. 34]*

*****

***250**. ..... The nine primary types of privacy are, according to the above depiction:*

(i) bodily privacy which reflects the privacy of the physical body. Implicit in this is the negative freedom of being able to prevent others from violating one's body or from restraining the freedom of bodily movement;

(ii) spatial privacy which is reflected in the privacy of a private space through which access of others can be restricted to the space; intimate relations and family life are an apt illustration of spatial privacy;

(iii) communicational privacy which is reflected in enabling an individual to restrict access to

communications or control the use of information which is communicated to third parties;

(iv) proprietary privacy which is reflected by the interest of a person in utilising property as a means to shield facts, things or information from others;

(v) intellectual privacy which is reflected as an individual interest in the privacy of thought and mind and the development of opinions and beliefs;

(vi) decisional privacy reflected by an ability to make intimate decisions primarily consisting one's sexual or procreative nature and decisions in respect of intimate relations;

(vii) associational privacy which is reflected in the ability of the individual to choose who she wishes to interact with;

(viii) behavioural privacy which recognises the privacy interests of a person even while conducting publicly visible activities. Behavioural privacy postulates that even when access is granted to others, the individual is entitled to control the extent of access and preserve to herself a measure of freedom from unwanted intrusion; and

(ix) informational privacy which reflects an interest in preventing information about the self from being disseminated and controlling the extent of access to information."

42. An individual's right to exercise control over their personal data has also been recognised by the Supreme Court in K.S. Puttaswamy v. Union of India (supra). It was observed therein that while it is not an absolute right, this right to exercise control over personal data would also encompass an

individual's right to control their existence on the internet. The following observation was made:

> ***"629. The right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the internet. Needless to say that this would not be an absolute right. The existence of such a right does not imply that a criminal can obliterate his past, but that there are variant degrees of mistakes, small and big, and it cannot be said that a person should be profiled to the nth extent for all and sundry to know."***

43. This right to privacy is also inextricably linked with the right to live a life with dignity. As noted in Section 66E of the IT Act as well, individuals have a reasonable expectation to privacy which is not lost within the confines of a domestic relationship, or even if any intimate image is shared with another person with the understanding and the expectation that the same will not be shared with third persons. The context in such situations matter with privacy being the expectation that information about an individual will be treated appropriately and in accordance with the individual's expectations; it is the said individual who retains control over any information pertaining to themselves. As a corollary, if the individual has the right to informational privacy, it also subsumes the individual's right to be forgotten which has been held to be the consequence of the dignity of an individual and, thus, a facet of the right to privacy.

44. A Division Bench of the Kerala High Court has recently in Vysakh K.G. v. Union of India and Ors., **2022 SCC OnLine Ker 7337**, while adjudicating upon right to privacy *vis-à-vis* right to information, referred to Cécile de Terwangne's paper on "Internet Privacy and Right to be

Forgotten/Right to Oblivion" to state that *"in the context of the Internet this dimension of privacy means informational autonomy or informational self-determination…Information self-determination means the control over one's personal information, the individual's right to decide which information will be disclosed, to whom and for what purpose".* The Judgement goes on to observe that, in the digital context, the "right to delisting" and "right to oblivion" are facets of the right to be forgotten.

45. The argument that has been advanced by the learned Senior Counsel appearing for the Respondent intermediaries is that as search engines merely provide access to content and are not responsible for hosting the said content, directions must be rendered to the publishers and not the search engines themselves. It is at this stage that a search engine's role in ensuring that one's right to privacy is not contravened comes into prominence, especially with Rule 3(1)(m) which states that the intermediary shall respect all the rights accorded to the citizens under the Constitution, including Articles 14, 19 and 21. It is further essential to state that the continued existence of NCII content on the internet does not serve any public interest and it is punishable under Section 66E of the IT Act. The argument, therefore, put forth on behalf of the Respondent intermediaries is not acceptable to this Court.

Social Responsibility of Search Engines

46. The duty and the liability of a search engine has been expounded in Judgement of the Court of Justice of the European Union (CJEU) in Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, **Case C-131/12**, wherein the Plaintiff's grievance was that a Google Search of his

name retrieved links to newspaper articles on his insolvency proceedings. The CJEU held that the role played by a search engine is such that it can significantly affect the fundamental rights to privacy and protection of personal data, and thus, a search engine must ensure that, within the framework of its responsibilities, powers and capabilities, its activities must comply with the law which would be rendered ineffective without its compliance. The CJEU also recognised the "right to be forgotten" and held that if the user's request was found to be in consonance with the law, then it was incumbent upon the search engine to remove the links in question as the law would supersede the search engine's financial interests as well as the interest of the general public in accessing that information. The relevant portion of the Press Release No. 70/2014 on the said Judgement issued in the English language by the Court of Justice of European Union at Luxembourg on 13.05.2014 reads as under:

> *"The Court further holds that the operator of the search engine is the 'controller' in respect of that processing, within the meaning of the directive, given that it is the operator which determines the purposes and means of the processing. The Court observes in this regard that, inasmuch as the activity of a search engine is additional to that of publishers of websites and is liable to affect significantly the fundamental rights to privacy and to the protection of personal data, the operator of the search engine must ensure, within the framework of its responsibilities, powers and capabilities, that its activity complies with the directive's requirements. This is the only way that the guarantees laid down by the directive will be able to have full effect and that effective and complete protection of data subjects (in particular of their privacy) may actually be achieved.*

As regards the directive's territorial scope, the Court observes that Google Spain is a subsidiary of Google Inc. on Spanish territory and, therefore, an 'establishment' within the meaning of the directive. The Court rejects the argument that the processing of personal data by Google Search is not carried out in the context of the activities of that establishment in Spain. The Court holds, in this regard, that where such data are processed for the purposes of a search engine operated by an undertaking which, although it has its seat in a non-member State, has an establishment in a Member State, the processing is carried out 'in the context of the activities' of that establishment, within the meaning of the directive, if the establishment is intended to promote and sell, in the Member State in question, advertising space offered by the search engine in order to make the service offered by the engine profitable.

So far as concerns, next, the extent of the responsibility of the operator of the search engine, the Court holds that the operator is, in certain circumstances, obliged to remove links to web pages that are published by third parties and contain information relating to a person from the list of results displayed following a search made on the basis of that person's name. The Court makes it clear that such an obligation may also exist in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

The Court points out in this context that processing of personal data carried out by such an operator enables any internet user, when he makes a search on the basis of an individual's name, to obtain, through the list of results, a structured overview of the information relating to that individual on the internet. The Court observes, furthermore, that this information potentially

concerns a vast number of aspects of his private life and that, without the search engine, the information could not have been interconnected or could have been only with great difficulty. Internet users may thereby establish a more or less detailed profile of the person searched against. Furthermore, the effect of the interference with the person's rights is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such lists of results ubiquitous. In the light of its potential seriousness, such interference cannot, according to the Court, be justified by merely the economic interest which the operator of the engine has in the data processing.

However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, the Court holds that a fair balance should be sought in particular between that interest and the data subject's fundamental rights, in particular the right to privacy and the right to protection of personal data. The Court observes in this regard that, whilst it is true that the data subject's rights also override, as a general rule, that interest of internet users this balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

Finally, in response to the question whether the directive enables the data subject to request that links to web pages be removed from such a list of results on the grounds that he wishes the information appearing on those pages relating to him personally to be 'forgotten' after a certain time, the Court holds that, if it is found, following a request by the data subject,

> ***that the inclusion of those links in the list is, at this point in time, incompatible with the directive, the links and information in the list of results must be erased. The Court observes in this regard that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where, having regard to all the circumstances of the case, the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed. The Court adds that, when appraising such a request made by the data subject in order to oppose the processing carried out by the operator of a search engine, it should in particular be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results that is displayed following a search made on the basis of his name. If that is the case, the links to web pages containing that information must be removed from that list of results, unless there are particular reasons, such as the role played by the data subject in public life, justifying a preponderant interest of the public in having access to the information when such a search is made."*** (emphasis supplied)

47. In another ruling of the CJEU in Google LLC v. Commission Nationale de l'informatique et des libertés (CNIL, **Case C-507/2017,** it was observed that it was for the search engine operator to take, if necessary, sufficiently effective measures to ensure the effective protection of the fundamental rights of the data subject (user/victim). These measures were required to meet all legal requirements and *"must have the effect of preventing or, at the very least, seriously discouraging internet users in the*

Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name".

48. However, in Da Cunha v. Yahoo de Argentina SRL and Another, **Expte. N 561/2010**, a case about defamatory search results, the Supreme Court of Justice of Argentina recognised that intermediary liability regimes in the European Union and the United States also accord immunity to intermediaries which remains contingent upon disabling of illegal content upon obtaining "actual knowledge" of the specific violation. They are, however, under no duty of general monitoring or policing of third-party data, and using filters to block search results would amount to prior censorship.

49. Closer to home, in Vysakh K.G. v. Union of India and Ors. (supra), the Kerala High Court has succinctly observed that Google cannot be said to be content-blind to publications made online and it is not a mere passive conduit. Rejecting the lack of liability as professed by the learned Counsel appearing for Google, the Kerala High Court observed as follows:

> *"**98**. We are not called upon here to determine the responsibility or liability of Google for publishing judgments online in terms of the Intermediary Rules. The publication of the judgments online and allowing the same to remain online forever may infringe upon the right of a party based on the right to be forgotten. We have already adverted to the nature of a right that can be claimed as a right to be forgotten. If the judgments of the Court are allowed to remain online for eternity, certainly, it would invade such rights of the parties. The problem that has arisen in the absence of legislation is determining the period or circumstances under which a party can invoke the aforesaid right. We are not remaining oblivious to this fact. A litigant may in the future, approach this Court to remove online content. In the absence of legislation,*

the Court may have to recognise his right and direct removal of such content available online on a case-to-case basis. The contention by the learned counsel for Google that they are only an intermediary and they are not liable for the contents or publication of the judgments, no doubt, the said contention has to be upheld. We are not here to decide upon compliance or non-compliance with the Intermediary Rules. The argument of the learned Central Government Counsel that Google has to be treated as an intermediary and therefore has to follow the Intermediary Rules does not require meritorious consideration in these cases. We are called upon, in these cases, to decide on the points involved qua fundamental rights claimed by the petitioners. Irrespective of these rules, the State and non-State actors are bound to respect the fundamental rights of the citizens. There is no difficulty in identifying Google as a non-State actor by its nature of function and operation which could have an impact on the socio, cultural, economic and political life of the citizen. They are qualified to be identified as a non-State actor. Even in the OECD Guidelines for Multi-national Enterprises, guiding principles on business and human rights, an enterprise like Google is liable as a non State actor for human rights violation. Google is incorporated in the United States of America and OECD is an intergovernmental organisation of which US is also a party. The Guidelines aim to promote positive contributions by enterprises to economic, environmental and social progress worldwide. [See OECD Guidelines for Multi-national Enterprises, 2011 Edition]. Further, there is no difficulty in holding that the claim based on fundamental rights can be enforced horizontally. However, the judgments are public records and, making them available to the public to view through the process of a search made online, cannot be found fault with. At the same time, we cannot hold that Google is content blind to the publications made online; can they allow any prohibited nature of content to appear online? For example, paedophilic

> *content. An algorithm means a set of procedures used for solving a problem or performing a computation. In the era of artificial intelligence, it is quite possible for Google to identify the nature of the content and remove the same. Google is not a mere passive conduit. They are now using AI tools to identify the needs and requirements of a user online and attempting to bring out the best results in what they are looking for online. Keeping aside the Intermediary Rules etc., we are of the firm view that Google cannot claim itself as a mere intermediary, allowing the contents to appear for the viewers or users in the digital platform. The publication of any valid records is protected by the Constitution as forming part of Article 19(1)(a), the right to freedom of speech and expression. There is no difficulty for Google during the era of advancement of AI to create a tool and identify particular data and remove the same. If that is not done, it would really infringe the claim based on the right to be forgotten."*

50. A review Petition, being R.P. No.107/2023, was preferred by Google Incorporation which was one of the Respondents, against the aforementioned judgment. Vide Order dated 30.03.2023, the Division Bench of the Kerala High Court observed as under:

> *"**4**. The above rule also requires Google to remove contents based on a Court order. In light of the above, it is clear that our observations do not run contrary to the statutory scheme. The further observation that Google can deploy AI tools to identify and locate data can be construed as only a suggestion and in no way would demand Google to deploy AI tools to identify such data. These are all matters which will have to be decided in future in the absence of any legislation, in appropriate litigation. These observations having no consequences, we find no reason to expunge the observations from the judgment. Review petitions are accordingly disposed of."*

It is necessary to note that the observations in R.P. No. 107/2023 shall have no bearing on the directions and the guidelines stipulated in the instant matter for the reason that the newly amended Rule 3 explicitly pronounces the obligation of the intermediary to not only "inform", but to make "reasonable efforts" to ensure that its users do not publish content that is prohibited under Rule 3(1)(b). Thus, any directions given herein fall squarely within the statutory regime with regard to obligations of intermediaries.

51. In a paper by L.M. Hinman on "Searching Ethics: The Role of Search Engines in the Construction and Distribution of Knowledge", it has been stated that with the increasing importance and pervasiveness of search engines, it can be found that search engines can no longer be said to be just providing access to knowledge, but are playing a central role in the constitution of knowledge itself. Users of search engines are increasingly dependent on search engines to filter through the ever-expanding universe of online data. Its pervasiveness is such that the very term "Google" is now used as a verb and is synonymous with "search". As a result, the mere de-indexing of an URL has an incremental impact on protecting one's right to be forgotten as it makes it almost impossible for someone to access the offending material if they are already not in possession of the specific URLs.

52. What can be culled out from the aforesaid legal literature is that a search engine plays an important role in the dissemination of content and its powers in connecting the said content to the consumers is undeniable. When viewed in this light, it is unfathomable as to how a search engine can feign helplessness when it comes to removal of or disabling access to links which *prima facie* contain content that is illegal as declared by the Court. There resides a social obligation in these intermediaries to be proactive in de-

indexing such links when it comes to its knowledge that such content is illegal. This Court finds the suggestion untenable that the user/victim must approach either the intermediary in question or the Courts every single time the NCII content is duplicated. Such a suggestion also frustrates the legislative intent behind the IT Rules which devises a time-bound schedule in removal of such content. An approach that entails the victim/user having to sift through the internet to identify and then share every URL hosting their NCII is unconscionable in the eyes of this Court.

Offending Entities Possess the Requisite Technology

53. Moreover, search engines cannot hide under the garb of not possessing the adequate technology to remove NCII content which has been reported without the victim/user having to approach the intermediary again and again. As per the Affidavit of Google LLC, hash-matching technology, which generates a unique identifier/fingerprint/hash, exists for the purpose of removing CSAM. This technology further allows detection and removal of the matched content that has previously been removed. For the purposes of removal of NCII, once such content has been identified and removed, the hash-matching technology can store *only* the unique identifier pertaining to the NCII content and in the event that such content is re-uploaded, it can filter out the same by going through its database of such fingerprints. A similar tool has already been built by Meta, available on www.stopncii.org to curtail the spread of NCII, and it can be used by the victim to create a unique fingerprint of the offending image which is stored in the database to prevent re-uploads. The tool is meant to compare this fingerprint (or hash) with the hashes of all the other images available on the site; if any image is

found to be identical, it is taken down. Microsoft has also developed a software by the name of Photo DNA which is currently being used to identify CSAM and is also being used by platforms such as Google and Twitter, and the database of the hashes generated is maintained by an independent organisation. YouTube has also developed CSAI (Child Sexual Abuse Imagery) Match which is used by NGOs and other companies to identify against the database of known abusive content

54. Flowing from the above, while this Court is of the opinion that entities of the nature of Google and Microsoft, considering their ubiquity, cannot abscond or withdraw from their duties to the public at large in the name of reducing the liability they might incur, this Court is inclined to agree with the submissions of the learned Senior Counsel appearing for Google and Microsoft that any direction that necessitates pro-active filtering on the part of intermediaries may have a negative impact on the right to free speech. No matter the intention of deployment of such technology, its application may lead to consequences that are far worse and dictatorial.

Is Right to Free Speech Being Violated ?

55. One of the concerns that arises when we consider the right to privacy of an individual under Article 21 is its impact on the right to freedom of expression and speech under Article 19(1)(a) which is an argument that has been posed by all parties in the instant matter. This issue requires an interpretation of the phrase "such content" in Rule 3(2)(b) and whether the same means a specific instance of identified NCII, as has been contended by the intermediaries, or all such content of identical nature, as submitted by the learned *Amicus Curiae.* This Court is of the opinion that construing the

phrase "such content" as "all content" is necessary to reduce the burden on the user/victim, however, "all content", access to which is to be disabled, must pertain to NCII abuse that has already been reported. Further, it is pertinent to note that unlike copyright infringement [as was the issue in MySpace Inc. v. Supercassettes Industries Ltd. (supra)], defamation, etc., NCII content conveys a higher degree of harm in society.

56. In a Judgement of this Court in X v. Union of India, **W.P.(Crl.) 1082 of 2020,** a direction had been given to all intermediaries by the learned Single-Judge Bench to engage in proactive monitoring and removal of NCII content that the Court had deemed to be illegal. There is currently an appeal pending against the said Judgement, however, no stay has been granted, and thus, the Order is still in operation. The working paper published by CCG records the risks that overbroad directions may pose, however, the viability of the directions in the said Judgement is of no consequence in the instant matter as the directions and suggestions being issued herein are restricted to search engines only. The relevant portion of the working paper is as under:

> *"**Proactive monitoring for NCII content**: In 2021, a Single Judge of the Delhi High Court attempted to address the problem of re-uploading of known NCII by stipulating that all intermediaries must engage in the proactive monitoring and removal of NCII that the Court had previously determined to be illegal.16 Such mandatory monitoring obligations create significant free speech and privacy risks as intermediaries must monitor all users to identify those uploading unlawful content.17 Such automated filtering has also been demonstrated to disproportionately restrict lawful expression by individuals from racial and linguistic minorities.18 Imposing a monitoring requirement on all intermediaries could lead to more content removal, but not necessarily better content removal, resulting in the removal of lawful speech. Therefore, curbing the*

redistribution of NCII requires a more nuanced approach. "

57. In such circumstances, a reading of the provisions that bestow an obligation upon an intermediary cannot be done in isolation and has to be conducted in a purposive manner. The principle of purposive interpretation focuses on interpretation of a provision in light of the purpose for which it was enacted. As has been stated by the MEITY itself, the IT Rules, which increases the burden upon intermediaries and widens their scope of losing their safe harbour under Section 79, were notified for ensuring open, safe, trusted and accountable Internet. The recent 2022 Amendment Rules also demonstrate the increase in the obligations of the intermediaries which is explicit in how intermediaries are now required to expend "reasonable efforts" in ensuring that its users do not host, publish, display, share, etc. any offending material defined under Rule 3(1)(b) instead of merely "informing" the users about the same, which was the case earlier. Search engines being an intermediary cannot hide behind the argument that they merely provide access to third-party websites as due diligence exercised as per Rule 3 is applicable to *all* intermediaries.

58. However, at this juncture, this Court finds to necessary to reiterate that in the instant case, the lackadaisical approach of the Respondents has come to light after a valid Court order has been rendered regarding takedown of the offending content. There is substance in the submission of the learned *Amicus Curiae* that the intermediaries cannot take shelter of the decision of the Apex Court in Shreya Singhal v. Union of India (supra) for the reason that an effective Court order regarding takedown of the unlawful content has already been rendered. Further, the IT Rules have now come into place which was not the case when the decision in Shreya Singhal v.

Union of India (supra) was rendered. In addition to "actual knowledge" as defined in Shreya Singhal v. Union of India (supra) as a Court order or upon being notified by the appropriate Government, Rule 3(2)(b) and (c) of the IT Rules now allows the victim/user to approach the intermediary on their own with their grievance. Further, it already mandates a timeline that must be adhered to when it comes to disabling access/de-linking the offending content. If read holistically, if the user/victim is required to approach with each specific URL again and again, this will only frustrate the purpose of the timelines and the grievance mechanism redressal as expounded under the IT Rules. It has been submitted that the sustained practice with regard to content removal under the IT Act has been to provide specific URLs, however, this practice fails to account for a grievance redressal mechanism available to the user/victim and it is not justifiable, morally or otherwise, to suggest that an NCII abuse victim will have to constantly subject themselves to trauma by having to scour the internet for NCII content relating to them and having to approach the authorities again and again. Once it has been reported by the user/victim or a Court order or an order of the appropriate Government has been rendered, then the search engine cannot contend that any filtering of the content that is done subsequent to the reporting or the Order is proactive in nature; it can only be termed as being in pursuance to the reporting of existence of such content specific to an individual or a judicial Order.

59. The fact that search engines do not host or publish or create content themselves is of no consequence when it comes to the question of removal of the access to the offending content. It is undeniable that they do have the ability, the capacity, and the legal obligation to disable access to the

offending content; this responsibility of the search engine cannot be brushed under the carpet on the ground that it does not host content.

60. This Court painfully notes that there is an abysmal absence of a collaborative effort that should ideally be undertaken by the intermediaries and the State. The focus of such entities and authorities should be on the quick redressal of the complaint brought before them rather than the shirking of blame or making submissions on the onerous nature of their duties. In the process of shirking responsibility, precious time is lost in removal of the offending content and it enables the offender to keep reposting the content. It further encourages other potential offenders to undertake such dissemination of NCII content as they are aware of the lack of consequences. This in turn frustrates the legal redressal mechanism in place and the harm, both emotional and reputational, caused to the victim/user persists and perpetuates. In a conservative country like India where matters of this nature are not a part of dinner table conversations, NCII abuse does indeed lead to harrowing consequences and everlasting stigma for the victim. In light of this, the endeavour of every entity involved should be to expeditiously resolve the issue.

DIRECTIONS AND RECOMMENDATIONS

61. In view of the foregoing observations, this Court deems it fit to render the following directions and recommendations to the Respondent Intermediaries, the Ministry of Electronics and Information Technology (MEITY), as well as the Delhi Police, for ensuring that cases of the instant nature are dealt in a manner that minimises the trauma caused to the victim and resolves the problem at hand expeditiously:

i. On approaching the Court for a takedown order in a matter involving NCII content, the Petitioner must, along with the petition, file an affidavit in a sealed cover identifying the specific audio, visual images and key words that are being complained against, in addition to the allegedly offending URLs for *ex facie* determination of their illegality.

ii. The Grievance Officer, as defined under Rule 2(1)(k), who is appointed by the intermediary for receiving complaints of the users/victims must be appropriately sensitised. The definition of NCII abuse must be interpreted liberally by the intermediaries to include sexual content obtained without consent and in violation of an individual's privacy as well as sexual content obtained and intended for a private and confidential relationships.

iii. The "Online Cybercrime Reporting Portal", which is a central platform available on cybercrime.gov.in, must have a status tracker for the complainant, commencing from filing of a formal complaint to the removal of the offending content. The portal must specifically display the various redressal mechanisms that can be accessed by the victim in cases of NCII dissemination. This display should be in all languages specified in the Eighth Schedule. The cybercrime.gov.in website, along with every other website of Delhi Police, should also notably display the contact details/address of each District Cyber Police Station present in the National Capital Territory of Delhi.

iv. On the receipt of information, noting the nature of NCII content which is punishable under Section 66E of the IT Act and the distress that its continued existence may cause to the victim, the Delhi Police must immediately register a formal complaint in order to initiate an investigation and bring the perpetrators to book as soon as possible so as to prevent the repeated upload of the unlawful content.

v. Every District Cyber Police Station must have an assigned Officer who must liaise with the intermediaries against which grievances have been raised by the victim who has approached the Delhi Police and an endeavour should be made to ensure that the grievance is resolved within the time schedules stipulated under the IT Rules. The intermediaries are directed to cooperate unconditionally as well as expeditiously respond to Delhi Police, and thereafter follow the time schedules under the IT Rules.

vi. A fully-functioning helpline which is available round-the-clock should be devised for the purpose of reporting NCII content. Operators and individuals manning this helpline must be sensitised about the nature of NCII content and must, under no circumstances, indulge in victim-blaming or shaming the victim. Considering the impact that NCII content has on the mental health of its victims, these operators should also have a database of organisations with registered counsellors, psychologists and psychiatrists available for reference to the victims. The Delhi Legal Services Authority may also be apprised and engaged in case the victims need legal aid.

vii. Search engines must employ the already existing mechanism with the relevant hash-matching technology on the lines of the one developed by Meta as has been discussed above. They cannot be allowed to avoid their statutory obligations by stating that they do not have the necessary technology, which is patently false as has been exhibited during the course of hearing.

viii. The reporting mechanism under Rule 3(2)(c) of the IT Rules must be conveyed to the users by the intermediaries by way of prominent display of the same on the website of the intermediary. It is necessary for users to be made aware of the reporting mechanism and the onus for educating the users lies on the intermediaries.

ix. The timeframe as stipulated under Rule 3 of the IT Rules must be strictly followed without any exceptions, and if there is even minor deviation from the said timeframe, then the protection from liability accorded to a search engine under Section 79 of the IT Rules cannot be invoked by the search engine.

x. When a victim approaches a Court or a law enforcement agency and obtains a takedown order, a token or a digital identifier based approach must be adopted by search engines to ensure that the de-indexed content does not resurface. This means that the user/victim may be assigned a unique token upon initial takedown of NCII content. If the user/victim subsequently discovers that the same content has resurfaced, then it is the responsibility of the search

engine to use the tools that already exist to ensure that access to the offending content is immediately ceased without requiring the victim to approach the Courts or other authorities again and again for removal of the same. The search engine cannot insist on requiring the specific URLs from the victim for the purpose of removing access to the content that has already been ordered to be taken down, and the victim cannot be made to face humiliation or harassment by having to approach the authorities or Courts seeking the same relief.

xi. As a long-term suggestion, a trusted third-party encrypted platform may be developed by MEITY in collaboration with various search engines under Rule 3(2)(c) for registering the offending NCII content or the communication link by the user/victim. Accordingly, the intermediaries in question may assign cryptographic hashes/identifiers to the said NCII, and automatically identify and remove the same through a safe and secure process. This would reduce the burden on the victim/user to constantly have to scour the internet for NCII pertaining to them and having to request for the removal/de-indexing of individual URLs. Utmost importance should accorded to the fact that the privacy of the user/victim must remain inviolable and the data collected for the purposes of using the hash-matching technology is not stored and misused. On account of the vulnerability of the data involved, the platform must be subject to greatest of transparency and accountability standards.

62. This lengthy exercise undertaken by this Court became necessary to protect the sanctity of due process so that a stop could be put to the Orders

of the Court being frustrated and undermined. Despite the existence of a legal framework governing the instant subject as well as the existence of the automated tools required to prevent the reproduction of NCII content that is *ex facie* illegal, this Court has taken judicial notice of the reluctance exhibited by intermediaries and the actual state of affairs when it comes to implementation of the law. This Court hopes that the directions and the suggestions provided herein will be duly followed by the entities involved.

63. This Court acknowledges the contribution of the learned *Amicus Curiae,* Mr. Saurabh Kirpal, and is pleased to extend its immense gratitude to him and his colleagues for their invaluable assistance and inputs on an issue of this nature and bringing much needed clarity to the same. This Court also acknowledges the contribution of Ms. Radhika Roy, Law Researcher, for her research, assistance and inputs in the case.

64. While there may be some issues that remain unaddressed, this Court feels compelled to state that the IT Act and the IT Rules are comprehensive and unambiguous in delineating the nature of obligations of intermediaries. Thus, the concerned authorities and entities must, without fail, comply with and implement the provisions stipulated thereunder. This Court, therefore, grants liberty to the learned *Amicus Curiae* to move an appropriate application in this regard, including any application for modification or clarification of directions/suggestions given above.

65. In view of the above observations and directions, the instant writ petition is disposed of, along with pending application(s), if any.

SUBRAMONIUM PRASAD, J

APRIL 26, 2023/*Rahul/RR*