***via* Video-conferencing**

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

Date of decision: 20th April 2021

\+ W.P.(CRL) 1082/2020 & Crl. M.A. Nos.9485/2020, 10986-87/2020

'X' .....Petitioner

Through: Mr. Sarthak Maggon, Advocate alongwith petitioner in-person.

versus

UNION OF INDIA AND ORS. .....Respondents

Through: Dr. Pavan Duggal, *Amicus Curiae.*
Mr. Ajay Digpaul, CGSC with Mr. Kamal R. Digpaul, Advocate for UOI.
Ms. Gayatri Virmani, Advocate for Ms. Nandita Rao, ASC for the State.
Mr. Meet Malhotra, Senior Advocate with Mr. Aditya Vaibhav Singh, Advocate for respondent No.3.
Mr. Parag P Tripathi, Senior Advocate with Mr. Tejas Karia, Mr. Ajit Warrier, Mr. Gauhar Mirza, Mr. Shyamal Anand, Mr. Thejesh Rajendran, Ms. Malikah Mehra and Ms. Mishika Bajpai, Advocates for respondent No. 4.
Mr. Sajan Poovayya, Senior Advocate with Ms. Mamta R. Jha, Advocate, Ms. Shruttima Ehersa, Advocate, Mr. Pratibhanu, Advocate, Ms. Raksha, Advocate and Mr. Sharan, Advocate for respondent No. 7.

CORAM:
HON'BLE MR. JUSTICE ANUP JAIRAM BHAMBHANI

J U D G M E N T

ANUP JAIRAM BHAMBHANI, J.

The internet never sleeps ; and the internet never forgets ! The true enormity of this fact has dawned over the course of hearings conducted in the present matter, when it transpired that despite orders of this court, even the respondents who were willing to comply with directions issued to remove offending content from the world-wide-web, expressed their inability to fully and effectively remove it in compliance with court directions; while errant parties merrily continued to re-post and re-direct such content from one website to another and from one online platform to another, thereby cocking-a-snook at directions issued against them in pending legal proceedings.

2. As submitted by Mr. Sarthak Maggon, learned counsel appearing for the petitioner, the principal grievance of the petitioner is that her photographs and images that she had posted on her private social media accounts on 'Facebook' and 'Instagram' have been taken without her knowledge or consent and have been unlawfully posted on a pornographic website called *'www.xhamster.com'* by an unknown entity called *'Desi Collector'* whereby the petitioner's photographs and images have become offensive by association. While certain other details of the petitioner and the photographs taken from her social media accounts have been recited in the petition, the same are not being recorded here for reasons of privacy and confidentiality. The

petitioner claims that her social media accounts had the requisite 'privacy settings' activated and yet these accounts were compromised, and her photographs and images were taken and placed on the pornographic website. It is the petitioner's contention that even though her photographs and images are otherwise unobjectionable, by placing the same on a pornographic website, the errant respondents have *ex-facie* committed the offence of publishing and transmitting material that appeals to the prurient interests, and which has the effect of tending to deprave and corrupt persons, who are likely to see the photographs, which is an offence under section 67 of the Information Technology Act 2000 ('IT Act', for short). The petitioner also contends that the errant parties have attached captions to her photographs, which act falls within the mischief of other penal provisions of the IT Act and the Indian Penal Code 1860 ('IPC', for short).

3. When the petitioner filed the present writ petition, she claimed she had already filed a complaint on the National Cyber-Crime Reporting Portal as well as to the jurisdictional police but to no avail; and by reason of inaction on the part of the authorities, the photographs had received some 15000 views within a week of being posted.

4. Since the particulars of respondents Nos. 5 and 6, namely the pornographic website and the the unknown entity, which it is claimed was responsible for placing the petitioners photographs on that website, were not available in the petition, nor even their address, no notice was issued to the said respondents in the beginning. Considering the nature of the matter, the said two respondents would

not be required to be heard at least in the present proceedings but may defend themselves at the hands of the state respondents including the jurisdictional police subsequently; and considering the nature of the order that this court proposes to pass in the present proceedings, it was not considered necessary to await the service of the said two respondents.

5. In the course of preliminary hearings in the matter it transpired that the specialised cybercrime unit of the Delhi Police, namely the Cyber Prevention Awareness and Detection Unit (CyPAD), submitted before this court that while it was ready and willing to comply with the court directions of removing/disabling access to the offending content relating to the petitioner, by reason of technological limitations and impediments, it could not assure the court that it would be able to entirely efface the offending content from the world-wide-web. On the other hand, the petitioner complained in the course of the hearings, that while this court was seized of the matter and interim orders for immediate removal of the offending content from the errant website had been directed, in brazen and blatant disregard of such directions, the errant respondents and other mischief-makers had re-directed, re-posted and re-published the offending content onto other websites and online platforms, thereby rendering the orders of the court ineffective.

6. This court accordingly perceived that the issue of making effective and implementable orders in relation to a grievance arising from offending content placed on the world-wide-web, needed to be examined closely; and a solution to the problem needed to be crafted-

out so that legal proceedings of the nature faced by this court did not become futile.

7. Addressing the foregoing issue required examination of our own statutory landscape, the technological limitations and reality and also as to how such matters have been addressed internationally. This court therefore appointed Dr Pavan Duggal, Advocate, who specialises in cyber-law and cyber-crime, as *Amicus Curiae* to assist in addressing the issues involved.

8. It may be noted that the issue of removing offending content is equally, if not more, significant at the time a matter is heard initially on a prayer for interim relief, for the reason that if the court is not in a position to pass *effective and implementable* orders and is unable to ensure that such orders are complied with at the interim stage, subsequent adjudication of the matter could well be rendered infructuous.

9. The court cannot permit itself to resign to the cat-and-mouse game of errant parties evading court orders by re-posting offending content across the world-wide-web, in an act of defiance and contumacy.

10. In this backdrop *vidé* order dated 07.08.2020 this court framed certain queries to get answers as to *what would be the implementable and effective directions* that should, and could, be issued by a court if it finds that certain content appearing on the world-wide-web is illegal or offending and ought to be removed. As observed above, the queries arose since despite directions issued by this court to remove certain content from the world-wide-web, the concerned respondents reverted, in effect, to say that *technologically it is impossible to*

entirely efface offending content from the world-wide-web; and the aggrieved party and the court would simply have to contend with an errant party or a mischief-maker continuing to re-post and re-direct offending content onto other platforms and websites on the world-wide-web despite the court ordering its removal. The respondents said that the only option for an aggrieved party would be to keep coming back to court each time and getting fresh orders for removal of offending content from each such online platform and website.

11. The queries framed were to the following effect :

i. Where a party seeks relief from the court to the effect that certain offending or illegal content be removed from the world-wide-web, *what directions* are required to be passed by a court to make its order implementable and effective; and to *which parties* are such directions required to be issued;

ii. What steps are required to be taken by law enforcement agencies to implement such directions issued by a court to ensure that despite court orders/directions offending content does not 'resurface' or remain available on the world-wide-web at the instance of errant parties; and such parties do not succeed in brazenly evading compliance of such orders/directions with impunity.

Submissions of Learned Amicus Curiae

Statutory landscape in India

12. In response to the foregoing queries, by way of his written submissions dated 16.09.2020 and 21.10.2020 as further elaborated in

the course of oral submissions, Dr. Pavan Duggal, learned *Amicus Curiae* has first drawn attention of this court to the following provisions of the Information Technology Act, 2000 as amended by Information Technology (Amendment) Act, 2008; and to the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009 ('2009 Rules', for short) and Information Technology (Intermediaries Guidelines) Rules 2011 ('2011 Rules', for short), which provisions are being extracted herein-below for ease of reference:

Information Technology Act, 2000 :

> "***1. Short title, extent, commencement and application. —***
>
> *...*
>
> *(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it* ***applies also*** *to any offence or contravention thereunder* ***committed outside India*** ***by any person***.
>
> * * * * *
>
> *"2. Definitions —*
>
> *(1) In this Act, unless the context otherwise requires, —*
>
> * * * * *
>
> *(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;*
>
> * * * * *

(v) "information" includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

(w) "intermediary", with respect to any particular electronic records, means ***any person*** *who on behalf of another person receives, stores or transmits that record* ***or provides any service*** *with respect to that record and* ***includes telecom service providers****, network service providers, internet service providers,* ***web-hosting service providers****,* ***search engines****, online payment sites, online-auction sites, online-market places and cyber cafes;*

* * * * *

*"**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 in 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.

*"**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.

* * * * *

*"**75. Act to apply for offences or contravention committed outside India-** (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to **any offence or contravention committed outside India by any person** irrespective of his nationality.*

*(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person **if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India**.*

* * * * *

*"**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."*

* * * * *

"***81. Act to have overriding effect**.—The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force:*

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957) or the Patents Act, 1970 (39 of 1970).]"

* * * * *

"***85. Offences by companies.***—*(1) Where a person committing a* ***contravention*** *of any of the provisions of this Act* ***or of any rule, direction or order made thereunder*** *is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:*

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is ***attributable to any neglect on the part of, any director, manager****, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.*

Explanation.—For the purpose of this section,—

(i) "company" means any body corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm."

(emphasis supplied)

Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 :

"***10. Process of order of court for blocking of information*** *– In case of an order from a competent court in India for blocking of*

*any information or part thereof generated, transmitted, received, stored or hosted in a computer resource, the Designated Officer shall, **immediately** on receipt of certified copy of the court order, submit it to the Secretary, Department of Information Technology and **initiate action as directed by the court**."*

(emphasis supplied)

Information Technology (Intermediaries Guidelines) Rules 2011:

*"**3. Due diligence to be observed by intermediary.—** The intermediary shall observe following due diligence while discharging his duties, namely:-*

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

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

...

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

* * * * *

*(3) The **intermediary shall not knowingly host or publish any information** or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission **as specified in sub-rule (2)**:*

*Provided that the following actions by an intermediary **shall not amount** to hosting, publishing, editing or storing of any such information as specified in sub-rule (2)—*

(a) *temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;*

(b) ***removal of access*** *to any information, data or communication link* ***by an intermediary after*** *such information, data or communication link* ***comes to the actual knowledge*** *of a person authorised by the intermediary* ***pursuant to any order or direction*** *as per the provisions of the Act*

(4) The ***intermediary****, on whose computer system the information is stored or hosted or published,* ***upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email*** *signed with electronic signature about any such information as mentioned in sub-rule (2) above,* ***shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2)****. Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.*

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove non-compliant information.

(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) ***When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective,***

> ***cyber security activity***. *The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.*
>
> * * * * *
>
> *(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of Rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint."*

(emphasis supplied)

13. While the proceedings in the present case were underway and counsel had made detailed submissions *inter alia* in respect of the 2011 Rules, in exercise of the powers conferred upon it under various provisions of section 87 of the IT Act, by way of notification bearing GSR No.139 (E) dated 25.02.2021, the Central Government has made the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('2021 Rules', for short) superseding the 2011 Rules. The relevant 2021 Rules are extracted below:

> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
>
> ***"2. Definitions: (1) In these rules, unless the context otherwise requires-***

…

*(j) 'grievance' includes any complaint, whether regarding **any content**, **any duties of an intermediary** or publisher under the Act, **or other matters** pertaining to the computer resource of an intermediary or publisher, as the case may be;*

* * * * *

(v) 'significant social media intermediary' means a social media intermediary having number of registered users in India above such threshold as notified by the Central Government;

(w) 'social media intermediary' means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;

(x) 'user' means any person who accesses or avails any computer resource of an intermediary or a publisher for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information and includes other persons jointly participating in using such computer resource and addressee and originator;

* * * * *

"***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 for access or usage of its computer resource by any person;

(b) the rules and regulations, privacy policy or user agreement of the intermediary shall inform 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 defamatory, obscene, pornographic, paedophilic, **invasive of another's privacy**, **including bodily privacy**,*

insulting or harassing *on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;*

(iii) is harmful to child;

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

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

(vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;

(vii) impersonates another person;

(viii) 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;

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

(x) ***is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person****, entity or agency for financial gain or to cause any injury to any person;*

(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 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.

(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 dispose off such complaint within a period of fifteen days from the date of its receipt;

(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 materia****l 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.

"***4. Additional due diligence to be observed by significant social media intermediary.***— *(1) In addition to the due diligence observed under rule 3, a significant social media intermediary shall, within three months from the date of notification of the threshold under clause (v) of sub-rule (1) of rule 2, observe the following additional due diligence while discharging its duties, namely:—*

(a) ***appoint a Chief Compliance Officer*** *who shall be responsible for ensuring compliance with the Act and rules made thereunder and shall be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Act and rules made thereunder:*

Provided that no liability under the Act or rules made thereunder may be imposed on such significant social media intermediary without being given an opportunity of being heard.

Explanation.—For the purposes of this clause —Chief Compliance Officer‖ means a key managerial personnel or such other senior employee of a significant social media intermediary who is resident in India;

(b) ***appoint a nodal contact person for 24x7 coordination with law enforcement agencies*** *and officers to ensure compliance to their orders or requisitions made in accordance with the provisions of law or rules made thereunder.*

Explanation.—For the purposes of this clause —nodal contact person‖ means the employee of a significant social media intermediary, other than the Chief Compliance Officer, who is resident in India;

*(c) **appoint a Resident Grievance Officer**, who shall, subject to clause (b), be responsible for the functions referred to in sub-rule (2) of rule 3.*

Explanation.—For the purposes of this clause, ―Resident Grievance Officer‖ means the employee of a significant social media intermediary, who is resident in India;

*(d) publish periodic compliance report every month mentioning the details of complaints received and action taken thereon, and the number of specific communication links or parts of information that the intermediary has removed or disabled access to **in pursuance of any proactive monitoring conducted by using automated tools** or any other relevant information as may be specified;*

(2) A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form:

Provided that an order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years:

Provided further that no order shall be passed in cases where other less intrusive means are effective in identifying the originator of the information:

Provided also that in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users:

Provided also that where the first originator of any information on the computer resource of an intermediary is located outside the territory of India, the first originator of that information within the territory of India shall be deemed to be the first originator of the information for the purpose of this clause.

(3) A significant social media intermediary that provides any service with respect to an information or transmits that information on behalf of another person on its computer resource–

(a) for direct financial benefit in a manner that increases its visibility or prominence, or targets the receiver of that information; or

(b) to which it owns a copyright, or has an exclusive license, or in relation with which it has entered into any contract that directly or indirectly restricts the publication or transmission of that information through any means other than those provided through the computer resource of such social media intermediary, shall make that information clearly identifiable to its users as being advertised, marketed, sponsored, owned, or exclusively controlled, as the case may be, or shall make it identifiable as such in an appropriate manner.

(4) ***A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts*** *any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit,* ***or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled*** *on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:*

Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:

Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this sub-rule, including a periodic review of any automated tools deployed by such intermediary:

Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.

(5) The significant social media intermediary shall have a physical contact address in India published on its website, mobile based application or both, as the case may be, for the purposes of receiving the communication addressed to it.

(6) The significant social media intermediary shall implement an appropriate mechanism for the receipt of complaints under sub-rule (2) of rule 3 and grievances in relation to the violation of provisions under this rule, which shall enable the complainant to track the status of such complaint or grievance by providing a unique ticket number for every complaint or grievance received by such intermediary:

Provided that such intermediary shall, to the extent reasonable, provide such complainant with reasons for any action taken or not taken by such intermediary in pursuance of the complaint or grievance received by it.

(7) The significant social media intermediary shall enable users who register for their services from India, or use their services in India, to voluntarily verify their accounts by using any appropriate mechanism, including the active Indian mobile number of such users, and where any user voluntarily verifies their account, such user shall be provided with a demonstrable and visible mark of verification, which shall be visible to all users of the service:

Provided that the information received for the purpose of verification under this sub-rule shall not be used for any other purpose, unless the user expressly consents to such use.

(8) Where a significant social media intermediary removes or disables access to any information, data or communication link, under clause (b) of sub-rule (1) of rule 3 on its own accord, such intermediary shall,—

> *(a) ensure that **prior to the time** at which such intermediary removes or disables access, **it has provided the user** who has created, uploaded, shared, disseminated, or modified information, data or communication link using its services with **a notification explaining the action being taken and the grounds or reasons for such action**;*
>
> *(b) **ensure that the user** who has created, uploaded, shared, disseminated, or modified information using its services **is provided with an adequate and reasonable opportunity to dispute the action being taken by such intermediary and request for the reinstatement of access** to such information, data or communication link, which may be decided within a reasonable time;*
>
> *(c) ensure that the Resident Grievance Officer of such intermediary maintains appropriate oversight over the mechanism for resolution of any disputes raised by the user under clause (b).*
>
> *(9) The Ministry may call for such additional information from any significant social media intermediary as it may consider necessary for the purposes of this part.*
>
> * * * * *
>
> ***7. Non-observance of Rules.**— **Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the Act shall not be applicable** to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.*"

(emphasis supplied)

14. A perusal of the 2021 Rules shows that the regulatory regime governing intermediaries has been sharpened in several ways. Notably, a 'grievance' has now been defined under Rule 2(1)(j) of the 2021 Rules; the concept of a 'social media intermediary' and 'significant social media intermediary' has also been brought in under

Rule 2(1)(w) and (v) respectively; and the definition of 'user' has been expanded under Rule 2(1)(x) of the 2021 Rules.

15. Under the 2021 Rules, as part of the due diligence to be exercised by it, an intermediary is now required by way of its rules and regulations, privacy policy or user agreement to *inter alia* inform its users that they must not host, display, upload modify, publish, transmit, store, update or share any information that 'belongs to another person and to which the user does not have any right' or which is *inter alia* 'invasive of another's privacy'. Under Rule 3(1)(d) of the 2021 Rules, it has been made encumbent upon an intermediary not to host, store or publish any unlawful information which *inter-alia* includes information that is violative of decency or morality, upon receiving actual knowledge about such information in the form of a court order or on being notified by the appropriate government or its agency. The Second Proviso to Rule 3(1)(d) makes it obligatory upon an intermediary to remove or disable access to such information as early as possible, but in no case later than 36 hours from the receipt of a court order or on being notified by the appropriate government or its agency. It is significant to note that the Third Proviso to Rule 3(1)(d) specifies that even *voluntary* removal or disabling of access to such information, data or communication link " ... shall not amount to a violation of the conditions of clauses ... " under section 79(2)(a) or (b) of the IT Act. Under Rule 3(1)(g), an obligation has also been cast upon an intermediary to preserve such information and associated records, without vitiating the evidence in any manner, for 180 days or

for such longer period as may be required by court or by a governmental agency, for purposes of investigation.

16. Rule 3(1)(j) further mandates an intermediary to provide information under its control or possession and assistance to a governmental agency, as soon as possible but not later than 72 hours of receipt of an order, for the purposes of investigation or cyber-security or protection, for the purposes of verification of identity, or for the prevention, detection, investigation or prosecution of offences.

17. A detailed and time-bound grievance redressal mechanism has also been engrafted in Rule 3(2) of the 2021 Rules, which mandates the nomination of a Grievance Officer by an intermediary, with contact details published on the intermediary's website, mobile-based application, or both, as the case may be, as well as a mechanism by which a user or victim may complain against violations of the rule; or any other matters pertaining to the computer resources made available by the intermediary.

18. In the context of the present case, it is relevant to note that Rule 3(2)(b) of the 2021 Rules sets-out a time frame of 24 hours from the receipt of a complaint, for an intermediary to '*take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it*' *inter alia* for 'artificially morphed images' of an individual.

19. Insofar as significant social media intermediaries are concerned, Rule 4 of the 2021 Rules prescribes additional due diligence to be observed by such entities, which is over and above the due diligence to be observed by all intermediaries under Rule 3. Broadly, the additional

due diligence engrafted in Rule 4(1)(a) includes the appointment of a 'Chief Compliance Officer' who is to be responsible for ensuring compliance with the IT Act and the rules made thereunder; and who is also to be liable for any proceedings relating to relevant third-party information, data or communication link made available or hosted by that intermediary.

20. Rule 4(1)(b) contemplates appointment of a 'Nodal Contact Person', being an employee of the intermediary other than the Chief Compliance Officer; who is to be resident in India and is to be available for 24x7 co-ordination with law enforcement agencies to ensure compliance of orders or requisitions made by them in accordance with the provisions of law or the rules made thereunder.

21. Furthermore, under Rule 4(1)(c), a significant social media intermediary is required to appoint a Resident Grievance Officer who is also required to be resident in India, and who is required *inter alia* to be responsible for the grievance redressal mechanism in terms of Rule 3(2). Moreover, under Rule 4(1)(d), the intermediary is required also to:

> "*(d) publish periodic compliance report every month mentioning the details of complaints received and action taken thereon, and the* ***number of specific communication links or parts of information that the intermediary has removed or disabled access to in pursuance of any proactive monitoring conducted by using automated tools*** *or any other relevant information as may be specified;*"

22. It may be mentioned in passing that in relation to the more serious offences impacting the sovereignty and integrity of India, security of

the State and other such matters, a significant social media intermediary is now also mandated to enable the identification of the 'first originator of the information on its computer resources'. It is important to note that under Rule 4(4) a significant social media intermediary is now required to '***endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information***' that depicts *inter alia* '***any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary***'. The intermediary is also required to display a notice to any user attempting to access such information, notifying that such information has been so removed or access-disabled. The Second Proviso to Rule 4(4) contemplates the implementation by a significant social media intermediary of 'appropriate human oversight' of the measures deployed under this sub-rule and the periodic review of automated tools so deployed.

23. Rule 4(6) mandates a significant social media intermediary to implement an appropriate mechanism for receipt of the complaints and grievances as required under Rule 3(2), including measures to enable the complainant to track the status of a complaint or grievance, and also for a complainant to be provided reasons for any action taken or not taken by such intermediary upon a complaint or grievance.

24. Rule 4(8) provides 'an adequate and reasonable opportunity' for a person who has created, uploaded, shared, disseminated or modified information that is removed or access-disabled by an intermediary to dispute and 'request for the reinstatement' of access to such

information, to be decided within a reasonable period of time. What is notable is that Rule 4(8) contemplates the opportunity of disputing the action of removal or access disablement and *request for reinstatement*, meaning thereby that information, data or communication link ***may***, in the first instance, be removed or access-disabled by a significant social media intermediary, if a significant social media intermediary, of its own accord, considers the information to be in contravention of Rule 3(1)(b), and the ***opportunity to the concerned user/person to dispute the action is required to be given subsequently***.

25. In fact, Rule 6 of the 2021 Rules empowers the Central Government to even notify any intermediary which is not otherwise a significant social media intermediary 'to comply with all or any of the obligations mentioned under Rule 4', in circumstances of material risk of harm to the sovereignty and integrity of India, security of the State and other similar serious situations.

26. What is most significant in the 2021 Rules is that while on the one hand, the Third Proviso to Rule 3(1)(d) protects an intermediary from action under section 79(2)(a) or (b) of the IT Act if the intermediary *even voluntarily* removes or disables access to any information, data or communication link that *inter-alia* falls within the categories specified in Rule (3)(1)(b), *Rule 7 of the 2021 Rules clearly and unequivocally stipulates that the exemption from liability otherwise available to an intermediary under section 79(1)* ***shall not be available*** *if a intermediary fails to fulfil its obligation under the 2021 Rules*. The exact wording of Rule 7 of the 2021 Rules bears repetition : *Where an intermediary fails to observe these rules, the*

provisions of sub-section (1) of section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.

27. Since this court is informed that the 2021 Rules have been challenged in certain proceedings which are pending before a Division Bench of this court as also before other High Courts; which proceedings have since been stayed by the Hon'ble Supreme Court which is seized of transfer petitions calling such matters before itself, it is necessary to clarify that no view is being expressed in the present matter as to the constitutional *vires* or any similar aspects of the 2021 Rules.

28. Moreover, this court is informed that the principal thrust of the challenge to the 2021 Rules is in relation to the Part III thereof which lays-down the "Code of Ethics and Procedure and Safeguards in Relation to Digital Media", which is not subject matter of consideration or application in the present matter. As presently advised there is no stay on the operation of the 2021 Rules, which have come into effect *vidé* notification dated 25.02.2021.

29. Now, what is clear from the enactment of the 2021 Rules in supersession of the 2011 Rules is *firstly*, that the Central Government has sharpened and expanded various aspects of the liabilities and obligations cast upon intermediaries to deal with unlawful content; *secondly*, specific timelines have been set-down for dealing with complaints by users/victims relating to unlawful content, more particularly the time for taking action for removal or disablement of access to *prima-facie* unlawful material has been effectively reduced

from 01 month under Rule 3(11) of the 2011 Rules to 24 hours under Rule 3(2)(b) of the 2021 Rules; *thirdly*, it has been expressly said in the 2021 Rules that omission on the part of an intermediary to remove or disable access to unlawful content would revoke the exemption from liability enjoyed by the intermediary under section 79 of the IT Act. Clearly the Central Government has brought in the afore-stated changes, appreciating the fact that to effectively remove or disable access to unlawful content, it is imperative that action be initiated *immediately* since any delay in such action can render the same ineffective and futile. The purport of the 3rd proviso to Rule 3(1)(d) is also clear, namely, that even if an intermediary removes or disables access to unlawful content "on a voluntary basis" in compliance with the other provisions of the rules, that shall not amount to violation of section 79(2)(a) or (b) of the IT Act by the intermediary; but *omission* by an intermediary to observe the 2021 Rules shall expose the intermediary to punishment both under the IT Act as well as under the Indian Penal Code in view of the new Rule 7 of the 2021 Rules.

Judicial Precedents in Foreign Jurisdictions :

30. Having noticed the basic statutory architecture in India relevant to the questions under consideration, it would be useful at this stage to examine how courts in foreign jurisdictions have viewed the position of 'intermediaries' such as internet service providers and search engines. This is especially relevant since search engines and other big technology companies, which *run the internet* as it were, operate on an international scale; and there is no reason why intermediaries

should be treated differently in India as compared to how they are treated in foreign jurisdictions.

31. In this backdrop, certain extracts from orders/judgements of foreign courts are placed below, which are self-explanatory, both as to the context and the view taken by such courts.

32. Explaining that an *'equitable obligation of confidence'* arises upon an intermediary; and holding that in certain cases the court may acquire statutory jurisdiction even over a foreign defendant, the Hon'ble Supreme Court of New South Wales, Australia in its decision in ***X. vs. Twitter Inc.***[1] has ruled as under:

> ***"The Plaintiff's Claim***
>
> *17. The jurisprudential basis of the plaintiff's claim against the defendants is uncontroversial. There is no necessity to prove that Twitter was 'knowingly concerned' in the user's breach of duty as against the plaintiff. The cause of action against Twitter is direct. It operates independently of the claim against the person originally responsible for the 'leak'.* ***Where a third party such as Twitter comes into possession of confidential information and is put on notice of the character of the information and the circumstances in which it was unlawfully obtained, it becomes subject to an equitable obligation of confidence****. It is liable to be restrained from publishing the information."*
>
> * * * * *
>
> ***"Jurisdiction***
>
> *20. Equally uncontroversial is the jurisdiction of this court to entertain the plaintiff's claim. In a case such as this, a defendant's presence in New South Wales is* ***not*** *a prerequisite to jurisdiction. When the circumstances stipulated in the Rules of court apply, it is*

[1] [2017] NSWSC 1300

unnecessary to serve the writ on the defendant within the territory of the state-which is the common law's ancient formula. The categories of case where the court may allow service out of the state, and by doing so acquire statutory jurisdiction over a foreign defendant, include where the claim is for 'other relief in respect of a breach of a contract,' or 'an injunction to compel or restrain the performance of any act in Australia,' or when the 'claim is founded on a cause of action arising in Australia,' or any combination of the above. Among other things, the injunction sought to compel or restrain the performance of certain conduct by the defendants everywhere in the world. That necessarily includes Australia. It follows that whether the defendants 'submit' or not is beside the point, at least as far as jurisdiction is concerned."

* * * * *

"22. To those authorities, one can add ***Spry's Equitable Remedies****, 9th ed. (2014) at 38, which states that '****… a court of equity will not consider itself debarred from interceding … merely because … the acts that [the plaintiff] seeks to have performed or enjoined, as the case may be, will, if they take place at all, take place outside the jurisdiction****."*

* * * * *

"The Orders

…

26. The 'order 2' referred to was that made by Stevenson J on 6 September. My subsequent interlocutory orders on 8 and 15 September followed the same pattern. The effect of the first part of the order was to ***restrain publication*** *of and to* ***require the removal of the 'Offending Material'****, and to* ***suspend the relevant accounts*** *from which it emanated. The Offending Material was defined to mean, first, the 'information contained in or referred to in' the specified tweets that had emanated from the particular Twitter handles adopted by the person or persons responsible. I see no*

problem in principle with the breadth of that part of the order, which operates in relation to historical and clearly identified information.

*"27. However, the final part of the definition of 'Offending Material' meant that the order also related to '**any further tweets posted** on the Twitter platform or the defendants' websites by any person who is the user of one or more of the accounts' with the same Twitter handle as had been used for the previous tweets... '**including any new account opened by such a person**'. This part of the order is in a different category. It **operates in relation to any future tweets** by the user or users responsible for the previous tweets, as well as any new account that may be opened by such a person. The intended objective is understandable but this part of the definition of 'Offending Material' **operates prospectively and is unlimited as to time or subject-matter**"*

* * * * *

"29. Hinging off that definition of Offending Material, the substance of the plaintiff's proposed final injunctive orders requires that the defendants:

> *(a) be restrained from publishing the Offending Material **anywhere in the world on the Twitter platform, their website or otherwise**;*
>
> *(b) **cause the Offending Material to be removed everywhere in the world** from the twitter platform and their websites;"*

* * * * *

"Discretion

. . .

*36. **I accept the plaintiff's submission that there must be a mechanism to filter information on the Twitter service**. Content relating to issues of national security and classified intelligence is an obvious example. In the absence of evidence and submissions from the defendants, and in the circumstances of this case, **I do not consider it unreasonable or inappropriate to make orders that***

impose a requirement for the 'application of some degree of filtering, or checking, to ensure that the information either does not get posted or, if it is posted, it is removed'.*"*

* * * * *

"Utility

…

39. First, as the aphorism goes, 'Equity acts in personam'. The plaintiff's right derives from the unconscionability, in the circumstances, of the exercise by the defendants of their legal rights. The proposed orders are a personal direction to perform or abstain from performing particular acts. They do not affect the proprietary rights of the defendants; they are not declaratory by nature; and they do not affect any question of title. As I have explained, ***there is a long history of courts of equity making in personam orders that are intended to operate extra-territorially****."*

* * * * *

"42. Fourth, ***there is a public interest in making the proposed orders; in demonstrating that wrongful conduct will be remedied as effectively as can be achieved; and in ensuring that the plaintiff's rights are respected to the extent that it is possible to do so***. ***The plaintiff should not be left without a remedy****. Furthermore, the second defendant, Twitter International Company is the sole shareholder of the Australian Twitter entity and therefore has assets in the jurisdiction that may be sequestrated, if it becomes necessary to do so."*

(emphasis supplied)

33. Opining on the obligation of a 'search engine' in relation to the list of results displayed following a search made through it, the Hon'ble Grand Chamber of the Court of Justice of the European Union in

Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González[2] ruled as follows:

> *"88 In the light of all the foregoing considerations, the answer to Question 2(c) and (d) is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied,* ***the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also 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****."*

(emphasis supplied)

34. Answering the objection raised by Google Inc. as to the global reach of an injunction made by a court within a certain territory, the Hon'ble Supreme Court of Canada in ***Google Inc. vs. Equustek Solutions Inc. et al.***[3] has addressed the issue in the following way :

> *"[1] Abella J. — The issue in this appeal is whether Google can be ordered, pending a trial,* ***to globally de-index*** *the websites of a company which, in* ***breach of several court orders****, is using those web-sites to unlawfully sell the intellectual property of another company. The answer turns on classic interlocutory injunction jurisprudence: is there a serious issue to be tried; would irreparable harm result if the injunction were not granted; and does the balance of convenience favour granting or refusing the injunction.*

---

[2] Case C-131/12; ECLI:EU:C:2014:317

[3] 2017 SCC 34

Ultimately, the question is whether granting the injunction would be just and equitable in all the circumstances of the case."

* * * * *

*"[17] Equustek therefore sought an interlocutory injunction to enjoin Google from displaying any part of the Datalink websites on **any of its search results worldwide**. Fenlon J. granted the order (374 D.L.R. (4th) 537 (B.C.S.C.)). The operative part states:*

> *Within 14 days of the date of this order, **Google Inc. is to cease indexing or referencing in search results on its internet search engines** the [Datalink] websites . . ., **including all of the subpages and subdirectories of the listed websites**, until the conclusion of the trial of this action or further order of this court. [Emphasis added.]"*

* * * * *

*"[37] The British Columbia courts in these proceedings concluded that because Google carried on business in the province through its advertising and search operations, this was sufficient to establish the existence of in personam and territorial jurisdiction. Google does not challenge those findings. **It challenges instead the global reach of the resulting order. Google suggests that if any injunction is to be granted, it should be limited to Canada (or google.ca) alone**.*

*"[38] **When a court has in personam jurisdiction, and where it is necessary to ensure the injunction's effectiveness, it can grant an injunction enjoining that person's conduct anywhere in the world**. (See Impulsora Turistica de Occidente, S.A. de C.V. v. Transat Tours Canada Inc., [2007] 1 S.C.R. 867, at para. 6; Berryman, at p. 20; Pitel and Valentine, at p. 389; Sharpe, at para. 1.1190; Spry, at p. 37.) **Mareva injunctions have been granted with worldwide effect when it was found to be necessary to ensure their effectiveness**. (See Mooney v. Orr (1994), 98 B.C.L.R. (2d) 318 (S.C.); Berryman, at pp. 20 and 136; Babanaft International Co. S.A. v. Bassatne, [1990] 1 Ch. 13 (C.A.); Republic of Haiti v. Duvalier, [1990] 1 Q.B.*

202 (C.A.); Derby & Co. v. Weldon, [1990] 1 Ch. 48 (C.A.); and Derby & Co. v. Weldon (Nos. 3 and 4), [1990] 1 Ch. 65 (C.A.); Sharpe, at paras. 1.1190 to 1.1220.)

"[39] Groberman J.A. pointed to the international support for this approach:

> ***I note that the courts of many other jurisdictions have found it necessary, in the context of orders against Internet abuses, to pronounce orders that have international effects**. Several such cases are cited in the arguments of [International Federation of Film Producers Associations and International Federation of the Phonographic Industry], including APC v. Auchan Telecom, 11/60013, Judgment (28 November 2013) (Tribunal de Grande Instance de Paris); McKeogh v. Doe (Irish High Court, case no. 20121254P); Mosley v. Google, 11/07970, Judgment (6 November 2013) (Tribunal de Grande Instance de Paris); Max Mosley v. Google (see "Case Law, Hamburg District Court: Max Mosley v. Google Inc. online: Inform's Blog https://inforrm.wordpress.com/2014/02/05/case-law-hamburg-district-court-max-mosley-v-google- inc-google-go-down-again-this-time-in-hamburg- dominic-crossley/) and ECJ Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, C-131/12 [2014], CURIA.*[3]

"[40] Fenlon J. explained why Equustek's request that the order have worldwide effect was necessary as follows:

> *The majority of GW1000 sales occur outside Canada. Thus, quite apart from the **practical problem of endless website iterations**, the option Google proposes is not equivalent to the order now sought which would compel Google to remove the [Datalink] websites from all search results generated by any of Google's websites world-wide. I therefore conclude that [Equustek does] not have an out-of-court remedy available to [it].*[4]

.....

... ***to be effective, even within Canada, Google must block search results on all of its websites***.[5]

As a result, to ensure that Google did not facilitate Datalink's breach of court orders whose purposes were to prevent irreparable harm to Equustek, she concluded that the injunction had to have world-wide effect.

"[41] I agree. The problem in this case is occurring online and globally. ***The Internet has no borders its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates globally****. As Fenlon J. found, the majority of Datalink's sales take place outside Canada. If the injunction were restricted to Canada alone or to google.ca, as Google suggests it should have been, the remedy would be deprived of its intended ability to prevent irreparable harm. Purchasers outside Canada could easily continue purchasing from Datalink's web-sites, and Canadian purchasers could easily find Datalink's websites even if those websites were de-indexed on google.ca. Google would still be facilitating Datalink's breach of the court's order which had prohibited it from carrying on business on the Internet.* ***There is no equity in ordering an interlocutory injunction which has no realistic prospect of preventing irreparable harm****.*

"[42] The interlocutory injunction in this case is necessary to prevent the irreparable harm that flows from Datalink carrying on business on the Internet, a business which would be commercially impossible without Google's facilitation. ***The order targets Datalink's websites the list of which has been updated as Datalink has sought to thwart the injunction and prevents them from being displayed where they do the most harm: on Google's global search results****.*

"[43] Nor does the injunction's worldwide effect tip the balance of convenience in Google's favour. ***The order does not require that***

> ***Google take any steps around the world, it requires it to take steps only where its search engine is controlled. This is something Google has acknowledged it can do and does with relative ease***. *There is therefore no harm to Google which can be placed on its "inconvenience" scale arising from the global reach of the order.*
>
> *"[44]* ***Google's argument that a global injunction violates international comity because it is possible that the order could not have been obtained in a foreign jurisdiction, or that to comply with it would result in Google violating the laws of that jurisdiction is, with respect, theoretical***. *As Fenlon J. noted, "Google acknowledges that most countries will likely recognize intellectual property rights and view the selling of pirated products as a legal wrong".6 "*
>
> * * * * *
>
> *"[50]* ***Google did not suggest that it would be inconvenienced in any material way, or would incur any significant expense, in de-indexing the Datalink websites***. *It acknowledges, fairly, that it can, and often does, exactly what is being asked of it in this case, that is, alter search results.* ***It does so to avoid generating links to child pornography and websites containing "hate speech***". *It also complies with notices it receives under the US Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2680 (1998), to de-index content from its search results that allegedly infringes copyright, and removes websites that are subject to court orders."*
>
> (emphasis supplied)

35. Again in ***Equustek Solutions Inc. vs. Jack***[4] the Hon'ble Supreme Court of British Columbia had this to say :

> *"[22] The effect of the U.S. order is that no action can be taken against Google to enforce the injunction in U.S. courts.* ***That does not restrict the ability of this Court to protect the integrity of its***

[4] 2018 BCSC 610

own process through orders directed to parties over whom it has personal jurisdiction."

(emphasis supplied)

36. Dealing with a case with very similar factual backdrop, the Hon'ble Third Chamber of the Court of Justice of the European Union has *vidé* its judgment dated 03.10.2019 in ***Eva Glawischnig-Piesczek vs. Facebook Ireland Limited*** [5] held as under:

> "*36 Given that a social network facilitates the swift flow of information stored by the host provider between its different users,* ***there is a genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user*** *of that network.*
>
> *"37 In those circumstances,* ***in order to ensure that the host provider at issue prevents any further impairment of the interests involved, it is legitimate for the court having jurisdiction to be able to require that host provider to block access to the information stored, the content of which is identical to the content previously declared to be illegal, or to remove that information, irrespective of who requested the storage of that information****. In particular, in view of the identical content of the information concerned,* ***the injunction granted for that purpose cannot be regarded as imposing on the host provider an obligation to monitor generally the information which it stores, or a general obligation actively to seek facts or circumstances indicating illegal activity****, as provided for in Article 15(1) of Directive 2000/31.*
>
> * * * * *
>
> *"**Costs***
>
> *55*
>
> *...*

[5] Case C-18/18; ECLI:EU:C:2019:821

On those grounds, the Court (Third Chamber) hereby rules:

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from:

– ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;

– ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, and

– ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law."

(bold in original; underscoring supplied)

Judicial Precedents in India :

37. Injunction orders have been made in relation to content available on the internet *inter-alia* by the Delhi High Court in several matters,

which orders reflect the judicial opinion on this issue. Reference to extracts of some of these orders may be in place here. In ***Swami Ramdev & Ans. vs. Facebook, Inc. & Ors.***[6] a single Judge of this court has said :

> "*106. Applying these very principles to the present case, it is clear that* ***any order passed by the Court has to be effective****. The parties before this Court i.e. the platforms* ***are sufficiently capable to enforce an order of global blocking****. Further, it is not disputed that the platforms are subject to in personam jurisdiction of this Court. The argument of the platform is that owing to the disparity in the law of defamation in the different jurisdiction, such an order ought not to be passed.*"
>
> * * * * *
>
> **"*Final Conclusion***
>
> * * * * *
>
> "*108. This Court is of the opinion that any injunction order passed by the Court has to be effective.* ***The removal and disablement has to be complete in respect of the cause over which this Court has jurisdiction****. It cannot be limited or partial in nature, so as to render the order of this Court completely toothless. If geo-blocking alone is permitted in respect of the entire content, there cannot be any dispute that the offending information would still reside in the global platforms of the Defendants, and would be accessible from India, not only through VPN and other mechanisms, but also by accessing the international websites of these platforms. It is not unknown that the Canadian, European and American websites of Google, Facebook, You Tube and Twitter can be accessed in India through various technological means. This would thus result in partial disabling and partial removal.*

---

[6] 2019 SCC OnLine Del 10701

"*109. Orders of Courts are meant to be implemented fully and effectively. While the Defendant-platforms are raising issues in respect of comity of Courts, conflict of laws and the right of freedom of speech and expression under Article 19(1)(a),* ***what is to be borne in mind is also the rights of privacy, the right of reputation of a citizen****, national security, national integrity, threats to sovereignty, etc. The balance is always hard to seek, however, Courts can only endeavour to strike the balance. Ld. counsels for the parties have rightly raised various concerns on both sides. This Court has to implement the statute in its letter and spirit.*

"*110. The interpretation of Section 79 as discussed hereinabove, leads this Court to the conclusion that the* ***disabling and blocking of access has to be from the computer resource, and such resource includes a computer network, i.e., the whole network and not a mere (geographically) limited network****. It is not disputed that this resource or network is controlled by the Defendants. When disabling is done by the Platforms on their own, in terms of their policies, the same is global. So, there is no reason as to why court orders ought not to be global. All offending material which has therefore, been uploaded from within India on to the Defendants' computer resource or computer network would have to be disabled and blocked on a global basis. Since the unlawful act in case of content uploaded from India is committed from within India, a global injunction shall operate in respect of such content. In case of uploads which take place from outside India, the unlawful act would be the dissemination of such content in India, and thus in those cases the platforms may resort to geo-blocking.*"

* * * * *

"*112. Under these circumstances, the following directions are issued to the platforms:*

(i) The Defendants are directed to take down, remove block, restrict/disable access, on a global basis, ***to all such videos/weblinks/URLs in the list annexed to the plaint****,*

which have been uploaded from I.P. addresses within India.

(ii) Insofar as the URLs/links in the list annexed to the Plaint which were uploaded from outside India are concerned, the defendants are directed to block access and disable them from being viewed in the Indian domain and ensure that users in India are unable to access the same.

*(iii) **Upon the Plaintiffs discovering that any further URLs contain defamatory/offending content** as discussed in the present order, the **Plaintiffs shall notify the platforms**, which shall then take down/block access to the said URLs either on a global basis, or for the India domain, depending on from where the content has been uploaded in terms of (i) and (ii) above.*

(iv) If the Defendant - platforms, upon receiving notice from the Plaintiffs are of the opinion that the material/content is not defamatory or violative, they shall intimate the Plaintiffs and the Plaintiffs would seek their remedies in accordance with law."

(emphasis supplied)

For completeness, it may be stated that though the decision of the learned single Judge in the above case has been challenged by way of a first appeal against the order, the Appellate Court has not stayed the operation of the order, except to say in its order dated 31.10.2019, that on statement of the respondent in the appeal, no contempt proceedings shall be initiated for non-compliance of the learned single Judge's order since the appeal had (at that time) been set-down for final hearing.

38. In ***YouTube LLC & Anr. vs. Geeta Shroff***[7] a single Judge of this court issued the following directions :

> *"17. The Court would note that it was never the case of Google that the contents of the offending post had been uploaded from a place outside India. It held that the contents have been uploaded from India, hence they were ordered to be removed from the internet so as to restore the position as it was prior to the uploading of the contents. The impugned order went on to hold that the contents which were uploaded from India, if transposted outside the jurisdiction of the country, cannot be said to be beyond the jurisdiction of India, and it could well be blocked or removed following the path by which it was uploaded. The Court is of the view that in the first instance, the injunction order dated 04.06.2015, which has not been challenged, has attained finality. It holds that on the basis of the pleadings and/or lack of denial from Google that the offending post had been uploaded from India, Google was required to remove it so as to* ***restore status quo ante****."*

(emphasis supplied)

39. Then again, in ***ABC vs. DEF & Ors.***[8] another single Judge of this court said :

> *"20. The defendants No.5 to 8 namely Facebook Inc, Snapchat Inc, Yahoo Inc and Instagram Inc* ***are also directed to remove any other material which the plaintiff may report as objectionable qua her i.e. photographs relating to her or any other content relating to the plaintiff from any other account****. The counsel for the plaintiff on behalf of the plaintiff states that the plaintiff will complain to the defendants No.5 to 8 only qua material relatable to this suit and violating her privacy."*

(emphasis supplied)

---

[7] 2018 SCC OnLine Del 9439

[8] CS(OS) No.160/2017

40. Most importantly, the role, duties and obligations of intermediaries under the IT Act have been authoritatively delineated by our Hon'ble Supreme Court in ***Shreya Singhal vs. Union of India***[9], where it has been held as under :

> *"Section 79 and the Information Technology (Intermediary Guidelines) Rules, 2011*
>
> *117. Section 79 belongs to Chapter XII of the Act in which intermediaries are exempt from liability if they fulfil the conditions of the section. Section 79 states:*
>
> * * * * *
>
> *"118. Under the 2011 Rules, by Rule 3 an intermediary has not only to publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource but he has also to inform all users of the various matters set out in Rule 3(2). Since Rules 3(2) and 3(4) are important, they are set out hereinbelow:*
>
> * * * * *
>
> *"119. The learned counsel for the petitioners assailed Rules 3(2) and 3(4) on two basic grounds. **Firstly, the intermediary is called upon to exercise its own judgment under sub-rule (4) and then disable information that is in contravention of sub-rule (2), when intermediaries by their very definition are only persons who offer a neutral platform through which persons may interact with each other over the internet**. Further, no safeguards are provided as in the 2009 Rules made under Section 69-A. Also, for the very reasons that Section 66-A is bad, the petitioners assailed sub-rule (2) of Rule 3 saying that it is vague and over broad and has no relation with the subjects specified under Article 19(2)."*
>
> * * * * *

---

[9] (2015) 5 SCC 1

"121. It must first be appreciated that Section 79 is an exemption provision. Being an exemption provision, it is closely related to provisions which provide for offences including Section 69-A. We have seen how under Section 69-A blocking can take place only by a reasoned order after complying with several procedural safeguards including a hearing to the originator and intermediary. We have also seen how there are only two ways in which a blocking order can be passed—one by the Designated Officer after complying with the 2009 Rules and the other by the Designated Officer when he has to follow an order passed by a competent court. The intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69-A read with the 2009 Rules.

"122. Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook, etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject-matters laid down in Article 19(2). Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79. With these two caveats, we refrain from striking down Section 79(3)(b).

"123. The learned Additional Solicitor General informed us that it is a common practice worldwide for intermediaries to have user agreements containing what is stated in Rule 3(2). However, Rule 3(4) needs to be read down in the same manner as Section 79(3)(b). The knowledge spoken of in the said sub-rule must only be through

the medium of a court order. Subject to this, the Information Technology (Intermediaries Guidelines) Rules, 2011 are valid."

"124. In conclusion, we may summarise what has been held by us above:

124.1. Section 66-A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2).

124.2. Section 69-A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 are constitutionally valid.

124.3. ***Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material. Similarly, the Information Technology "Intermediary Guidelines" Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as indicated in the judgment.***

* * * * *"

(emphasis supplied)

Submissions of Delhi Police

41. Mr. Rahul Mehra, the (then) learned Standing Counsel (Criminal) appearing for the Delhi Police, has stated the position of the Delhi Police on the matter based on written submissions dated 22.12.2020 filed under signatures of the Deputy Commissioner of Police, CyPAD/ Special Cell. Referring to and relying upon the provisions of section 79 of the IT Act and the 2011 Rules, Mr. Mehra has referred to the

obligations that the intermediaries are required to fulfil by way of due diligence in relation to their operations.

42. It is the submission of the Delhi Police that to ensure successful removal of offensive and unlawful content from the world-wide-web and to prevent such content being re-posted, re-transmitted or re-published on the world-wide-web, directions ought to be issued to the concerned intermediaries under section 79(3)(b) of the IT Act for removal of such content as identified through unique identifiers such as the URL (Uniform Resource Locator), Account ID, Handle name, Internet Protocol Address, hash value, pixel matching, structural similarity index etc. of the content.

43. It has further been submitted by the Delhi Police that directions ought to be issued to intermediaries under section 79(3)(a) of the IT Act read with section 107 of the IPC and rule 3(2) of the 2011 Rules, to prevent further posting, transmission or publication of 'identified unlawful content'.

44. The Delhi Police have also said that it has become commonplace, that law enforcement agencies issue notices under section 91 of the Cr.P.C. and/or Rule 3(7) of the 2011 Rules calling upon intermediaries to furnish information; and to also remove identified unlawful content, however intermediaries often stymie efforts of law enforcement agencies to undertake quick investigation of cases by not co-operating with due expedition and also delay removal of such content. Furthermore, the Delhi Police say that for investigation of such matters, in order to apprehend the perpetrators and break the chain of repeated uploads, they require concerned intermediaries to share the

actual unlawful content that has been uploaded, the metadata, the data dump and also the basic subscriber information, access logs etc. relating to such information.

45. The Delhi Police have also expressed the grievance that instead of responding expeditiously to their requests for information, social media platforms, instant messaging services, e-mail services etc. sometimes even ask law enforcement agencies to adopt the route of getting Letters Rogatory (LRs) issued and ask them to resort to prolix remedies under Mutual Legal Assistance Treaties (MLATs), even when unlawful content has been uploaded from an Indian IP address. This, the Delhi Police complains, is cause for much delay in obtaining necessary information and material to bring the perpetrators to book, who (latter), in the meantime continue to repeatedly upload unlawful content.

Submissions of Google LLC

46. Mr. Sajan Poovayya, learned senior counsel appearing on behalf of Google LLC/respondent No. 7, has in the first instance, submitted that though Google LLC has no information on the actual nature of the offending content that is in question in the present proceedings, it has no opposition to removing access to the offending content as may be directed by this court. Mr. Poovayya, has explained in detail the exact business and role of Google LLC as the incorporated entity that *inter alia* owns the search engine called 'Google Search', alternatively also called just 'Google'. It has been submitted that intermediaries that run search engines are not 'publishers' and that they merely 'index' existing information on-line and to that extent have only a limited

role, owing to the automated manner of functioning of search engines. It has also been emphasized that the legal framework mandates that the internet be kept free from editorial intervention.

47. As regards the issue of removal of content or blocking access is concerned, it has been submitted that the role of the search engine is 'reactive' and is *limited to disabling access to specific URLs by effacing or removing such URLs from the search results*, once these are reported by governmental agencies or ordered by court; and that their role is not 'proactive'. It is submitted that search engines cannot be tasked with adjudicating the legitimacy of content that may be searched through them. It has further been submitted that prior restraint or blanket ban or censorship of content cannot be ordered since the same would be contrary to the freedom of speech and expression guaranteed by the Constitution and may even have a chilling effect on fundamental rights; and further that no orders may be passed that may affect legitimate or justified content, even as an inadvertent consequence of such restraint orders.

48. Learned senior counsel appearing on behalf of Google LLC has highlighted the difference between 'publisher websites' and 'search engines', to say that content is actually hosted on a given website or online platform, which website or online platform is controlled by a webmaster or owner; and it is the concerned website/online platform/ webmaster/owner that is the 'publisher' of such content; and that Google Search does not publish nor host nor control any content but only 'indexes' it. It is further submitted that search engines only access a small portion of the world-wide-web and 'private networks'

or 'walled gate' applications or other protected systems cannot even be assessed by search engines.

49. Further, explaining the manner in which Google Search operates, it is submitted that the search engine uses automatic software known as 'crawlers' that visit a web-page and analyse the text and non-text content on it. A 'crawler' sorts the information on a web-page into an 'index', which is a purely passive and automated process, by which similar content is grouped together. It is explained that an 'index' on a search engine is akin to a library catalogue that explains where books on a particular topic are located in a library and the catalogue itself *does not contain* the information, but merely points to its location, like a book on a shelf in the library. Each search result comprises a 'title' (which is the clickable hyperlink to the relevant webpage), the URL of the relevant web-page and a snippet (which is an automatically generated excerpt from the relevant web-page).

50. It has been further submitted before this court that Google Search also has the facility of searching for specific 'images' as opposed to specific 'text'. Google Image Search is a feature of Google Search that displays image-based results in response to a user's query instead of text-based results.

51. Learned senior counsel explains that unlike text-based search results, image-based search results are much more difficult to identify and retrieve since an image search employs complex algorithms that use information about an image such as the *name* of the image file as stored on a web-page, *information* about the web-page on which the image appears, and other similar information. It is submitted that in

order to locate an image on the world-wide-web it is crucial to have both the *Image URL* and *Web URL* pertaining to a particular image. This is particularly relevant in the context of the present matter since the petitioner is concerned about her photograph, whether in the same or similar form, that has been posted by the errant respondents on various inappropriate websites and platforms, in breach of her privacy and in order to embarrass her.

52. In response to the query made by this court as to whether it is possible for a search engine to *make content non-searchable* so that even if the content is available and continues to reside on various websites or online platforms, it should not be identifiable, locatable and cannot be searched-up, so that it is effectively unavailable for viewing, it has been explained that in the first instance, content can be made non-searchable by the web-master/owner of the website or online platform by choosing not to have the content 'indexed' by a search engine. This can be achieved either by password protecting the content or the server. The second way of doing this is for a web-master/owner to add a simple code "robot.txt" to its website root server; as a result of which when Google crawlers encounter this code, they would remove the content from the Google index. A third way to make content non-searchable is to add 'meta-tags' such as "noindex" to the HTML code of a website, and upon reading these meta-tags, the Google crawlers would not add such page/content to the Google index.

53. Learned senior counsel has further explained that the forgoing options for making content non-searchable are publicly available at "*https://developers.google.com/search/docs/advanced/crawling/control-what-*

you-share". However, it is submitted that these methods for making content non-searchable can only be initiated by a web-master/owner independently and not by a search engine like Google.

54. It is further submitted that Google has well-documented policies and robust webforms for notifying any content that is believed to be objectionable, all of which are available on-line. By this mechanism, Google reviews reports and complaints received from governmental agencies, by way of court orders or from users, which complaints are reviewed and acted upon, based on the applicable product policies and laws. Webform for this purpose are also stated to be publicly available at "*https://support.google.com/legal/answer/3110420*".

55. It is further stated that Google also has a Grievance Officer, whose details may be taken from "*https://www.google.com/intl/en_in/contact/grievance-officer.html*".

56. It is further stated that Google also has a well-documented policy for removing images from Google Search, which policy is publicly accessible at "*https://support.google.com/websearch/answer/4628134?hl=en*". Specifically, with reference to its operation in India, Google is stated to have created a dedicated webform for Governmental Agencies to report content that is unlawful, which form is publicly available at "*https://support.google.com/legal/contact/lr_gov_india*"; and it is assured that complaints received on this webform are acted upon on priority basis.

57. Learned senior counsel submitted that the surest way to ensure that offending content is not accessible is to *remove it from its source*, namely the website or online platform on which it is residing; but this

can only be undertaken by the web-master/owner of the website or online platform. Alternatively, the web-master/owner of a website or online platform may opt-out of indexing offending content from a search engine, by using publicly available tools, so that such content is no longer included in the search results of a search engine such as Google Search.

58. In this backdrop, it is learned senior counsel's contention that a search engine is not the entity to which directions are required to be passed if offending content is to be removed from the world-wide-web; and in the alternative, if such directions are at all passed, they must be only *qua* specific content, which have been duly adjudicated to be unlawful under specific provisions of applicable law, and no blanket directions or order that require proactive monitoring on the part of the search engine ought to be passed since such proactive monitoring is technologically impossible of compliance, apart from being legally untenable. In fact, it is pointed out that it has been repeatedly held by the Hon'ble Supreme Court that an intermediary *cannot be allowed* to apply its own mind to adjudge the legitimacy of online content *inter alia* in *Shreya Singhal* (supra). Mr. Poovayya submitted that it is not the intention of the Legislature to task intermediaries with policing or monitoring content in the garb of carrying-out due diligence; and that Google LLC is statutorily exempt from any liability resulting from any third-party content that may have been indexed on its search engine, and its role is limited to de-indexing content once it has been adjudicated as unlawful and reported to it.

59. In relation to the technological impossibility of monitoring what is perceived to be unlawful content, Google LLC further submitted that this becomes particularly unimplementable where the issue is not of the content *per se* but the *context in which certain content is appearing* on a website or online platform. It is submitted that in these circumstances it is impossible for Google LLC to determine which content is objectionable and which is legitimate, with reference to which context; and therefore it is necessary to *specify a particular URL for de-indexing* unlawful content, which is the only way by which such content can be identified and de-indexed. It is submitted that any other course of action would jeopardise legitimate and genuine content since technological and automated means would be unable to differentiate or exercise any discretion, particularly when content is unlawful by reason of the context.

60. Attention of this court is drawn to a judgment of a Division Bench of this court in ***Myspace Inc vs. Super Cassettes Industries***, 2017 (69) PTC 1 (Del) (DB), where the Division Bench has opined as follows:

> "*62. ...The remedy here is not to target intermediaries but to ensure that infringing material is removed in an orderly and reasonable manner. A further balancing act is required which is that of freedom of speech and privatized censorship. If an intermediary is tasked with the responsibility of identifying infringing content from non-infringing one, it could have a chilling effect on free speech; an unspecified or incomplete list may do that. In an order of relief such as that passed by the learned Single Judge, MySpace would be in contempt of court for not complying with an order, which is otherwise impossible or at best onerous and cumbersome of performance.* ***In order to avoid contempt action, an intermediary would remove all such content, which even remotely resembles***

> ***that of the content owner. Such kind of unwarranted private censorship would go beyond the ethos of established free speech regimes.***
>
> "*66. ... The Court is conscious of the fact that under the current system, MySpace hosts several hundreds and thousands of videos, which is only growing every single day. Without a notice containing the details and location of the exact works in which infringement is complained of, MySpace cannot be expected to scan through such large number of videos to discern infringement.* ***This is not only impractical but also dangerous for reasons discussed previously. A vague order of injunction against works which are yet to exist is not only contrary to law but also impossible to monitor****....*
>
> "*67. ...Apart from avoidable prolixity and attendant imprecision in the impugned judgment (which a reader may perhaps justifiably complain about this judgment as well) the width of the directions has resulted in what was colourfully described by the US Supreme Court in Reno v American Civil Liberties Union 521 US 244, as — to* ***burn the house to roast the pig*** *- (i.e a disproportionate response, or a remedy worse than the disease)...."*
>
> (emphasis supplied)

61. Google LLC has accordingly expressed reservation against passing of blanket orders, *inter-alia* citing constitutionally guaranteed free speech; and also submitting that content has to be adjudged on a case-by-case basis; and that a blanket-ban on publication even of a particular photograph, or presumptively and pre-emptively banning content, without considering the accompanying context and without adjudicating whether in a given instance publication of the content is liable to be restrained, would be contrary to law.

62. In conclusion, Google LLC has suggested that to make orders issued by this court effective, the following directions may be passed:

> "*i. At the outset, a direction may be passed to the website hosting the alleged content to remove/disable access to the URL of the impugned content. Once the impugned content is removed from the actual websites, the same will be organically removed from the search engines.*
>
> *ii. For the purpose of removal from the search engine, the court or an appropriate government agency can, upon holding the content to be unlawful, share the specific URL of the impugned content for the de-listing/cache removal.*"

63. In the opinion of this court, Google LLC's objection to orders of prior restraint or blanket ban of content is wholly unnecessary and misplaced, inasmuch as, far be it from this court to contemplate any prior restraint or blanket ban on free speech or expression; and the only effort in the present proceedings is to effectively implement directions and orders made for removal or de-indexing of content *which has been considered or found to be unlawful* and there is no question of any prior restraint or blanket ban orders being issued, least of all in these proceedings.

64. This court is also conscious that no untenable burden should be cast upon an intermediary; that no order should be made that is impossible of compliance; and that a direction for removal of content must be proportionate so as to achieve *and only achieve* the purpose of removing what has been found by the court to be *ex-facie* offending content.

Submissions of Ministry of Electronics & Information Technology

65. In a Power Point Presentation made before this court by the Ministry of Electronics and Information Technology ('MeitY'), after placing

the statutory provisions including the rules made thereunder, MeitY has made the following suggestions as regards directions that can be passed for removing offending content:

> "*(a) Direct the intermediary social media platforms to remove offending content OR*
>
> *(b) Direct the "appropriate government" or its "agency" ('agency' specifically constituted under any Act or Rules) including the Law enforcement Agency to get it removed OR*
>
> *(c) grant the right to the Petitioner (expressly written in order) to directly approach or send requests through a specific email to all social media platforms/appropriate government/police to seek removal of unlawful content.*"

66. Furthermore, the MeitY has suggested that the petitioner may lodge a complaint before the "Appropriate Government or its Agency or Police" or before the "Grievance Officer" of the online platform.

67. In particular, the following submissions and suggestions made by the Ministry in its presentation require to be noticed :

i. The Ministry says that the 'Online Cyber-Crime Reporting Portal' available at *www.cybercrime.gov.in*, which was primarily intended for reporting pornography/child pornography or gang rape content, has now widened its scope to include all cybercrimes; and that therefore, any aggrieved person can report any unlawful content through this portal as well;

ii. That in a case such as the present one, the provisions of section 66E of the IT Act, which is a penal provision relating to punishment for violation of privacy and Rules 3(2)(b), 3(2)(e),

3(6), and 3(8) of the '2011 Rules' are also attracted; and any aggrieved party can file a complaint for violation of privacy before the jurisdictional law enforcement agency;

iii. That law enforcement agencies have a role in protecting the individual's privacy and, for that reason, the recommendation by the learned *Amicus Curiae* for direct action by courts is *not* what the Legislature intended.

Submissions of Internet Service Providers Association of India

68. Insofar as respondent No. 3, Internet Service Providers Association of India ('ISPAI'), is concerned, Mr. Meet Malhotra, learned senior counsel appearing on behalf of the said association submitted that its members comprise internet service providers who hold licences issued by the Department of Telecommunications ('DoT') operating under the Ministry of Communications of the Government of India. Mr. Malhotra submitted that the ISPAI has no say in the working of individual internet service providers nor does it have any power to compel, order or regulate the functioning of its members, except to encourage them to follow healthy self-regulatory practices.

69. Furthermore, it is submitted that in any case, membership of the ISPAI comprises only about 82 internet service providers out of a total of 1314 internet service providers licensed by the DoT. It is explained that ISPAI's members only provide technological infrastructure and facilitates in the form of internet services to other entities, namely the intermediaries, who use such services to access and place content on the internet. It is submitted that ISPAI members

do not control the content that goes back-and-forth or is shared on the world-wide-web. Learned senior counsel submitted however that ISPAI members are mandated by law to comply with any 'blocking orders' issued by competent governmental authorities or by a court, which they scrupulously do; however, the members cannot regulate content of any intermediary, whether a social media intermediary or otherwise.

70. It is the ISPAI's stand that although 'intermediary' as defined in section 2(w) of the IT Act includes 'internet service providers', ISPAI members comprise only those entities that enable access to the internet but do not control the content hosted on websites or online platforms; and that ISPAI members enjoy the 'safe harbour' provisions contained in section 79(1) of the IT Act, which provides exemption from liability to such internet service providers. It is further submitted that since most websites and online platforms deploy encryption mechanisms using HTTPS (Hypertext Transfer Protocols Secure), it is technically impossible for an internet service provider to block unlawful content at the sub-page level on a website or online platform, which content can only be blocked by the website/ online platform itself; however upon directions received from the competent governmental authorities or a court of law, an internet service provider can certainly comply with instructions to *block the entire* website or online platform. It is further explained that the role of an internet service provider, such as the ISPAI members, is limited to transporting packets containing information from their source to

their destination, based upon the internet protocol address on such packet, and to deliver it to the end user.

71. By way of suggestions for addressing the queries raised in the present case, the ISPAI submitted that to prevent 'mirroring of content' it is necessary to ensure *expeditious global source blocking* at the level of the platform of the content provider/aggregator/intermediary. Accordingly it is the ISPAI's submissions that while it is possible for a member of the ISPAI to block an entire website under directions of the competent authority or a court, it is not possible for an ISPAI member to sift or monitor content or to block content partially, since they merely provide the technological infrastructure, on or through which, a website or online platform functions.

Submissions of Facebook Inc. / Instagram

72. Relying upon short affidavit dated 04.09.2020 filed on behalf of Facebook Inc./respondent No.4, which also owns the social media platform 'Instagram', Mr. Parag Tripathi, learned senior counsel has submitted that Facebook has a robust privacy policy and also adopts global best practices to protect the privacy of its users to permit a safe online experience. He points-out that though it is the petitioner's allegation that her photographs and images were taken from her Facebook/Instagram social media accounts, the petitioner does not claim any relief against Facebook/Instagram. He further submitted that Facebook/Instagram users have various privacy settings available to them, by which they may restrict access to their content and lock their profile so that others cannot view their photographs or posts nor zoom into and download their profile pictures, unless otherwise

permitted by the user. It is submitted that Facebook now also has features called 'Profile Picture Guard' and 'Audience selector', which give even more control to users over their profile pictures and other content available on their social media accounts. It is stated that similar features are also available on the Instagram social media platform.

73. That being said, in the short affidavit filed by them, Facebook submitted that it actively collaborates with other stakeholders for removal of unlawful online content; and complies with the mandate as contained *inter alia* in *Shreya Singhal* (supra). In any case, Mr. Tripathi submitted, that Facebook has in the past, and is also ready and willing in future, to cooperate with an aggrieved party and with law enforcement agencies to remove offending content in accordance with applicable law, and most certainly pursuant to any court order made in that regard.

Discussion and conclusions

74. At the outset what is notable is that on a combined reading of section 1(2), section 75 and section 81 of the IT Act, Parliament has given both extraterritorial jurisdiction and overriding application to the IT Act *provided* the computer, computer system or computer network *involved* are located within India.

75. The architecture of the penal provisions contained in the IT Act is evident from a combined reading of sections 67, 67A and 67B, viz. that section 67 forms the parent provision which makes the publishing or transmitting of 'obscene material' in electronic form an offence.

Section 67A adds further specificity to the generic phrase 'obscene material', and refers to material which contains 'sexually explicit act or conduct' and makes publishing or transmitting of such material a more egregious offence, with enhanced punishment. Section 67B engrafts an even more aggravated form of offence, bringing within its ambit obscene material relating to children; with further enhanced punishment, 'children' being defined as persons who have not yet completed the age of 18 years.

76. Section 2(1)(o) defines 'data' and 2(1)(v) defines 'information', which definitions when read together, essentially cover all forms of electronic material that is processed, stored or generated, in or through, computer systems or computer networks.

77. Most importantly, section 2(1)(w) defines an 'intermediary' as a person who 'receives, stores or transmits' electronic records on behalf of another person or *provides 'any service'* in relation to electronic records. The *definition is inclusive* and *inter-alia* includes within its ambit telecom service providers, network service providers, internet service providers, web-hosting service providers and search engines.

78. As pointed-out by learned *Amicus Curiae* as also by counsel appearing for the State/respondent No. 2, though section 79(1) of the IT Act exempts intermediaries from certain liability under the IT Act, what is noteworthy is that such *exemption is not unqualified or unconditional* and *applies only if the intermediary fulfils certain conditions and obligations*. This is clear from the plain wording of section 79(1), which makes the exemption from liability "subject to the provisions of sub-sections (2) and (3)". Sub-section (2) lays down

the conditionalities and obligations subject to fulfilment of which sub-section (1) *would apply*; and sub-section (3) lays down the conditionalities and obligations subject to which sub-section (1) *would not apply.*

79. Rule 10 of the 2009 Rules mandates a 'Designated Officer', who is to be notified by the Central Government under Rule 3, to immediately initiate action for blocking of any information where an order is passed by a competent court in India, upon receipt of a certified copy of such order, by submitting the order to the Secretary, Department of Information Technology. It is true that the Designated Officer contemplated under Rule 2(c) read with Rule 3 of the 2009 Rules is otherwise notified for purposes of blocking access to information at the instance of the Central Government in the context of section 69A(2) of the IT Act, which relates to matters pertaining to sovereignty and integrity of India, defence of India, security of the State and other similar matters; *but on a plain reading of Rule 10 of the 2009 Rules it is seen that there is no restriction that if an order is made by a competent court for blocking any information, such order must only pertain to matters referred to in section 69A(2)*. The Designated Officer is therefore obliged to initiate action as may be directed by the court *immediately* on receipt of a certified copy of such order. It must be mentioned here, that though the 2021 Rules superseded the 2011 Rules, neither the 2011 Rules nor the 2021 Rules supersede the 2009 Rules.

80. If any doubt was to remain as to the legislative intent behind section 79, that now stands answered and resolved in the 2021 Rules framed

by the Central Government in exercise of its powers of delegated legislation under section 87 of the IT Act, in which rules, apart from sharpening and emphasising the liabilities and obligations upon intermediaries for dealing with offending content, it has been expressly laid down in the newly added Rule 7 of the 2021 Rules that omission by an intermediary to observe the 2021 Rules shall expose it to penal consequences, both under the IT Act and under the IPC. In fact, to emphasise the importance of removing or disabling access to offending content even on voluntary basis, in the Third Proviso to Rule 3(1)(d) the Central Government has provided, that removal of or disablement of access to, offending content by an intermediary *on voluntary basis*, upon actual knowledge or on grievance received by it, *would not amount to* a violation of section 79(2)(a) or (b) of the IT Act on the part of the intermediary, thereby cementing the exemption available to an intermediary, *provided the intermediary otherwise strictly follows the 2021 Rules*.

81. Most importantly, in para 124.3 of *Shreya Singhal* (supra), while striking down section 66A of the IT Act as being unconstitutional *inter alia* on the ground of over-breadth; and holding section 69A and the 2009 Rules as constitutionally valid; and while reading down section 79(3)(b), the Hon'ble Supreme Court has held that an intermediary would lose the exemption from liability that it enjoys under section 79(1) if it does not 'expeditiously remove or disable access to' offending content or material despite receiving 'actual knowledge', which would mean knowledge *inter-alia* by way of a court order or on being notified by the appropriate government or its

agency, which in the present context would mean the concerned police authorities. Furthermore, in *Shreya Singhal* (supra), the Hon'ble Supreme Court has (had) also upheld the 2011 Rules subject to Rule 3(4) being read-down. Though the 2011 Rules have now been superseded by the 2021 Rules, the corresponding provision for Rule 3(4) of the 2011 Rules is now subsumed in Rule 3(1)(d) of the 2021 Rules.

82. Upon a composite reading of section 79(2) and (3), the conditionalities and obligations subject to which an intermediary enjoys exemption from liability under the IT Act, may be summarized as under :

(a) The exemption applies only if the function of the intermediary is *limited* to providing access to a communication system over which information is transmitted, temporarily stored or hosted;

(b) The exemption applies only if the intermediary *does not initiate* the transmission *nor selects* the receiver of the transmission *nor selects or modifies* the information contained in the transmission;

(c) The exemption applies only if the intermediary *observes due diligence* while discharging its duties under the IT Act and *observes all other guidelines* prescribed by the Central Government in relation to its duties;

(d) The exemption is *not* available if the intermediary has *conspired, abetted or induced* the commission of an unlawful act;

(e) Most importantly, the exemption is ***not available if the intermediary fails to expeditiously remove or disable access to material upon receiving actual knowledge or being notified by the appropriate government or its agencies*** that any information/data/communication link residing in or connected to a computer resource *controlled* by that intermediary is being used to commit an unlawful act.

83. Clearly therefore, if the intermediary fails to fulfil the conditionalities and obligations cast upon it, both in the positive and in the negative, as set-out above, such intermediary is liable to forfeit the exemption from liability available to it under section 79(1) of the IT Act.

84. Section 85 of the IT Act, while dealing with *contraventions* of the IT Act or rules committed by companies, also makes the directors, manager, secretary or other officer of a company also liable if *inter alia* the *contravention* has been committed by reason of neglect attributable to such person. It is to be noted that what is brought within the provision is *any contravention* of *any provision* of the IT Act or any rules made thereunder.

85. In the present case, the petitioner's photographs and images, though not in themselves obscene or offensive, were taken from her Facebook and Instagram accounts without her consent and were uploaded on a pornographic website, adding derogatory captions to them. It is an irrefutable proposition that if the name and/or likeness of a person appears on a pornographic website, as in the present case, without the the consent or concurrence of such person, such act would by and in itself amount to an offence *inter-alia* under section 67 of the

IT Act. This is so since section 67 makes it an offence to publish or transmit, or causes to be published or transmitted, in the electronic form, *any material which appeals to the prurient interests* of those who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. The only purpose of posting the petitioner's photograph on a pornographic website could be to use it to appeal to the prurient interests of those who are likely to see it. That apart, the inclusion of the name and/or likeness of a person on such website, even if the photograph of the person is not in itself obscene or offensive, without consent or concurrence, would at the very least amount to breach of the person's privacy, which a court may, in appropriate cases, injunct or restrain. It is is evident that such publication would likely result in ostracisation and stigmatisation of the person concerned in society; and therefore *immediate* and *efficacious* remedy is required in such cases.

86. While appreciating the indisputably anarchic nature of the internet as a medium and accepting that the world-wide-web is intractable by reason of its global expanse, interconnectedness and the fact that content, including offending content, can be very easily placed on the world-wide-web by people from the farthest corners of the world, which it is almost impossible to control, it cannot be ignored that the law and judicial opinion in India as also in several other jurisdictions, as gathered from the foregoing discussion, mandates intermediaries to remove and disable access to offending content once they receive 'actual knowledge' by way of a court order or upon being notified by the appropriate government or its agency, failing which the

intermediary is liable to lose the exemption from liability available to it under section 79(1) of the IT Act.

87. In the first instance therefore, an intermediary cannot be heard to say that it is *unable* to remove or disable access to offending content despite such actual knowledge as contemplated in law. That being said however, this court cannot ignore the difficulties expressed by the intermediaries in the present case, in identifying and removing offending content, which intermediaries, this court thinks, effectively represent the perspective and point-of-view of several other intermediaries who are similarly placed.

88. To be fair, none of the respondent intermediaries has at all taken a stand before this court that they are *not* ready or willing to remove offending content if directed by a court order or by an appropriate governmental agency. The intermediaries have only said that it *may not be possible* to identify the offending content appearing in various disguises and corrupted *avatars*; and further that, it would be too onerous and impractical to place upon them the responsibility to keep on a lookout for offending content re-surfacing in the various different disguises and corrupted *avatars* at the instance of mischief-makers, on a continuing basis.

89. In the opinion of this court, for an order directing the removal or access disablement of offending content to be effective even within India, *a search engine must block the search results throughout the world* since no purpose would be served by issuing such an order if it has no realistic prospect of preventing irreparable harm to a litigant. To borrow the words of the Hon'ble Supreme Court of Canada in

Google Inc. v. Equustek Solutions Inc. et al. (supra), as also observed by others courts in other jurisdictions, the de-indexing of offending content globally does not require the search engine to " .... take any steps around the world, it requires it to take steps only where its search engine is controlled. This is something Google has acknowledged it can do and does with relative ease. There is therefore no harm to Google which can be placed on its "inconvenience" scale arising from the global reach of the order ... " It is also to be noted that search engines are already employing requisite automated tools to prevent generating links to child pornography and hate speech, which tools can equally well be used in making a court order, such as the one in the present case, implementable and effective. None of this would impose upon the website, online platform or search engine(s) any obligation to generally monitor content or to adjudicate the illegitimacy of any content or operate as a prior restraint or a blanket ban or censorship of content generally.

Suggested template directions that should ordinarily be issued and the parties to whom these should be issued :

90. On an overall appreciation of the legal and practical aspects of the matter, and to answer the queries framed in para 11 of this judgment, in the opinion of this court, a fair balance between the obligations and liabilities of the intermediaries and the rights and interests of the aggrieved user/victim would be struck by issuing directions as detailed below, which would be legal, implementable, effective and would enable meaningful compliance of the orders of a court without putting any impossible or untenable burden on intermediaries.

(i) Based on a 'grievance' brought before it, as contemplated in Rule 2(1)(j) of the 2021 Rules *or otherwise*, and upon a court being satisfied in any proceedings before it, whether at the interim or final stage, that such grievance requires immediate redressal, the court may issue a direction to the *website or online platform* on which the offending content is hosted*, to remove* such content from the website or online platform, forthwith and in any event within 24 hours of receipt of the court order. Since this timeframe is mandated in Rule 3(2)(b) of the 2021 Rules read with Rule 10 of the 2009 Rules for other *similar* kinds of offensive content, in the opinion of this court, the same timeframe ought to be applied if the court is satisfied that *any* offending content requires immediate removal;

(ii) A direction should also be issued *to the website or online platform* on which the offending content is hosted to *preserve all information and associated records* relating to the offending content*,* so that evidence in relation to the offending content is not vitiated, at least for a period of 180 days or such longer period as the court may direct, for use in investigation, in line with Rule 3(1)(g) of the 2021 Rules;

(iii) A direction should also be issued by the court *to the search engine(s)* as the court may deem appropriate, *to make the offending content non-searchable by 'de-indexing' and 'de-referencing'* the offending content in their listed search results, including de-indexing and de-referencing all concerned web-pages, sub-pages or sub-directories on which the offending

content is found. For reference, some of the most commonly used search engines in India are *Google Search, Yahoo Search, Microsoft Bing and DuckDuckGo*. This would be in line with the obligation of search engines to disable access to the offending content under the Second Proviso to Rule 3(1)(d) of the 2021 Rules. It is necessary to point-out that in the Second Proviso to Rule 3(1)(d), which deals with due diligence required by an intermediary, the time frame set-down *inter alia* for disabling access to offending content is "… as early as possible, but in no case later than *thirty-six hours* from the receipt of the court order …"; but under the grievance redressal mechanism engrafted in Rule 3(2)(b), the intermediary has been mandated to remove certain specified kinds of offending content within *twenty-four hours* from receipt of a complaint from any person. In the opinion of this court, the intermediary must be obliged to comply with a court order directing removal or disabling access to offending content within *twenty-four hours* from receipt of such order;

(iv) The directions issued must also mandate the concerned intermediaries, whether websites/online platforms/search engine(s), *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, as contemplated in Rule 4(1)(d) of the 2021 Rules;

(v) Directions should also be issued to the *concerned law enforcement agency/ies*, such as the jurisdictional police, to obtain from the concerned website or online platform all information and associated records, including all unique identifiers relating to the offending content such as the URL (Uniform Resource Locator), account ID, handle name, Internet Protocol address and hash value of the actual offending content alongwith the metadata, subscriber information, access logs and such other information as the law enforcement agency may require, in line with Rule 3(1)(j) of the 2021 Rules, as soon as possible but not later than seventy-two hours of receipt of written intimation in this behalf by the law enforcement agency;

(vi) Also, the court must direct the aggrieved party to furnish to the law enforcement agency *all available information* that the aggrieved party possesses relating to the offending content, such as its *file name, Image URL, Web URL* and other available identifying elements of the offending content, as may be applicable; with a further *direction to the law enforcement agency* to furnish such information to all other entities such as websites/online platforms/search engines to whom directions are issued by the court in the case;

(vii) The aggrieved party should also be permitted, on the strength of the court order passed regarding specific offending content, to notify the law enforcement agency to remove the offending content from *any other* website, online platform or search

engine(s) on which *same or similar offending content* is found to be appearing, *whether in the same or in a different context.* Upon such notification by the aggrieved party, the law enforcement agency *shall* notify the concerned website, online platform and search engine(s), who (latter) *would be obligated to comply with such request*; and, if there is any technological difficulty or other objection to so comply, the website, online platform or search engine(s) may approach the concerned court which passed the order, seeking clarification *but only after first complying* with the request made by the aggrieved party. This would adequately address the difficulty expressed by Google LLC in these proceedings that a search engine is unable to appreciate the offending nature of content appearing in a different context. In this regard attention must be paid to Rule 4(8) of the 2021 Rules which contemplates that an intermediary may entertain a 'request for the reinstatement' of content that it may have voluntarily removed; whereby the 2021 Rules now specifically provide that offending content *may be removed in the first instance*, giving to any interested person as specified in Rule 4(8) the liberty to object to such removal and to request for reinstatement of the removed content. This has been provided in the rules since, evidently, it *affords a more fair and just balance* between the irreparable harm that may be caused by retaining offending content on the world-wide-web *and* the right of another person to seek reinstatement of the content by challenging its removal;

(viii) The court may also direct the aggrieved party to make a complaint on the *National Cyber-Crime Reporting Portal* (if not already done so), to initiate the process provided for grievance redressal on that portal;

(ix) Most importantly, the court must refer to the provisions of section 79(3)(a) and (b) read with section 85 of the IT Act and Rule 7 of the 2021 Rules, whereby an ***intermediary would forfeit the exemption from liability*** enjoyed by it under the law if it were to fail to observe its obligations for removal/access disablement of offending content despite a court order to that effect.

91. Lest it be thought that the exercise done by this court in the present matter was needless, this court would like to record that what impelled it to undertake this somewhat prolix and painstaking exercise, is that the *integrity of the court process has to be protected* in the most effective way, the anarchical nature of the internet notwithstanding. *It cannot be overemphasised that even if, given the nature of the internet, offending content cannot be completely 'removed' from the world-wide-web, offending content can be made unavailable and inaccessible by making such content 'non-searchable' by de-indexing and de-referencing it from the search results of the most widely used search engines, thereby serving the essential purpose of a court order almost completely*. In the opinion of this court, the directions issued by a court seized of a case such as the present one, must be *specific*, *pointed* and *issued to all necessary parties*, so as to ensure that the purpose sought to be achieved by the

court is fulfilled and that the directions and orders issued are not merely on paper or purposeless.

Directions in this matter :

92. In line with the above suggested template of directions, in the present case this court is satisfied that the action of the petitioner's photographs and images having been taken from her Facebook and Instagram accounts and having been posted on the website *www.xhamster.com*; and then having been re-posted onto other websites and online platforms, amounts *prima facie* to an offence under section 67 of the IT Act in addition to other offences under the IPC; and that appropriate directions are required to be issued directing the State and other respondents to *forthwith* remove and/or disable access to the offending content from the world-wide-web to the maximum extent possible. Accordingly the following directions are issued :

(i) The petitioner is directed to furnish in writing to the Investigating Officer of the subject FIR, all available information relating to the offending content, including the Image URL and Web URL pertaining to the offending image files, within 24 hours of receipt of a copy of this judgment, if not already done so;

(ii) The Delhi Police/CyPAD Cell are directed to remove/disable access to the offending content, the Web URL and Image URL of which would be furnished by the petitioner as above, *from all websites and online platforms*, *forthwith* and in any event

within 24 hours of receipt of information from the petitioner. It may be recorded that the Delhi Police have stated before this court that the offending content has already been removed from respondent No. 5 website *www.xhamster.com*;

(iii) A direction is issued to the search engines *Google Search*, *Yahoo Search*, *Microsoft Bing and DuckDuckGo*, to *globally* de-index and de-reference from their search results the offending content as identified by its Web URL and Image URL, including de-indexing and de-referencing all concerned web-pages, sub-pages or sub-directories on which the offending content is found, *forthwith* and in any event within 24 hours of receipt of a copy of this judgment alongwith requisite information from the Investigating Officer as directed below;

(iv) A further direction is issued to the search engines *Google Search*, *Yahoo Search*, *Microsoft Bing*, *DuckDuckGo*, to endeavour to use automated tools, to proactively identify and globally disable access to any content which is *exactly identical* to the offending content, that may appear on *any other websites/online platforms*;

(v) The Investigating Officer is directed to furnish in writing the Web URL and Image URL of the offending content to the other entities to whom directions have been issued by this court in the present matter, alongwith a copy of this judgment, within 24 hours of receipt of such copy;

(vi) The Delhi Police are directed to obtain from the concerned website, namely *www.xhamster.com* and from the search

engines *Google Search*, *Yahoo Search*, *Microsoft Bing*, *DuckDuckGo* (and any other search engines as may be possible) all information and associated records relating to the offending content such as the URL, account ID, handle name, Internal Protocol Address, hash value and other such information as may be necessary, for investigation of case FIR No. 286/2020 dated 18.07.2020 registered under section 354A IPC and 66C IT Act at P.S.: Dwarka South, *forthwith* and in any event within 72 hours of receipt of a copy of this judgment, if not already done so;

(vii) Furthermore, the petitioner is granted liberty to issue written communication to the Investigating Officer for removal/access disablement of the *same or similar* offending content appearing on *any other* website/online platform or search engine(s), *whether in the same or in different context*; with a corresponding direction to the Investigating Officer to notify such website/online platform or search engine(s) to comply with such request, immediately and in any event within 72 hours of receiving such written communication from the petitioner;

(viii) Notwithstanding the disposal of the present petition by this order, if any website, online platform, search engine(s) or law enforcement agency has any doubt or grievance as regards compliance of any request made by petitioner as aforesaid, such entity shall be at liberty to approach this court to seek clarification in that behalf.

93. It is made clear that non-compliance with the foregoing directions would make the non-compliant party liable to forfeit the exemption, if any, available to it generally under section 79(1) of the IT Act and as specified by Rule 7 of the 2021 Rules; and shall make such entity and its officers liable for action as mandated by section 85 of the IT Act.

94. In view of the directions issued hereinabove, no further orders are called for in the present petition, which is accordingly disposed of.

95. Other pending applications, if any, also stand disposed of.

96. This court records its deep appreciation for the invaluable assistance rendered in the matter by the learned *Amicus Curiae* Dr. Pavan Duggal.

97. A copy of this judgment be communicated to counsel for the petitioner and counsel for all the named respondents, as per the amended memo of parties immediately *via* e-mail, for compliance by the concerned parties.

ANUP JAIRAM BHAMBHANI, J.

April 20, 2021
j/Ne/*uj*