

IN THE HIGH COURT OF DELHI AT NEW DELHI
(*Ordinary Original Jurisdiction*)

C.S.(OS) NO. OF 2021

IN THE MATTER OF:

X ...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

INDEX - I
(PLAINT)

Sr. No.	Particulars	Page No.
1.	Index – I (Plaint)	1 – 2
2.	Suit Format	3 – 4
3.	Urgent Application	5
4.	Synopsis and List of Dates	6 – 8
5.	Memo of Parties	9 – 21
6.	Plaint	22 – 41
7.	Affidavit in Support	42 – 43
8.	Affidavit on behalf of the Plaintiff, under Section 65-B, Indian Evidence Act, 1872	44 – 47
9.	Statement Certifying Authenticity of Documents filed with the plaint	48 – 49
10.	List of Reliance	50
11.	Court fee for plaint and one time PF Rs. 236520/-	51

INDEX - II
(INTERIM APPLICATIONS)

Sr. No.	Particulars	Page No.
1.	Index - II (Interim Applications)	1 - 2
2.	Plaintiff's Application under Order 39 Rule 1 & 2 read with Section 151 of Code of Civil Procedure, 1908, along with affidavit in support.	3 - 19
3.	Plaintiff's Application under Section 151 of CPC seeking confidentiality of the proceedings along with affidavit in support.	20 - 26
4.	Plaintiff's Application under Section 151 of Code of Civil Procedure, 1908, along with affidavit in support, for exemption from filing original copies and fair typed copies of original documents along with affidavit in support.	27 - 31
5.	Application under section 80(2) of the code of civil procedure, 1908 along with affidavit in support.	32 - 36

INDEX - III
(VAKALATNAMA)

Sr. No.	Particulars	Page No.
1.	Index III (Vakalatnama)	1
2.	Vakalatnama	2 - 3
3.	Proof of Service along with Affidavit	4 - 7

INDEX - IV
(LIST OF DOCUMENTS)

Sl. No.	Details of Documents and Parties	In the Possession/Pow	Original/ Photocopy/Office	Mode of execution/Issuance of Receipt	Line of Custody	Page No.
----------------	---	------------------------------	-----------------------------------	--	------------------------	-----------------

		er/Custo dy of:	Copy/ Printout			
1.	INDEX IV (Documents)					1 - 3
2.	Print out of list of URLs	Plaintif f	Print out	Printout of URL links	Plaintiff to Plaintiff' s counsel	4 - 6
3.	Screenshots of Plaintiff's conversation with Ram Gopal Verma	Plaintif f	Printou t	Download ed from Plaintiff's phone and printed	Plaintiff to Plaintiff' s counsel	7 - 11
4.	Order of the Delhi High Court in <i>Jorawer Singh Mundy v. Union of India and Ors.</i> , 2021 SCC Online Del 2306	Plaintif f's Counse l	Printou t	Printed from Court website	Plaintiff' s counsel	12 - 13
5.	Order of the Delhi High Court in <i>Zulfiqar Ahman Khan v. Quintillion Business Media Pvt Ltd and Ors.</i> , 2019 SCC Online Del 8494	Plaintif f's Counse l	Printou t	Printed from Court website	Plaintiff' s counsel	14 - 16
6.	Order of the Odisha High Court in <i>Subhranshu Rout v. State of Odisha</i> , 2020 SCC Online Ori 878	Plaintif f's Counse l	Printou t	Printed from Court website	Plaintiff' s counsel	17 - 24
7.	Order of Karnataka High Court in <i>Vasunathan v. Registrar General</i> ,	Plaintif f's Counse l	Printou t	Printed from Court website	Plaintiff' s counsel	25 - 26

IN THE HIGH COURT OF DELHI AT NEW DELHI
(*Ordinary Original Jurisdiction*)

C.S.(OS) NO. OF 2021

IN THE MATTER OF:

X ...Plaintiff

Versus

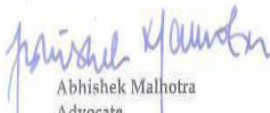
<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

INDEX - I
(PLAINT)

Sr. No.	Particulars	Page No.
1.	Index – I (Plaint)	1 – 2
2.	Suit Format	3 – 4
3.	Urgent Application	5
4.	Synopsis and List of Dates	6 – 8
5.	Memo of Parties	9 – 21
6.	Plaint	22 – 41
7.	Affidavit in Support	42 – 43
8.	Affidavit on behalf of the Plaintiff, under Section 65-B, Indian Evidence Act, 1872	44 – 47
9.	Statement Certifying Authenticity of Documents filed with the plaint	48 – 49
10.	List of Reliance	50
11.	Court fee for plaint and one time PF Rs. 236520/-	51

THROUGH



Abhishek Malhotra
Advocate

Abhishek Malhotra

TMT Law Practice

Counsel for the Plaintiff

C-2/39, Lower Ground Floor,

Safdarjung Development Area,

New Delhi - 110016

E-mail: amalhotra@tmtlaw.co.in

Phone# 9971053888, 9899597359

Place: New Delhi

Dated: August 16, 2021

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)
CS (OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

ADVOCATES

THROUGH

Mr. Abhishek Malhotra _____
 Counsel for the Plaintiff _____
 TMT Law Practice _____
 C-2/39, Lower Ground Floor
 Safdarjung Development Area
 New Delhi – 110 016 _____

PLAINTIFF

DEFENDANTS

INTERLOCUTORY APPLICATIONS (IAS)

S. No.	Year	Filed By	Provisions and Law	Nature of Relief Sought	Remarks
1.	2021	Plaintiff	Order 39, Rules 1 and 2, r/w Section 151, CPC, 1908	Interim Injunction	1
2.	2021	Plaintiff	Section 151, CPC, 1908	Application for protecting the Plaintiff's identity and keeping	1

				confidential the documents and pleadings in the present proceeding	
3.	2021	Plaintiff	Section 151, CPC, 1908	Exemption from filing original and fair typed copies	1
4.	2021	Plaintiff	Section 80 (2), CPC	Exemption from prior service on Department of Telecommunications and Ministry of Electronics and, Information Technology, both being governmental bodies	1

THROUGH



Abhishek Malhotra
Advocate

Abhishek Malhotra
TMT Law Practice
(Counsels for the Plaintiff)
C-2/39, Lower Ground Floor,
Safdarjung Development Area
New Delhi – 110 016

Place: New Delhi

Dated: August 16, 2021

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)

CS (OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

URGENT APPLICATION

To,
 The Registrar,
 Delhi High Court,
 New Delhi.

Sir,

Please treat the accompanying Application as an urgent one on the basis of High Court Orders and Rules. The cause of urgency is the urgent nature of relief sought.

Kindly list on August , 2021.

THROUGH


 Abhishek Malhotra
 Advocate

Abhishek Malhotra
 TMT Law Practice
 (Counsels for the Plaintiff)
 C-2/39, Lower Ground Floor,
 Safdarjung Development Area
 New Delhi - 110 016

Place: New Delhi
 Dated: August 16, 2020

SYNOPSIS

1. The present Suit is being filed seeking, *inter alia*, an order of permanent and mandatory injunction against the Defendants, directing them to remove the identified audio-visual content that form the subject matter of the suit (**Suit Video/s**) and refrain from hosting or uploading the said videos on any digital or other platform.
2. The Plaintiff, in her earlier avatar, worked extensively in Bengali movies and television shows as well as several ad films and music videos. Since 2017, the Plaintiff has created a distinctive identity and garnered reputation amongst viewers. The Suit Videos, however, are of a nature and carry content that shows the Plaintiff in poor light and are being made available/ communicated to the public without the Plaintiff's permission or consent and are being used by unknown third parties to blackmail the Plaintiff as also to hurt the reputation meticulously created by the Plaintiff over the years.
3. To protect the identity of the Plaintiff, the Plaintiff has been anonymously named and referred to as 'X' in the present proceedings.
4. The Plaintiff recorded the Suit Videos as a part of a proposed web series which was to be shot and themed on Mumbai Mafia in India and the internal conflicts amongst the members of organised crimes/ underworld in Mumbai (**Series**). It is pertinent to note that the Series was never produced as the project was shelved.
5. The Plaintiff submits that the Suit Videos have surfaced on multiple digital platforms and websites comprising explicit scenes of complete, frontal nudity of the Plaintiff. The Suit Videos have also been hosted on

several websites communicating to the public, obscene and pornographic content. Further, in the absence of any authorization, inter alia, from the Plaintiff, the Suit Videos could not have been uploaded on any platform including but not limited to the Defendant websites.

6. The present suit is against the Defendants, seeking a take down of the Suit Videos and restraint order against the Defendants from hosting the Suit Videos. The present case is an exercise of Plaintiff's 'right to be forgotten' and 'right to be left alone' which have been recognised as an inseparable and inherent aspects of right to privacy by the Supreme Court and multiple High Courts.
7. Hence, the present Suit.

LIST OF DATES

2017	<p>Plaintiff was engaged by Mr Ram Gopal Verma, owner of Ram Gopal Verma Studios for filming of a web series. The Plaintiff was promised lead role in the Series and on that pretext, was lured into participating in a demonstration video (Suit Videos).</p> <p>However, the Series was never produced as the project was shelved. In the absence of any contract, the short videos recorded for the Series could not be utilised in any manner neither by Ram Gopal Verma Studios nor any of the other Defendants herein.</p>
December 2020	<p>Plaintiff came to know that the video clips shot by Ram Gopal Verma Studios had been uploaded by</p>

	Mr Ram Gopal Verma on his YouTube channel/ the channel under the control of Ram Gopal Verma Studios and on the Studio's website.
December 2020	Plaintiff immediately reached out to Mr Ram Gopal Verma, requesting the latter to remove the Suit Videos uploaded on the Youtube channel as well as the website. Mr Ram Gopal Verma intimated the Plaintiff that he would render all assistance and cooperate in removal of the Suit Videos uploaded by him/Ram Gopal Verma Studios on Youtube and the website.
December 2020- January 2021	Plaintiff gained knowledge of the fact that the Suit Videos have been uploaded on several digital platforms and websites including that of the Defendant URLs/ websites.
June 2021	Plaintiff started receiving anonymous threats from individuals who threatened to disrepute and tarnish the reputation of the Plaintiff by publicising the Suit Videos and who also sought to extort money from the Plaintiff on the above pretext.
August 2021	Hence, the present Suit seeking mandatory and permanent injunctions and interim injunctions against the Defendants for take down of the videos and restraining them or the mirrored websites or the unknown defendants from hosting the Suit Videos.

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)
CS (OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

MEMO OF PARTIES

X

xx

xx

xx

Email: amalhotra@tmtlaw.co.in

Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0>

Defendant No. 1

+1 2083895770

Domain ID -

142504053_DOMAIN_COM-VRSN

Email: abusecomplaints@markmonitor.com

<https://www.youtube.com/watch?v=kLf5itQEC0M>

Defendant No. 2

+1 2083895770

Domain ID -

142504053_DOMAIN_COM-VRSN

Email: abusecomplaints@markmonitor.com

<https://www.youtube.com/watch?v=TYez5HliIkk>

Defendant No. 3

+1 2083895770

Domain ID -

142504053_DOMAIN_COM-VRSN

Email: abusecomplaints@markmonitor.com

https://www.youtube.com/watch?v=bJ2gZA9MLr4 +1 2083895770 Domain ID - 142504053_DOMAIN_COM-VRSN Email: abusecomplaints@markmonitor.com	Defendant no. 4
https://www.youtube.com/watch?v=8SNkrCM03B8 +1 2083895770 Domain ID - 142504053_DOMAIN_COM-VRSN Email: abusecomplaints@markmonitor.com	Defendant No. 5
https://www.youtube.com/watch?v=H4BFZb2pBFk +1 2083895770 Domain ID - 142504053_DOMAIN_COM-VRSN Email: abusecomplaints@markmonitor.com	Defendant No. 6
https://www.youtube.com/watch?v=vKH2UKGGrA +1 2083895770 Domain ID - 142504053_DOMAIN_COM-VRSN Email: abusecomplaints@markmonitor.com	Defendant No. 7
https://www.youtube.com/watch?v=sp8IsH2DK08 +1 2083895770 Domain ID - 142504053_DOMAIN_COM-VRSN Email: abusecomplaints@markmonitor.com	Defendant No. 8
https://www.youtube.com/watch?v=oiqvbrRf_B4 +1 2083895770 Domain ID - 142504053_DOMAIN_COM-VRSN Email: abusecomplaints@markmonitor.com	Defendant No. 9
https://www.google.com/imgres?imgurl=https%3A%2F%2Fpbs.twimg.com%2Fmedia%2FCJXnIzLUAAAcLOX.jpg&imgrefurl=https%3A%2F%2Ftwitter.com%2Fonlinetollywood%2Fstatus%2F618654668130922497&tbid=6-rlvu PeiWa_M&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygCegQIARBa..i&docid=CsunT4DbPekRtM&w=594&h=402&q=tilottama%20dutta&hl=en&aut	Defendant No. 10

**huser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeB
DVYQMygCegQIARBa**

+1 2083895770

Domain ID -

2138514_DOMAIN_COM-VRSN

Email: abusecomplaints@markmonitor.com

https://www.google.com/imgres?imgurl=https%3A%2F%2Flookaside.fbsbx.com%2Flookaside%2Fcrawler%2Fmedia%2F%3Fmedia_id%3D935461176518216&imgrefurl=https%3A%2F%2Fwww.facebook.com%2FTilottama-Dutta-

143633788665570%2Flikes&tbnid=vKF_4yBFrP9O-M&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygBegQIARBY..i&docid=TS6VMycLrRJTBM&w=960&h=640&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygBegQIARBY

+1 2083895770

Domain ID -

2138514_DOMAIN_COM-VRSN

Email: abusecomplaints@markmonitor.com

Defendant No. 11

https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.shorshe.com%2Fcelebrity%2Fposter%2F3%2F9%2F3981.jpg&imgrefurl=https%3A%2F%2Fwww.shorshe.com%2Fcelebrity%2FTilottama-dutta-tilottama-dutta.html&tbnid=HTZQOWM8iP2nzM&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygEegQIARBe..i&docid=e1GODwrjsaZPGM&w=150&h=231&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygEegQIARBe

+1 2083895770

Domain ID -

2138514_DOMAIN_COM-VRSN

Email: abusecomplaints@markmonitor.com

Defendant No. 12

https://www.google.com/imgres?imgurl=https%3A%2F%2Flookaside.fbsbx.com%2Flookaside%2Fcrawler%2Fmedia%2F%3Fmedia_id%3D143633788665570&imgrefurl=https%3A%2F%2Fm.facebook.com%2FTilottama-Dutta-

143633788665570%2F&tbnid=i4qL3SKJNFoXhM&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygDegQIARBe..i&docid=XmtyWGpHYgolfM&w=724&h=

Defendant No. 13

724&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygDegQIARBc

+1 2083895770

Domain ID -

2138514_DOMAIN_COM-VRSN

Email: abusecomplaints@markmonitor.com

[https://www.google.com/imgres?imgurl=https%3A%2F%2Flookaside.fbsbx.com%2Flookaside%2Fcrawler%2Fmedia%2F%3Fmedia_id%3D944938218903845&imgrefurl=https%3A%2F%2Fwww.facebook.com%2FTilottama-Dutta-](https://www.google.com/imgres?imgurl=https%3A%2F%2Flookaside.fbsbx.com%2Flookaside%2Fcrawler%2Fmedia%2F%3Fmedia_id%3D944938218903845&imgrefurl=https%3A%2F%2Fwww.facebook.com%2FTilottama-Dutta-1436337886665570%2Flikes&tbnid=Y64k3Y9c9Ew9YM&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygJegQIARBq..i&docid=TS6VMycLrRJTBM&w=1800&h=1200&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygJegQIARBq)

Defendant No. 14

[1436337886665570%2Flikes&tbnid=Y64k3Y9c9Ew9YM&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygJegQIARBq..i&docid=TS6VMycLrRJTBM&w=1800&h=1200&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygJegQIARBq](https://www.google.com/imgres?imgurl=https%3A%2F%2Flookaside.fbsbx.com%2Flookaside%2Fcrawler%2Fmedia%2F%3Fmedia_id%3D944938218903845&imgrefurl=https%3A%2F%2Fwww.facebook.com%2FTilottama-Dutta-1436337886665570%2Flikes&tbnid=Y64k3Y9c9Ew9YM&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygJegQIARBq..i&docid=TS6VMycLrRJTBM&w=1800&h=1200&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygJegQIARBq)

+1 2083895770

Domain ID -

2138514_DOMAIN_COM-VRSN

Email: abusecomplaints@markmonitor.com

<https://mypornsnap.top/photos/tilottama-dutta>

Defendant No. 15

+86 6502620100

Domain ID -

D20190416G10001G_07246130-top

Email: abuse@dynadot.com

<https://mypornsnap.top/photos/1/tilottama-dutta/hqdefault-jpg>

Defendant No. 16

+86 6502620100

Domain ID -

D20190416G10001G_07246130-top

Email: abuse@dynadot.com

<https://mypornsnap.top/photos/2/tilottama-dutta/3981-jpg>

Defendant No. 17

+86 6502620100

Domain ID -

D20190416G10001G_07246130-top

Email: abuse@dynadot.com

https://mypornsnap.top/photos/3/tilottama-dutta/cjxnizluaaaclox-jpg +86 6502620100 Domain ID - D20190416G10001G_07246130-top Email: abuse@dynadot.com	Defendant No. 18
https://mypornsnap.top/photos/5/tilottama-dutta/maxresdefault-jpg +86 6502620100 Domain ID - D20190416G10001G_07246130-top Email: abuse@dynadot.com	Defendant No. 19
https://mypornsnap.top/photos/16/tilottama-dutta/hqdefault-jpg +86 6502620100 Domain ID - D20190416G10001G_07246130-top Email: abuse@dynadot.com	Defendant No. 20
https://www.fap.plus/content/indian-actress-tilottama-dutta-naked-in-guns-and-thighs-nsfw/1957912.shtml +1 6613102107 Domain ID - e82ef8e9d5f0429da44e50e7474fabef-DONUTS Email: abuse@namecheap.com	Defendant No. 21
https://xnxx.plus/ja/mov/indian-actress-tilottama-dutta-naked-in-guns-and-thighs-nsfw/109243.html +1 6613102107 Domain ID - 46c9b34388d949138bfab746ff2ab0c0-DONUTS Email: abuse@namecheap.com	Defendant No. 22
https://mobileporn4u.com/video/59922-indian-actress-tilottama-dutta-naked-in-guns-and-thighs-nsfw/ +1 6613102107 Domain ID - 2586868293_DOMAIN_COM-VRSN Email: abuse@namecheap.com	Defendant No. 23
https://mobileporn4u.com/video/59923-indian-actress-tilottama-dutta-naked-in-guns-and-thighs-nsfw/	Defendant No. 24

+1 6613102107
 Domain ID –
 2586868293_DOMAIN_COM-VRSN
 Email: abuse@namecheap.com

https://daftsex.com/watch/-107646916_456248758 Defendant No. 25
+1 6613102107

Domain ID –
 1939823170_DOMAIN_COM-VRSN
 Email: abuse@namecheap.com

<https://hugetits.win/video/ViciousAmazingAfricanaugurbuzzard/> Defendant No. 26

+1 6613102107
 Domain ID –
 D2213454-WIN
 Email: abuse@namecheap.com

<https://www.reddit.tube/video/ff3554de124e31b7149f0cb750ae36db2c20d5a> Defendant No. 27

+1 6613102107
 Domain ID –
 D3C3D1955E9B84738AAE8637CC5AB89EC-NSR
 Email: abuse@namecheap.com

<https://greygif.com/tilotama-dutta-in-guns-amp-thighs> Defendant No. 28

+357 95713635
 IP Address–
 172.67.218.70 ; 104.21.45.190
 Email: abuse@danescenames.com

<https://pinkgif.com/tilotama-dutta-in-guns-amp-thighs> Defendant No. 29

+357 95713635
 Domain ID –
 2520560350_DOMAIN_COM-VRSN
 Email: abuse@danescenames.com

<https://xxxpornxvideos.com/xxxvid/ViciousAmazingAfricanaugurbuzzard/> Defendant No. 30

+357 95713635
 IP Address–
 104.21.15.18. ; 172.67.161.6

Email: abuse@danescenames.com

<https://celegif.com/tilotama-dutta/>

Defendant No. 31

+357 95713635

IP Address-

104.21.6.212; 172.67.135.73

Email: abuse@danescenames.com

<https://adultseries.net/videos/tilotama-dutta-nude-guns-thighs-s01-trailer-2017/>

Defendant No. 32

+357 95713635

IP Address-

188.164.249.69

Email: abuse@danescenames.com

<https://xxxdata.net/vid/ViciousAmazingAfricanaugurbuzzard/>

Defendant No. 33

+1 5163015301

Domain ID -

1930683989_DOMAIN_NET-VRSN

Email: abuse@tldregistrarsolutions.com

<https://twitter.com/onlinetollywood/status/618654668130922497>

Defendant No. 34

+1 8887802723

Domain ID -

18195971_DOMAIN_COM-VRSN

Email: domainabuse@cscglobal.com

<https://www.shorshe.com/celebrity/tilottama-dutta-tilottoma-dutta.html>

Defendant No. 35

+1 8003337680

Domain ID -

1741815023_DOMAIN_COM-VRSN

Email: abuse@web.com

<https://www.dailymotion.com/video/x68p5fa>

Defendant No. 36

+33 241182828

Domain ID -

146399472_DOMAIN_COM-VRSN

Email: abuse@nameshield.net

Reliance Communications Infrastructure Limited

Defendant No. 37

H Block, 1st Floor, Dhirubhai Ambani Knowledge City,
Navi Mumbai

Mh 400710

Email: mca.rocfileing@relianceada.com

Reliance Jio Infocomm Limited

9th Floor, Maker Chambers IV, 222, Nariman Point,
Mumbai MH 400021

Email: Neelakantan.An@ril.com; jyoti.jain@ril.com

Defendant No. 38

Sify Technologies Limited

Tidel Park, 2nd Floor, No.4, Canal Bank Road,
Taramani, Chennai-113.

Tn 600113 IN

Email: ramanujan.veeraraghavan@sifycorp.com

Defendant No. 39

Southern Online Bio Technologies Limited

Flat # A3, 3rd Floor, Office Block, Samrat Complex,
Opposite to AG's Office, Saifabad,
Hyderabad

TG 500004 IN

Email: bnswamy@sol.net.in; babukvb@sol.net.in;
info@sol.net.in

Defendant No. 40

Syscon Infoway Private Limited

402, fourth floor, skyline icon, Andheri Kurla Road,
Behind Mittal ind. Estate, Andheri east,
Mumbai, Maharashtra 400059

Email: nikunj@joister.net

Defendant No. 41

Tata Teleservices Limited

10th Floor, Tower I, Jeevan Bharati,
124 Connaught Circus

New Delhi DI 110001 IN

Email: rishabh.aditya@tatatel.co.in

Defendant No. 42

Tikona Infinet Ltd.

3rd Floor, Office 3 A, Corpora Building, Lbs Marg,
Bhandup West, Mumbai - 400078

Email: compliance@tikona.in

Defendant No. 43

Vainavi Industries Limited

H. No. 1-8-741, Prakash Nagar Begumpet
Hyderabad TG 500016 IN

Email: rameshkrishnanaidu@gmail.com

Defendant No. 44

VIDEOCON TELECOMMUNICATIONS LIMITED

Defendant No. 45

R H No. 2, Pratapnagar Shahnoorwadi Road
 Aurangabad MH 431001 IN
 Email: corp.secretarial@videocon.com

VIVA Communications Private Limited

Defendant No. 46

No.9f & 9g, Gee Gee Emerald Old No 151, New No 312,
 Valluvar Kottam High Road, Nungambakkam
 Chennai Tn 600034 IN
 Email: accounts@vivacommunication.com

Vodafone Idea Ltd.

Defendant No. 47

Suman Tower, Plot No.18, Sector-11, Gandhinagar
 Gujarat - 382011
 Email: Arun.Madhav@vodafoneidea.com;
lakshmisree.chakraborty@vodafoneidea.com

You Broadband & Cable India Ltd

Defendant No. 48

Plot No. 54, Marol Co-operative Industrial Estate,
 Makwana, Andheri East,
 Mumbai MH 400059 IN
 Email: Arun.Madhav@vodafoneidea.com;
lakshmisree.chakraborty@vodafoneidea.com

Bharat Sanchar Nigam Ltd.

Defendant No. 49

Harish Chandra,
 Mathura Lane, Janpath,
 New Delhi - 110001
 Email: hcpant@bsnl.co.in

Bharti Airtel Limited

Defendant No. 50

Bharti Crescent,
 1, Nelson Mandela road, Vasant Kunj, Phase II,
 New Delhi - 110070
 Email: amit.bhatia@airtel.com;
compliance.officer@bharti.in

Hathway Cable & Datacom Limited

Defendant No. 51

Rahejas, 4th Floor, Main Avenue,
 Santacruz (w), Mumbai
 Email: paresh.t4@gmail.com; heena.t4@gmail.com;
ajay.singh@hathway.net;

Amber Online Services Limited

Defendant No. 52

106, Shamshiri Estate, 11-5-423, Lakdi Ka Pul,
Hyderabad, Telangana 500004
Email: amberonlineservices@gmail.com

City Online Services Limited

Defendant No. 53

701, 7th floor,
Aditya Trade Centre , Ameerpet,
Hyderabad – 500 038
Email: corp@cityonlines.com

Data Ingenious Global Limited

Defendant No. 54

Dalda Factory Road,
Durgapura, Jaipur,
Rajasthan – 302018
Email: cs1@dil.in

Excitel Broadband Private Limited

Defendant No. 55

O-2, Second Floor, O Block Lajpat Nagar-II,
Central Market, DELHI
South Delhi DL 110024 IN
Email: cs@excitel.com

Asianet Satellite Communications

Defendant No. 56

2A, II floor,
Leela Infopark, Technopark,
Kazhakkootam,
Kerala – 695581
Email: jobymathew@asianet.co.in

Home Systems Private Limited

Defendant No. 57

A/17, Gaurav Annex,
R.R.T Road,
Mulund (W).
Mumbai 4000 80
Email: nishanaker01@rediffmail.com

Honesty Net Solutions (India) Private Limited

Defendant No. 58

A-2009 – Station Plaza, Station Road, Bhandup (west),
Mumbai: 400 078
Email: suresh@hns.net.in

Atria Convergence Technologies Pvt. Ltd

Defendant No. 59

A-25 Ground Floor, Mohan Cooperative Estate,

New Delhi, 110044

Email: jithesh.chathambil@actcorp.in

Limras Eronet Broadband Services Private Limited

Defendant No. 60

18/7 Postal Colony, 3rd Street,

West Mambalam,

Chennai – 600 033

Email: venkatesh.trm@gmail.com

Mahanagar Telephone Nigam Limited

Defendant No. 61

Mahanagar Doorsanchar Sadan 5th Floor,

9 CGO Complex Lodhi Road DI 110003 IN

Email: mtnlcsco@gmail.com

My Network India Internet Services Pvt Limited

Defendant No. 62

Swaraj Hsg. Soc., Rh - 125, 'G' -Block,

Shahu Nagar, Chinchwad,

Pune - 411019 IN

Email: info@mynetworkindia.com

Netcom Online Solutions India Private Limited

Defendant No. 63

Viswa Paradise,

23, 23/4 Kalidasa road,

Ram Nagar,

Coimbatore: 641 009

Tamil Nadu

Email: cprabhuram1979@gmail.com

Nettlinx Limited

Defendant No. 64

3rd Floor, My Home Ssarovar Plaza,

Secretariat Road, Saifabad

Hyderabad – 500 063

Telangana State

Email: secretarial@nettlinx.org

Pioneer eLabs Limited

Defendant No. 65

GF, Pioneer towers,

Plot no 16

Software Units Layouts, Madhapur,

Hyderabad – 500081

Email: financecontroller@pioneerelabs.in

Quadrant Televentures Ltd.

Defendant No. 66

Autocars Compound Adalat Road Aurangabad

MH 431005 IN,

Email: secretarial@infotelconnect.com

Hathway Rajesh Multichannel Private Limited

41/2 Parvati Sadan Tilak Road,

Ghatkopar East Mumbai MH 400077

Email: paresh.t4@gmail.com; heena.t4@gmail.com

Defendant No. 67

Readylink Internet Services Limited

Plot No 7 Sakthi Colonyr K Puram Ganapathy

Coimbatore, Tamil Nadu - 641006

Email: accounts@readylink.in

Defendant No. 68

Google LLC

+1 (650) 253-000

1600 Amphitheatre Parkway,

Mountain View, California- 94043,

United States of America

Email: support-in@google.com

Defendant No. 69

Google India

+91-12-44512900

Unitech Signature Tower-II, Tower-B,

Sector-15, Part-II Village Silokhera,

Gurgaon 122001, India

Email: support-in@google.com

Defendant No. 70

Department of Telecommunications

Ministry of Communications

Sanchar Bhawan 20, Ashoka Road,

New Delhi 110001

Email: mohammedmuqem@gmail.com

Defendant No. 71

Union of India

**Through Ministry of Electronics and Information
Technology**

Electronics Niketan, 6, CGO Complex,

Lodhi Road, New Delhi: 110003

Email: mohammedmuqem@gmail.com

Defendant No. 72

Unknown Persons

Defendant No. 73

1. Note: All Defendants are contesting Defendants, the present suit is a John Doe Suit, and Defendant No. 1 to 36 are websites/URLs for whom no proper address is available.
2. In view of confidentiality and for preserving identity of the Plaintiff, Plaintiff has been named anonymously as 'X'



Abhishek Malhotra
Advocate

Abhishek Malhotra
TMT Law Practice
(Counsels for the Plaintiff)
C-2/39, Lower Ground Floor, Safdarjung
Development Area
New Delhi - 110 016

Place: New Delhi
Dated: 16 August 2021

E-mail: amalhotra@tmtlaw.co.in
Phone# 9971053888, 9899597359

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)
 CS (OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

SUIT FOR PERMANENT AND MANDATORY INJUNCTION

1. The present Suit is being filed seeking, *inter alia*, an order of permanent and mandatory injunction against the Defendants, directing them to remove the identified audio-visual content that form the subject matter of the suit (**Suit Video/s**) and refrain from hosting or uploading the said videos on any digital or other platform.

DESCRIPTION OF PARTIES

2. The Plaintiff, in her earlier avatar, worked extensively in Bengali movies and television shows as well as several ad films and music videos. Since 2017, the Plaintiff has created a distinctive identity and garnered reputation amongst viewers. The Plaintiff is a well-known personality in the industry. The Suit Videos, however, are of a nature and carry content that shows the Plaintiff in poor light and are being made available/communicated to the public without the Plaintiff's permission or consent

V.D

and are being used by unknown third parties to blackmail the Plaintiff as also to hurt the reputation meticulously created by the Plaintiff over the years.

3. To protect the identity of the Plaintiff, the Plaintiff has been anonymously named and referred to as 'X' in the present proceedings.
4. The Defendant Nos. 1 to 36 are websites engaged in the business of uploading content. These Defendants are in the business of broadcasting / relaying / communicating to the public content, in a licensed or unauthorized/ pirated manner. The Plaintiff submits that the Suit Videos are available on the websites of Defendant Nos. 1 to 36. The Defendants have uploaded the Suit Videos in an unauthorized manner without seeking consent either of the Plaintiff or even of the copyright owner of the Suit Videos. In any event, the Suit Videos comprise of revealing and explicit video clippings of the Plaintiff without receiving any prior consent from the Plaintiff, and the continued proliferation/ dissemination of such Suit Videos, despite Plaintiff's efforts to take down the same, has given rise to the present suit. These Defendants are amongst those websites known to the Plaintiff who are communicating to the public the explicit content in the form of Suit Videos. The Plaintiff craves leave of this Hon'ble Court to add more such parties as Defendants in the future, as and when the

V.D

Plaintiff acquires knowledge and is made aware of similar illegal activity by such other parties.

5. The Defendant Nos. 37 to 68 are Internet Service Providers (ISP) who are engaged in the business of providing basic telephony, mobile services and broadband network all over the world and whose obligations include those set out in under the Information Technology Act, 2000 and Rules formed thereunder, The Copyright Act, 1957, as well as the Telecom Regulatory Authority of India Act, 1997. These Defendants provide a medium to access World Wide Web (www) and telecommunication services through wired and wireless telephony to their respective customers. The Defendants have, in the past, allowed access to various websites and web pages that permit illegal/un-authorized/un-licensed videos. The said entities are necessary and proper parties for the reason that it is these ISPs who can restrict or limit the access to the Suit Videos by employing technological means or “filters”, which “block” the Defendant websites (Defendant Nos. 1 to 36) from delivering and hosting the Suit Videos either in a licensed/ unlicensed manner. Hence, they are arrayed as proforma Defendants to this suit, for the limited purpose of compliance of the orders of this Hon’ble Court to block the URLs where the Suit Videos are broadcast/communicated to the public. Under the Information Technology Act, 2000, the Government of India has issued the Information Technology (Intermediary Guidelines and Digital Media

V.D

Ethics Code) Rules, 2021 vide notification dated February 25, 2021, mandating an ISP, like other intermediaries, to prevent the broadcast of explicit content upon receipt of complaint and preserve an individual's rights and cooperate in taking down pornographic content or content which is objectionable or sexually explicit upon a complaint from an individual, so that it is not circulated further. It is submitted that the ISPs herein are under an obligation to protect the Plaintiff's rights since the Plaintiff is the aggrieved person whose explicit Suit Videos have been broadcast and communicated to public through the Defendant websites.

6. Defendant No. 69 and 70 are Google LLC and Google India. The Plaintiff submits that the Suit Videos are available on the search engine which are under the control and ownership of the Defendant Nos. 69 & 70. By way of the present suit, the Plaintiff seeks a mandatory and permanent injunction against Defendant Nos. 69 and 70 for removing the tags, metatags and other metadata in relation to the user searches, results whereof, lead the user/ person searching to the Suit Videos.
7. The Defendant Nos. 71 and 72 are the Union of India through the Ministry of Electronics and Information Technology (**MEITY**) and through the Department of Telecommunications (**DOT**) respectively under the Ministry of Communications. The Plaintiff states that MEITY and DOT are being impleaded for the limited purpose of enabling

V.D

part of this short video clip. The Plaintiff was promised that upon engagement she would be offered a role in the Series.

11. It is pertinent to note that the Series was never produced as the project was shelved. Thus, till date, the Plaintiff has not executed any formal contract with Ram Gopal Verma Studios, producers of the Series for shooting of the Suit Videos. That in the absence of any contract, the short videos recorded for the Series could not be utilised in any manner neither by Ram Gopal Verma Studios nor any of the other Defendants herein.
12. Despite the fact that the Series was never released, in and around December 2020, the Plaintiff came to know that the video clips shot by Ram Gopal Verma Studios had been uploaded by Mr Ram Gopal Verma on his YouTube channel/ the channel under the control of Ram Gopal Verma Studios and on the Studio's website.
13. The Plaintiff submits that the Suit Videos, ostensibly being referred to as the "trailer" for the defunct Series have surfaced on multiple digital platforms and websites comprising explicit scenes of complete, frontal nudity of the Plaintiff (**Suit Video/s**).
14. The Plaintiff states that while the Plaintiff had verbally consented to the filming of the explicit content as a demonstration recording, the Suit Videos could not have been either released by Ram Gopal Verma/ Ram

V.D

Gopal Verma Studios or utilised or made available by third parties/ Defendants.

15. That the Plaintiff immediately reached out to Mr Ram Gopal Verma, requesting the latter to remove the Suit Videos uploaded on the Youtube channel as well as the website. Mr Ram Gopal Verma intimated the Plaintiff that he would render all assistance and cooperate in removal of the Suit Videos uploaded by him/Ram Gopal Verma Studios on Youtube and the website. In support of this understanding, the Plaintiff places on record print out of the conversation exchanged with Mr Ram Gopal Verma through WhatsApp along with the list of documents filed with the suit.

16. It is stated that pursuant to the conversation with Mr Ram Gopal Verma, the videos uploaded by him/ his studio were deleted and removed from the said digital platforms. Further, Mr Ram Gopal Verma also confirmed in December 2020 that the Suit Video uploaded on Youtube and the website had been removed by him.

17. The Plaintiff states that especially as the Series was shelved by Ram Gopal Verma Studios, the unauthorised release of the so called "trailer" comprising of portions of Plaintiff's explicit video clippings/ Suit Videos by the Defendants have severely affected the Plaintiff's reputation and profession.

V.D

18. It is pertinent to note that the Suit Videos have also been hosted on several websites communicating to the public, obscene and pornographic content. Further, in the absence of any authorization, inter alia, from the Plaintiff, the Suit Videos could not have been uploaded on any platform including but not limited to the Defendant websites.

19. It is noteworthy that the unauthorised exploitation of the explicit video clippings and the hosting of such videos on pornographic websites has prejudiced and adversely the Plaintiff's professional endeavours. The Plaintiff further states that on the basis of the explicit videos which have been broadcast on several of the Defendant websites, the Plaintiff has received multiple calls from anonymous individuals who have threatened to publicise the explicit content in the Suit Videos, to disrepute the Plaintiff and disrupt her professional endeavours. The Plaintiff also states that such anonymous callers have held the Plaintiff to ransom and sought to extort money from the Plaintiff as a consideration to refrain from publicising the explicit Suit Videos.

20. Owing to the above, particularly the anonymous threats received and the constant harassment, the Plaintiff has also undergone a change in name. Due to the surfacing of the explicit Suit Videos on several websites including pornographic websites, the name and the identity of the Plaintiff was completely tarnished. As a result, to avoid any further harassment, the Plaintiff has officially undergone a name change and is currently

V.D

known by her new name. The erstwhile and present names of the Plaintiff are not being disclosed in the present plaint in order to protect the identity of the Plaintiff. However, upon direction of the Court, the Plaintiff is willing to produce to proof in support of her erstwhile name and the present name in a sealed cover, for perusal and satisfaction of this Hon'ble Court.

21. That 'right to be forgotten' and 'right to be left alone' have been recognised as an inseparable and inherent aspects of right to privacy in India. Decisions of this Hon'ble Court as well as Supreme Court of India and High Courts across India, including the Hon'ble High Court of Odisha, Karnataka and Madras have recognised and enforced right to be forgotten as an intrinsic aspect of the right to privacy. Plaintiff craves leave to rely on the relevant decisions at the time of hearing of the present matter. Accordingly, the Plaintiff by the present suit seeks removal of the Suit Videos from the Defendant websites.

22. The Plaintiff submits that in the past, this Hon'ble Court has granted similar injunctive reliefs to other parties in suits, by allowing enforcement of right to be forgotten as an intrinsic part of right to privacy. Copy of such relevant orders are annexed to the present suit.

23. The Plaintiff states that the Suit Videos can be accessed by viewers and users of the internet by an input of a search query on a search engine such as Google Search which is controlled by Defendant Nos. 69 & 70. By

V.D

mere use of key words such as the erstwhile name of the Plaintiff along with the name of the Series, leads to population of results for the explicit videos on Defendant websites. The Plaintiff states that the search engine will process certain search results, which may contain links to websites/web pages that are authorized as well as unauthorized. The availability of multiple such "search indexed" links provides very easy access to the content which are uploaded in an unauthorised manner.

24. It is stated that such ease of access to Defendants' and other rogue websites/mobile application, as facilitated by the search engines, is one of the major concerns for the Plaintiff, as it contributes to large scale infringement of Plaintiff's legal right, resulting in constant harassment and loss of reputation in addition to jeopardising the Plaintiff's career as an actor.

25. It is submitted that, this Hon'ble Court has held that the test for whether a Defendant website is a rogue website is a qualitative one, and is focused on whether the Defendant website is prima facie infringing. Some of the illustrative criteria laid down by this Hon'ble Court for determining whether a website is a "*Flagrantly Infringing Online Location*" (FIOL)/Rogue Website and the satisfaction of those conditions in the context of the Defendant websites arrayed in the present case is set out below:-

V.D

- a. whether the primary purpose of the website is to commit or facilitate infringement- It is submitted that the Defendant websites hosting pornographic content and/ or other content without the consent or prior authorization of individuals videographed such as the Plaintiff in the present case amounts to infringement.
- b. The flagrancy of the infringement, or the flagrancy of the facilitation of the infringement- It is submitted that some of the Defendant rogue websites facilitate infringement by providing features such as indexing, detailed search functions, categorization, etc. thereby making it very convenient for a user to search and download the illegal Suit Videos.
- c. Whether the detail of the registrant is masked and no personal or traceable detail is available either of the Registrant or of the user – It is noteworthy that most of the Defendant websites' WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user.

26. It is further submitted that in the absence of any specific order from this Hon'ble Court, the Plaintiff's objective of protecting and enforcing its legal right cannot be fulfilled. The Plaintiff submits that as it is the business of search engines to process search results, the said search engines are unlikely to accede to Plaintiff's requests to delete the

V.D

URLs/indexed links from the search pages that lead the viewers to websites/web pages broadcasting/ comprising of the explicit Suit Videos, unless the Plaintiff has the mandate/order from this Hon'ble Court, allowing the Plaintiff to enforce such requests against search engines.

27. It is accordingly submitted that the Plaintiff is entitled to such an order, directing the search engines, to act on the requests of the Plaintiff to remove the links to websites of Defendant Nos.1 to 36 and/or any other website that the Plaintiff discovers, at any later point in time, after grant of orders by this Hon'ble Court, to be indulging in the broadcasting of the Suit Videos complained of in the present suit.

28. The Plaintiff submits that this Hon'ble Court may also direct the search engines such as Google to also disclose details of the server of the website streaming the Suit Videos. Consequently, once the server details are revealed, the source from which content emanates may be directed in order to obstruct relevant parties from engaging in such illegal and unauthorized dissemination of the Suit Videos. The Plaintiff's aforesaid submission is based on the fact that the rogue websites use common servers to direct their infringing activity/traffic. Such information is required because, very often, these rogue websites are able to either (i) mask the geographical location of the sites/have dynamic websites so that in the event that the order is obtained in a particular name/title/URL, they

V.D.

can quickly change the said external details and escape liability; and/or (ii) the rogue website operators are able to very quickly “shift” the illegal operation on to a “new” redirect / mirror / alphanumeric websites etc, with minimal difficulty. In the event, however, that the server details are disclosed by the ISPs/TSPs, which information is in the sole knowledge of the ISPs/TSPs, then, on service of the order of this Hon’ble Court, upon such servers, they will either have to necessarily block such rogue operators themselves, from using the server/platform for such illegal activity, or provide the Plaintiff the access to seek further orders of blocking such servers themselves.

29. On earlier occasions, this Hon’ble Court has issued website blocking orders against rogue websites. In *UTV Software Communication Limited & Others v. 1337x.to & Ors (CS (Comm) 724 of 2017)*, this Hon’ble Court has recognized that in many cases like the present one, after the issuance of an injunction in respect of the main website by way of an initial injunction order, several mirror/alphanumeric/redirect websites are subsequently created to circumvent the injunction orders. Hence, in the interest of liberating the courts from constantly monitoring and adjudicating the issue of mirror/redirect/alphanumeric websites and also unburdening plaintiffs from filing fresh suits with respect thereto, this Hon’ble Court endorsed the concept of “dynamic injunctions” and

V.D

directed that the plaintiffs in such cases may file an affidavit confirming that the newly impleaded website is a mirror/redirect/alphanumeric website with sufficient supporting evidence and, on being satisfied that the impugned website is indeed a mirror/redirect/alphanumeric website of injuncted Rogue Website(s) and merely provides new means of accessing the same primary infringing website, the Joint Registrar shall issue directions to ISPs to disable access in India to such mirror/redirect/alphanumeric websites in terms of the orders passed.

30. In light of the same, the Plaintiff submits that it is entitled to an order from this Hon'ble Court making the injunction orders applicable to the creators of such redirect / mirror / alphanumeric websites etc. to restrain them from unauthorizedly broadcasting or hosting the Suit Video. In this regard, the Plaintiff also seeks liberty to file an affidavit before the Joint Registrar to implead the mirror/redirect/alphanumeric websites under Order I Rule 10 CPC in the event they merely provide new means of accessing the same primary infringing websites that have been injuncted. The Plaintiff further submits that it is also entitled to protection by way of a direction to the ISPs / TSPs to make disclosures of the origin servers for the rogue website, so as to enable the Plaintiff to seek appropriate enforcement and observance of orders of this Hon'ble Court.

CAUSE OF ACTION

V.D.

31. The cause of action for filing the present suit arose in December 2020 when the Plaintiff gained knowledge of the explicit Suit Videos which were hosted on some of the Defendant websites. Thereafter, cause of action arose in June 2021 when the Plaintiff started receiving anonymous threats from individuals who threatened to disrepute and tarnish the reputation of the Plaintiff by publicising the Suit Videos and who also sought to extort money from the Plaintiff on the above pretext. The Plaintiff submits that the cause of action is a continuing one as the explicit Suit Videos are still available on Defendant websites and there is constant harassment of the Plaintiff by anonymous individuals.

JURISDICTION

32. The Plaintiff submits that this Hon'ble Court has the necessary territorial and pecuniary jurisdiction to consider the present petition. The Suit Videos are available and accessible by viewers by using the Defendant websites within the territorial jurisdiction of this Hon'ble Court. In view of this, a part of the cause of action has arisen within the jurisdiction of this Hon'ble Court. Accordingly, the Court has the requisite territorial jurisdiction. This Court, therefore, has the necessary jurisdiction to consider the suit and grant necessary reliefs under Section 20 of the Code of Civil Procedure, 1908 (CPC).
33. It is submitted that the Plaintiff has not filed any other suit either before this Hon'ble Court or before any other forum for the relief sought herein.

V.D.

34. The present suit is of non-commercial nature. The subject matter of the Suit relates to loss of reputation of the Plaintiff caused owing to the Suit Videos.

VALUATION

1. For the purpose of court fees and jurisdiction, the Plaintiff values its claim as follows:
 - a. For an order of permanent injunction at INR 2,00,00,000, for restraining the Defendants from hosting the Suit Videos. Accordingly, court fee of Rs 2,00,000/- is affixed thereon ;
 - b. For an order of mandatory injunction at INR 200/-, for directing the Defendants to take down and remove the Suit Videos. Accordingly, court fee of Rs 20/- is affixed thereon

In view of the above, the present Suit is valued at a total of INR 2,00,00,200/- and a total court fee of INR 2,00,020/- is affixed thereon. The Plaintiff further undertakes to affix such further court fee as may be required and directed by this Hon'ble Court.

The Plaintiff has also affixed the one-time process fee of INR 36,500/- for service on defendants. The Plaintiff states that she has paid the total court fee and the one-time process fee of INR 2,36,520/-, from the bank account originally in the name of the Plaintiff. As the present suit is filed by the Plaintiff anonymously as 'X', the court fee remitted from the bank account of the Plaintiff may be accepted by this Hon'ble Court.

PRAYER

36. In light of the aforementioned facts and circumstances and submissions made, it is prayed that this Hon'ble Court be pleased to pass:-

- I. Pass a decree of mandatory injunction against the Defendants, their partners, proprietors, their officers, servants, agents and representatives, franchisees, and all others in capacity of principal or agent, acting for and on their behalf, directing them to remove the explicit Suit Videos, footage, clip, audio only and/or any part of the Suit Videos featuring the Plaintiff without/in the absence of the release of the Series and without the express authorization and consent of the Plaintiff.
- II. Pass a decree of permanent injunction restraining the Defendants, their partners, proprietors, their officers, servants, agents and representatives, franchisees, head-ends and all others in capacity of principal or agent, acting for and on their behalf from broadcasting / communicating to public/ making available to viewers/ users through online platforms the explicit Suit Videos, footage, clip, audio only and/or any part of the Suit Videos featuring the Plaintiff outside the Series and depiction of the Suit Videos without/in the absence of the release of the Series and without the express authorization and consent of the Plaintiff.
- III. Pass an order making the aforesaid injunction order applicable to the mirror/redirect/alphanumeric websites/mobile applications created by the Defendant Nos. 1 to 36 or by any other person to grant access to the websites/mobile applications of Defendant Nos. 1 to 36 or any other rogue website that the Plaintiff comes across.

V.D

- IV. Permit the Plaintiff to file an affidavit before the Joint Registrar to implead the mirror/redirect/alphanumeric websites/mobile applications under Order I Rule 10 CPC in the event they merely provide new means of accessing the same primary infringing websites that have been injuncted;
- V. Pass an order giving the Plaintiff liberty to notify all search engines and seek take down/deletion from their search results pages, listings of websites/ URLs/mobile applications which are infringing upon the Plaintiff's legal right;
- VI. Pass an order directing the ISPs i.e., Defendant Nos. 37 to 68 to disclose the details of all servers being used by Defendant Nos. 1 to 36 and any other websites/mobile applications that are found to be indulging in the broadcast/ communicating to the public the Suit Videos or clips thereof;
- VII. In respect of Defendants that are currently not identified and/or are unknown as of date, an order may be passed whereby the said Defendant(s) be restrained in terms of prayers I and II stated above;
- VIII. In order to effectuate the above orders, the Registry may be directed to issue extra summons in the name of Ashok Kumars / Unnamed Defendants, whose details would be supplied by the Plaintiff as and when the Plaintiff receives information regarding the same; AND/ OR

V.D

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)
 CS (OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

**STATEMENT CERTIFYING AUTHENTICITY OF DOCUMENTS
 FILED WITH THE PLAINT**

The following documents are attached as Exhibits/Annexures in our
 Plaint:

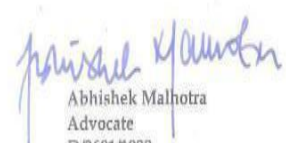
S. No.	Particulars
A.	Print out of list of URLs
B.	Screenshots of Plaintiff's conversation with Ram Gopal Verma
C.	Order of the Delhi High Court in <i>Jorawer Singh Mundy v. Union of India and Ors.</i> , 2021 SCC Online Del 2306
D.	Order of the Delhi High Court in <i>Zulfiqar Ahman Khan v. Quintillion Business Media Pvt Ltd and Ors.</i> , 2019 SCC Online Del 8494
E.	Order of the Odisha High Court in <i>Subhranshu Rout v. State of Odisha</i> , 2020 SCC Online Ori 878

F.	Order of Karnataka High Court in <i>Vasunathan v. Registrar General</i> , 2017 SCC Online Kar 424
G.	Order of Madras High Court in WP(MD) No. 12015 of 2021
H.	Judgment of the Delhi High Court in <i>UTV Software Communication Ltd. and Ors. v. 1337X.To and Others</i> , 2019 SCC Online Del 8002

We hereby certify that the above-mentioned documents are authentic.

Plaintiff

THROUGH



Mr. Abhishek Malhotra
For TMT Law Practice
 Counsels for the Plaintiff
 C-2/39, Lower Ground Floor,
 Safdarjung Development Area
 New Delhi – 110 016

Place: New Delhi

Dated: August 16, 2021

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)
 CS (OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

LIST OF RELIANCE FILED BY THE PLAINTIFF

Sl. No.	Particulars
1.	Records of the Plaintiff
2.	Documents demonstrating unauthorized hosting and uploading of Plaintiff's videos on digital platforms.
3.	Such other documents reliance on which may be found necessary after the issues are settled between the parties herein.


 Abhishek Malhotra
 Advocate

TMT Law Practice
 Counsels for the Plaintiff
 C-2/39, Lower Ground Floor,
 Safdarjung Development Area
 New Delhi – 110 016

Place: New Delhi

Dated: August 16, 2021

IN THE HIGH COURT OF DELHI AT NEW DELHI

(Ordinary Original Jurisdiction)

C.S.(OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus


<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

**INDEX - II
(INTERIM APPLICATIONS)**

Sr. No.	Particulars	Page No.
1.	Index - II (Interim Applications)	1 - 2
2.	Plaintiff's Application under Order 39 Rule 1 & 2 read with Section 151 of Code of Civil Procedure, 1908, along with affidavit in support.	3 - 19
3.	Plaintiff's Application under Section 151 of CPC seeking confidentiality of the proceedings along with affidavit in support.	20 - 26
4.	Plaintiff's Application under Section 151 of Code of Civil Procedure, 1908, along with affidavit in support, for exemption from filing original copies and fair typed copies of original documents along with affidavit in support.	27 - 31
5.	Application under section 80(2) of the code of civil procedure, 1908 along with affidavit in support.	32 - 36

THROUGH



Abhishek Malhotra
Advocate

Place: New Delhi
Dated: August 16, 2021

Abhishek Malhotra
TMT Law Practice
Counsel for the Plaintiff
C-2/39, Lower Ground Floor,
Safdarjung Development Area,
New Delhi - 110016
E-mail: amalhotra@tmtlaw.co.in
Phone# 9971053888, 9899597359

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)

IA NO. OF 2021
 IN
 CS (OS) NO. OF 2021

IN THE MATTER OF:

X ...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

**APPLICATION ON BEHALF OF THE PLAINTIFF UNDER ORDER
 XXXIX RULES 1 & 2 OF THE CODE OF CIVIL PROCEDURE, 1908,
 READ WITH SECTION 151 OF THE CODE OF CIVIL PROCEDURE,
 1908**

1. The present Suit is being filed seeking, *inter alia*, an order of permanent and mandatory injunction against the Defendants, directing them to remove the identified audio-visual content that form the subject matter of the suit (**Suit Videos**) and refrain from hosting or uploading the said videos on any digital or other platform.
2. The present application is being filed seeking interim reliefs against the Defendants, injuncting the latter and directing them to take down the Suit Videos and restraining them from uploading the Suit Videos, any further.

3. In 2017, the Plaintiff was engaged by Mr Ram Gopal Verma, owner of Ram Gopal Verma Studios for the filming of the web series, name of which has been disclosed in the plaint (**Series**). The Series was themed on Mumbai Mafia in India and the internal conflicts amongst the members of organised crimes/ underworld in Mumbai.
4. The Plaintiff was promised lead role in the Series and on that pretext, was lured into participating in a demonstration video. The Suit Video forms a part of this short video clip. The Plaintiff was promised that upon engagement she would be offered a role in the Series.
5. It is pertinent to note that the Series was never produced as the project was shelved. Thus, till date, the Plaintiff has not executed any formal contract with Ram Gopal Verma Studios, producers of the Series for shooting of the Suit Videos. That in the absence of any contract, the short videos recorded for the Series could not be utilised in any manner neither by Ram Gopal Verma Studios nor any of the other Defendants herein.
6. Despite the fact that the Series was never released, in and around December 2020, the Plaintiff came to know that the video clips shot by Ram Gopal Verma Studios had been uploaded by Mr Ram Gopal Verma on his YouTube channel/ the channel under the control of Ram Gopal Verma Studios and on the Studio's website.
7. The Plaintiff submits that the Suit Videos, ostensibly being referred to as the "trailer" for the defunct Series have surfaced on multiple digital

platforms and websites comprising explicit scenes of complete, frontal nudity of the Plaintiff (**Suit Video/s**).

8. The Plaintiff states that while the Plaintiff had verbally consented to the filming of the explicit content as a demonstration recording, the Suit Videos could not have been either released by Ram Gopal Verma/ Ram Gopal Verma Studios or utilised or made available by third parties/ Defendants.
9. That the Plaintiff immediately reached out to Mr Ram Gopal Verma, requesting the latter to remove the Suit Videos uploaded on the Youtube channel as well as the website. Mr Ram Gopal Verma intimated the Plaintiff that he would render all assistance and cooperate in removal of the Suit Videos uploaded by him/Ram Gopal Verma Studios on Youtube and the website. In support of this understanding, the Plaintiff places on record print out of the conversation exchanged with Mr Ram Gopal Verma through WhatsApp along with the list of documents filed with the suit.
10. It is stated that pursuant to the conversation with Mr Ram Gopal Verma, the videos uploaded by him/ his studio were deleted and removed from the said digital platforms. Further, Mr Ram Gopal Verma also confirmed in December 2020 that the Suit Video uploaded on Youtube and the website had been removed by him.

11. The Plaintiff states that especially as the Series was shelved by Ram Gopal Verma Studios, the unauthorised release of the so called “trailer” comprising of portions of Plaintiff’s explicit video clippings/ Suit Videos by the Defendants have severely affected the Plaintiff’s reputation and profession.
12. It is pertinent to note that the Suit Videos have also been hosted on several websites communicating to the public, obscene and pornographic content. Further, in the absence of any authorization, inter alia, from the Plaintiff, the Suit Videos could not have been uploaded on any platform including but not limited to the Defendant websites.
13. It is noteworthy that the unauthorised exploitation of the explicit video clippings and the hosting of such videos on pornographic websites has prejudiced and adversely the Plaintiff’s professional endeavours. The Plaintiff further states that on the basis of the explicit videos which have been broadcast on several of the Defendant websites, the Plaintiff has received multiple calls from anonymous individuals who have threatened to publicise the explicit content in the Suit Videos, to disrepute the Plaintiff and disrupt her professional endeavours. The Plaintiff also states that such anonymous callers have held the Plaintiff to ransom and sought to extort money from the Plaintiff as a consideration to refrain from publicising the explicit Suit Videos.

14. Owing to the above, particularly the anonymous threats received and the constant harassment, the Plaintiff has also undergone a change in name. Due to the surfacing of the explicit Suit Videos on several websites including pornographic websites, the name and the identity of the Plaintiff was completely tarnished. As a result, to avoid any further harassment, the Plaintiff has officially undergone a name change and is currently known by her new name. The erstwhile and present names of the Plaintiff are not being disclosed in the present plaint in order to protect the identity of the Plaintiff. However, upon direction of the Court, the Plaintiff is willing to produce to proof in support of her erstwhile name and the present name in a sealed cover, for perusal and satisfaction of this Hon'ble Court.
15. That 'right to be forgotten' and 'right to be left alone' have been recognised as an inseparable and inherent aspects of right to privacy in India. Decisions of this Hon'ble Court as well as Supreme Court of India and High Courts across India, including the Hon'ble High Court of Odisha , Karnataka and Madras have recognised and enforced right to be forgotten as an intrinsic aspect of the right to privacy. Plaintiff craves leave to rely on the relevant decisions at the time of hearing of the present matter. Accordingly, the Plaintiff by the present suit seeks removal of the Suit Videos from the Defendant websites.
16. The Plaintiff submits that in the past, this Hon'ble Court has granted similar injunctive reliefs to other parties in suits, by allowing enforcement of right

to be forgotten as an intrinsic part of right to privacy. Copy of such relevant orders are annexed to the present suit.

17.The Plaintiff states that the Suit Videos can be accessed by viewers and users of the internet by an input of a search query on a search engine such as Google Search which is controlled by Defendant Nos. 69 and 70. By mere use of key words such as the erstwhile name of the Plaintiff along with the name of the Series, leads to population of results for the explicit videos on Defendant websites. The Plaintiff states that the search engine will process certain search results, which may contain links to websites/web pages that are authorized as well as unauthorized. The availability of multiple such “search indexed” links provides very easy access to the content which are uploaded in an unauthorised manner.

18.It is stated that such ease of access to Defendants’ and other rogue websites/mobile application, as facilitated by the search engines, is one of the major concerns for the Plaintiff, as it contributes to large scale infringement of Plaintiff’s legal right, resulting in constant harassment and loss of reputation in addition to jeopardising the Plaintiff’s career as an actor.

19.It is submitted that, this Hon’ble Court has held that the test for whether a Defendant website is a rogue website is a qualitative one, and is focused on whether the Defendant website is prima facie infringing. Some of the illustrative criteria laid down by this Hon’ble Court for determining

whether a website is a “*Flagrantly Infringing Online Location*” (FIOL)/Rogue Website and the satisfaction of those conditions in the context of the Defendant websites arrayed in the present case is set out below:-

- a. whether the primary purpose of the website is to commit or facilitate infringement- It is submitted that the Defendant websites hosting pornographic content and/ or other content without the consent or prior authorization of individuals videographed such as the Plaintiff in the present case amounts to infringement.
- b. The flagrancy of the infringement, or the flagrancy of the facilitation of the infringement- It is submitted that some of the Defendant rogue websites facilitate infringement by providing features such as indexing, detailed search functions, categorization, etc. thereby making it very convenient for a user to search and download the illegal Suit Videos.
- c. Whether the detail of the registrant is masked and no personal or traceable detail is available either of the Registrant or of the user – It is noteworthy that most of the Defendant websites’ WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user.

20. It is further submitted that in the absence of any specific order from this Hon'ble Court, the Plaintiff's objective of protecting and enforcing its legal right cannot be fulfilled. The Plaintiff submits that as it is the business of search engines to process search results, the said search engines are unlikely to accede to Plaintiff's requests to delete the URLs/indexed links from the search pages that lead the viewers to websites/web pages broadcasting/ comprising of the explicit Suit Videos, unless the Plaintiff has the mandate/order from this Hon'ble Court, allowing the Plaintiff to enforce such requests against search engines.
21. It is accordingly submitted that the Plaintiff is entitled to such an order, directing the search engines, to act on the requests of the Plaintiff to remove the links to websites of Defendant Nos.1 to 36 and/or any other website that the Plaintiff discovers, at any later point in time, after grant of orders by this Hon'ble Court, to be indulging in the broadcasting of the Suit Videos complained of in the present suit.
22. The Plaintiff submits that this Hon'ble Court may also direct the search engines such as Google to also disclose details of the server of the website streaming the Suit Videos. Consequently, once the server details are revealed, the source from which content emanates may be directed in order to obstruct relevant parties from engaging in such illegal and unauthorized dissemination of the Suit Videos. The Plaintiff's aforesaid submission if

based on the fact that the rogue websites use common servers to direct their infringing activity/traffic. Such information is required because, very often, these rogue websites are able to either (i) mask the geographical location of the sites/have dynamic websites so that in the event that the order is obtained in a particular name/title/URL, they can quickly change the said external details and escape liability; and/or (ii) the rogue website operators are able to very quickly “shift” the illegal operation on to a “new” redirect / mirror / alphanumeric websites etc, with minimal difficulty. In the event, however, that the server details are disclosed by the ISPs/TSPs, which information is in the sole knowledge of the ISPs/TSPs, then, on service of the order of this Hon’ble Court, upon such servers, they will either have to necessarily block such rogue operators themselves, from using the server/platform for such illegal activity, or provide the Plaintiff the access to seek further orders of blocking such servers themselves.

23. On earlier occasions, this Hon’ble Court has issued website blocking orders against rogue websites. In *UTV Software Communication Limited & Others v. 1337x.to & Ors* (CS (Comm) 724 of 2017), this Hon’ble Court has recognized that in many cases like the present one, after the issuance of an injunction in respect of the main website by way of an initial injunction order, several mirror/alphanumeric/redirect websites are subsequently created to circumvent the injunction orders. Hence, in the interest of

liberating the courts from constantly monitoring and adjudicating the issue of mirror/redirect/alphanumeric websites and also unburdening plaintiffs from filing fresh suits with respect thereto, this Hon'ble Court endorsed the concept of "dynamic injunctions" and directed that the plaintiffs in such cases may file an affidavit confirming that the newly impleaded website is a mirror/redirect/alphanumeric website with sufficient supporting evidence and, on being satisfied that the impugned website is indeed a mirror/redirect/alphanumeric website of injuncted Rogue Website(s) and merely provides new means of accessing the same primary infringing website, the Joint Registrar shall issue directions to ISPs to disable access in India to such mirror/redirect/alphanumeric websites in terms of the orders passed.

24. In light of the same, the Plaintiff submits that it is entitled to an order from this Hon'ble Court making the injunction orders applicable to the creators of such redirect / mirror / alphanumeric websites etc. to restrain them from unauthorizedly broadcasting or hosting the Suit Video. In this regard, the Plaintiff also seeks liberty to file an affidavit before the Joint Registrar to implead the mirror/redirect/alphanumeric websites under Order I Rule 10 CPC in the event they merely provide new means of accessing the same primary infringing websites that have been injuncted. The Plaintiff further submits that it is also entitled to protection by way of a direction to the ISPs

/ TSPs to make disclosures of the origin servers for the rogue website, so as to enable the Plaintiff to seek appropriate enforcement and observance of orders of this Hon'ble Court.

25. It is submitted that a prima facie case exists in favour of the Plaintiff as the Suit Videos of the Plaintiff were uploaded by the Defendant websites without any authorization neither from the producer of the Series nor the Plaintiff. Prima facie case exists in favour of the Plaintiff in view of the settled legal position which recognizes an individual's right to be forgotten as an intrinsic right under right to privacy. In view of the fact that the Plaintiff has altered her name, a further prima facie case exists in favour of enforcing Plaintiff's right to be forgotten by directing the Defendants to take down the Suit Videos.
26. Plaintiff submits that the balance of convenience exists in her favour. It is submitted that the correct measure of balance of convenience can only be ascertained by recognizing the inconvenience caused to the Plaintiff due to the unauthorised exploitation of the explicit video clippings and the hosting of such videos on Defendant websites. It is submitted that the Plaintiff shall suffer irreparable injury unless the Defendants are restrained by an interim injunction order of this Hon'ble Court. Irreparable injury is being caused and will continue further on account of such unauthorized hosting and uploading of the Suit Videos. Plaintiff's reputation and professional

endeavors are gravely affected due to the release of the Suit Videos on different digital platforms including the Defendant websites.

27. The present application is being filed *bona fide* and in the interest of justice.

PRAYER:

28. In light of the aforementioned facts and circumstances and submissions made, it is prayed that this Hon'ble Court be pleased to:-

- a. Pass an order of interim injunction against the Defendants, their partners, proprietors, their officers, servants, agents and representatives, franchisees, and all others in capacity of principal or agent, acting for and on their behalf, directing them to remove the explicit Suit Videos, footage, clip, audio only and/or any part of the Suit Videos featuring the Plaintiff without/in the absence of the release of the Series and without the express authorization and consent of the Plaintiff.
- b. Pass an order of interim injunction restraining the Defendants, their partners, proprietors, their officers, servants, agents and representatives, franchisees and all others in capacity of principal or agent, acting for and on their behalf from broadcasting / communicating to public/ making available to viewers/ users through online platforms the explicit Suit Videos, footage, clip,

audio only and/or any part of the Suit Videos featuring the Plaintiff outside the Series and depiction of the Suit Videos without/in the absence of the release of the Series and without the express authorization and consent of the Plaintiff.

- c. Pass an order making the aforesaid injunction order applicable to the mirror/redirect/alphanumeric websites/mobile applications created by the Defendant Nos. 1 to 36 or by any other person to grant access to the websites/mobile applications of Defendant Nos. 1 to 36 or any other rogue website that the Plaintiff comes across.
- d. Permit the Plaintiff to file an affidavit before the Joint Registrar to implead the mirror/redirect/alphanumeric websites/mobile applications under Order I Rule 10 CPC in the event they merely provide new means of accessing the same primary infringing websites that have been injuncted;
- e. Pass an order giving the Plaintiff liberty to notify all search engines and seek take down/deletion from their search results pages, listings of websites/ URLs/mobile applications which are infringing upon the Plaintiff's legal right;
- f. Pass an order directing the ISPs i.e., Defendant Nos. 37 to 68 to disclose the details of all servers being used by Defendant Nos. 1 to

36 and any other websites/mobile applications that are found to be indulging in the broadcast/ communicating to the public the Suit Videos or clips thereof;

- g. In respect of Defendants that are currently not identified and/or are unknown as of date, an order may be passed whereby the said Defendant(s) be restrained in terms of prayers a. and b. stated above;
- h. In order to effectuate the above orders, the Registry may be directed to issue extra summons in the name of Ashok Kumars / Unnamed Defendants, whose details would be supplied by the Plaintiff as and when the Plaintiff receives information regarding the same;
- i. Pass ex- parte interim reliefs in terms of prayers a. to h. stated above

AND/ OR

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)

IA NO. OF 2021

IN

CS (OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

**APPLICATION ON BEHALF OF THE PLAINTIFF UNDER
SECTION 151 OF THE CODE OF CIVIL PROCEDURE, 1908
SEEKING CONFIDENTIALITY OF THE PROCEEDINGS**

1. The present Suit is being filed seeking, *inter alia*, an order of permanent and mandatory injunction against the Defendants, directing them to remove the identified audio-visual content that form the subject matter of the suit (**Suit Videos**) and refrain from hosting or uploading the said videos on any digital or other platform.
2. The present application is being filed seeking an order from this Hon'ble Court to retain confidentiality in the present proceedings.
3. The Plaintiff is not repeating the facts of the present suit for the sake of brevity. However, the Plaintiff craves leave to rely upon the facts

of the plaint. The brief facts pertinent to the present application are set out hereunder:

- 3.1. In 2017, the Plaintiff was engaged by Mr Ram Gopal Verma, owner of Ram Gopal Verma Studios for the filming of the web series, name of which is set out in the plaint (**Series**). The Series was themed on Mumbai Mafia in India and the internal conflicts amongst the members of organised crimes/ underworld in Mumbai.
 - 3.2. The Plaintiff was promised lead role in the Series and on that pretext, was lured into participating in a demonstration video. The Suit Video forms a part of this short video clip. The Plaintiff was promised that upon engagement she would be offered a role in the Series.
 - 3.3. The Plaintiff submits that the Suit Videos, ostensibly being referred to as the “trailer” for the defunct Series have surfaced on multiple digital platforms and websites comprising explicit scenes of complete, frontal nudity of the Plaintiff (**Suit Videos**).
 - 3.4. It is pertinent to note that the Suit Videos have also been hosted on several websites communicating to the public, obscene and pornographic content. Further, in the absence of any authorization, inter alia, from the Plaintiff, the Suit Videos could not have been uploaded on any platform including but not limited to the Defendant websites.
4. It is noteworthy that the unauthorised exploitation of the explicit video clippings and the hosting of the Suit Videos on pornographic

websites has prejudiced and adversely the Plaintiff's professional endeavours.

5. In view of the sensitive nature of the Suit Videos, the Plaintiff craves leave of this Hon'ble Court to consider the present suit which has been filed anonymously on behalf of the Plaintiff. Further, in the interest of justice and in order to protect the personal identity of the Plaintiff, the Plaintiff seeks retention of the pleadings, affidavits and documents filed in the present matter by this Hon'ble Court in a sealed cover. The Plaintiff also seeks exemption from serving the executed copy of the plaint along with documents filed along with the plaint on the Defendants. The Plaintiff craves leave of this Court to allow service of the plaint by allowing the Plaintiff to redact the name of the Series, personal details and/ or any other identifiable details of the Plaintiff prior to service on the Defendants.
6. The Plaintiff submits that in the event her identity is revealed through the present case, grave prejudice will be caused to Plaintiff. Further, the Plaintiff apprehends that in the event the Suit Video is served on the Defendants, the Plaintiff's right to be forgotten may not be given effect to.
7. The present application is being filed *bonafide* and in the interest of justice.

PRAYER

8. In light of the aforementioned facts and circumstances and submissions made, it is prayed that this Hon'ble Court be pleased to pass an order:-
 - a. Directing the Registry of this Hon'ble Court to retain the pleadings, affidavits and the documents filed along with the present plaint in a sealed cover;
 - b. Allowing the Plaintiff to anonymously pursue the present case against the Defendants;
 - c. Allowing the Plaintiff to serve a copy of the plaint along with the documents filed along with it after redacting the name of the Series, personal details and/ or any other identifiable details of the Plaintiff prior to service on the Defendants;And/or

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)

IA NO. OF 2021
 IN
 CS (OS) NO. OF 2021

IN THE MATTER OF:

X ...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors. ...Defendants

**APPLICATION UNDER SECTION 151 OF CPC, 1908 FOR
 EXEMPTION FROM FILING ORIGINAL, CERTIFIED, FAIR
 TYPED COPIES OF DIM/ PROPER MARGIN/ UNDERLINE/
 SINGLE LINE SPACING OF THE ANNEXURES.**

The Plaintiff submits as follows:

1. The present Suit is being filed seeking, *inter alia*, an order of permanent and mandatory injunction against the Defendants, directing them to remove the identified audio-visual content that form the subject matter of the suit (**Suit Videos**) and refrain from hosting or uploading the said videos on any digital or other platform.

2. This application is being filed by the Plaintiff seeking exemption from this Hon'ble Court from filing original certified copies, fair typed copies and the dim copies of the Annexures.
3. Due to the urgency in filing the present suit, the Plaintiff craves leave of this Hon'ble Court to exempt from filing original certified copies, fair typed copies and the dim copies of the Annexures/ documents and allow the filing of the present suit with the annexures/ documents accompanying the suit.
4. That this application is *bona fide* and is in the interest of justice, and is being filed owing to the urgency in the case.

PRAYER

5. It is therefore respectfully prayed that this Hon'ble Court be pleased to:
 - a. Exempt the Plaintiff from filing original certified copies, fair typed copies of the dim/ proper margining/ underline/ single spacing of the Annexures; and

1. The present Suit is being filed seeking, *inter alia*, an order of permanent and mandatory injunction against the Defendants, directing them to remove the identified audio-visual content that form the subject matter of the suit and refrain from hosting or uploading the said videos on any digital or other platform.
2. That the Plaintiff is filing the present Application seeking exemption from serving a notice to the statutory bodies under

section 80 of the Code of Civil Procedure, 1908, which have been made a party to the present proceeding.

3. That the Plaintiff has made the statutory bodies as a party to the present proceedings for the sole reason of ensuring compliance of this Hon'ble Court's order(s) which may be passed.
4. That the Plaintiff is seeking urgent reliefs from this Hon'ble Court, and prays for exemption from serving the Defendants a notice under Section 80 of the Code of Civil Procedure, 1908.

PRAYER

In view of the foregoing submissions, it is prayed that this Hon'ble Court be pleased to:

- a. Exempt the Plaintiff from serving a notice under section 80 of the Code of Civil Procedure 1908 to the Defendant; AND

IN THE HIGH COURT OF DELHI AT NEW DELHI

(Ordinary Original Jurisdiction)

C.S.(OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus


<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

**INDEX - III
(VAKALATNAMA)**

Sr. No.	Particulars	Page No.
1.	Index III (Vakalatnama)	1
2.	Vakalatnama	2 - 3
3.	Proof of Service along with Affidavit	4 - 7

THROUGH


 Abhishek Malhotra
 Advocate

Abhishek Malhotra

TMT Law Practice

Counsel for the Plaintiff

C-2/39, Lower Ground Floor,

Safdarjung Development Area,

New Delhi - 110016

E-mail: amalhotra@tmtlaw.co.in

Phone# 9971053888,9899597359

Place: New Delhi

Dated: August 16, 2021

VAKALATNAMA
IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY CIVIL JURISDICTION)
 CS (OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

KNOW all to whom these presents shall come that the Plaintiff herein, anonymously represented as 'X' do hereby appoint:

**ABHISHEK MALHOTRA (D/2681/1999), SAPNA CHAURASIA,
 NAOMI CHANDRA, AAHNA MEHROTRA (D/1943/2011),
 BAGMISIKHA PUHAN (F/600/2014), SHILPA GAMNANI (D/3877/2017),
 ATMAJA TRIPATHY (D/4666/2018), GURMUKH CHOUDHRI (D/4108
 /2018), SANYA DUA(D/2968/2018), SANYA SEHGAL(D/2682/2017),
 SAKSHI NAYAK(UP/2907/2018), SIDDHANT GUPTA(D/4488/2020),
 ANJALI TIWARI (D/2185/2019)
 ADVOCATES**

TMT Law Practice

Office: C-2/39, Safdarjung Development Area, New Delhi 110016
 Phone # 41682996

Hereinafter called the Advocates to be my/our Advocates, in the above-noted case and authorize them: -

To act, appear and plead in the above-noted case in this Court, or in any other Court in which the same may be tried or heard and in the appellate Courts including High Court.

To sign, file, verify and present pleadings replications, appeals cross-objections, or petitions for executions, review, revision, restoration, withdrawal, compromise, or other petitions, replies, objections, or affidavits or other documents as may be deemed necessary or proper for the prosecution of the said case in all its stages.

To file and take back documents.

To withdraw, or compromise said the case or submit to arbitration any difference or disputes that may arise touching or in any manner relating to the said case.

To take out execution proceedings.

V.D

From: Atmaja Tripathy <atmaja.tripathy@tmtlaw.co.in>
Sent: 16 August 2021 20:13
To: mca.rocfilling@relianceada.com; jyoti.jain@ril.com; Neelakantan.An@ril.com; ramanujan.veeraraghavan@sifycorp.com; bnswamy@sol.net.in; babukvb@sol.net.in; info@sol.net.in; nikunj@joister.net; rishabh.aditya@tatatel.co.in; compliance@tikona.in; rameshkrishnanaidu@gmail.com; corp.secretarial@videocon.com; accounts@vivacommunication.com; lakshmisree.chakraborty@vodafoneidea.com; Arun.Madhav@vodafoneidea.com; hcpant@bsnl.co.in; compliance.officer@bharti.in; amit.bhatia@airtel.com; ajay.singh@hathway.net; paresht4@gmail.com; heena.t4@gmail.com; amberonlineservices@gmail.com; corp@cityonlines.com; cs1@dil.in; cs@excitel.com; jobymathew@asianet.co.in; nishanaker01@rediffmail.com; suresh@hns.net.in; jithesh.chathambil@actcorp.in; venkatesh.trm@gmail.com; mtnlcsco@gmail.com; info@mynetworkindia.com; abusecomplaints@markmonitor.com; cprabhuram1979@gmail.com; secretarial@nettlinx.org; gopal.j@cloud4c.com; secretarial@infotelconnect.com; accounts@readylink.in; mohammedmuqem@gmail.com; abuse@dynadot.com; abuse@namecheap.com; abuse@danescenames.com; abuse@tldregistrarsolutions.com; domainabuse@cscglobal.com; abuse@web.com; abuse@nameshield.net; financecontroller@pioneerelabs.in; support-in@google.com
Cc: Abhishek Malhotra; Sikandar Pandit
Subject: Advance Service of Suit- Delhi High Court
Attachments: image003.png; Suit on behalf of X- Advance Service.pdf

Dear All:

We write on behalf of our client, Plaintiff in the captioned suit. Our client is filing the captioned suit before the Hon'ble Delhi High Court. Please note that the present suit is being served on all defendants who are arrayed to the captioned suit as Defendant Nos. 1 – 73, as and by way of advance service of the captioned suit on the Defendants.

The matter is likely to be listed before the Court on 19.08.2021.

This is for your information and necessary action.

Regards,

Atmaja

Atmaja Tripathy

Senior Associate,

TMT Law Practice

C-2/39 | Safdarjung Development

Area | New Delhi – 110016 | India



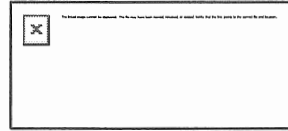
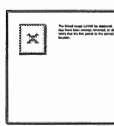
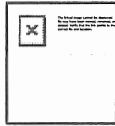
Tel: +91 11 41682996 | +91 11 26512813

5

Mobile: +91 7768060955

Email: atmaja.tripathy@tmtlaw.co.in

Website: www.tmtlaw.co.in



TMT Law Practice allows reasonable use of the e-mail system. Views and opinions expressed in these communications do not necessarily represent those of TMT Law Practice. This communication (including any attachments) is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. If you are not the intended recipient, any disclosure, copying, distribution or use of the contents of this communication is prohibited. If you have received this in error, please contact the sender immediately and delete this communication without copying.

True copy
AP

6

IN THE HIGH COURT OF DELHI AT NEW DELHI
(ORIGINAL ORDINARY JURISDICTION)

CS (OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

AFFIDAVIT OF SERVICE

I, Atmaja Tripathy, D/o Dr D Tripathy, aged about 26 years, having office at C-2/39, Safdarjung Development Area, New Delhi- 110016, do hereby solemnly affirm and declare as under:

1. That I am the Counsel for the Plaintiff and am well conversant with the facts and circumstances of the present case. I am competent to swear and depose the affidavit.
2. I say that on 16.08.2021, I served a copy of entire plaint, accompanying applications and documents by way of email on Defendant Nos. 1-73. The emails were delivered to the aforesaid Defendants and did not bounce back.
3. I say that I am not deposing falsely.


DEPONENT



VERIFICATION:

Verified at New Delhi on this 16th day of August, 2021, that the contents of Paragraphs 1 to 3 of my above affidavit are true to the best of my knowledge and nothing material has been concealed therefrom.

CERTIFIED THAT THE CONTENTS EXPLAINED TO THE
DEPONENT/EXECUTANT WHO IS SEEMED PERFECTLY TO
UNDERSTAND AFFIRMED & DEPOSED BEFORE ME AT NEW DELHI

IDENTIFY THE EXECUTANT/DEPONENT WHO HAS
SIGNED IN MY PRESENCE
NOTARY PUBLIC (NEW DELHI)
NAND KISHOR AGARWAL Advocate



16 AUG 2021



A handwritten signature of the deponent, appearing to be "Anuja", written in dark ink.

DEPONENT

IN THE HIGH COURT OF DELHI AT NEW DELHI
(*Ordinary Original Jurisdiction*)

C.S.(OS) NO. OF 2021

IN THE MATTER OF:

X

...Plaintiff

Versus

<https://www.youtube.com/watch?v=iQ6K5Z3zyS0> and Ors.

...Defendants

INDEX - IV
(LIST OF DOCUMENTS)

Sl. No.	Details of Documents and Parties	In the Possession/Power/Custody of:	Original/ Photocopy/Office Copy/ Printout	Mode of execution/Issuance of Receipt	Line of Custody	Page No.
1.	INDEX IV (Documents)					1 - 3
2.	Print out of list of URLs	Plaintiff	Print out	Printout of URL links	Plaintiff to Plaintiff's counsel	4 - 6
3.	Screenshots of Plaintiff's conversation with Ram Gopal Verma	Plaintiff	Printout	Downloaded from Plaintiff's phone and printed	Plaintiff to Plaintiff's counsel	7 - 11
4.	Order of the Delhi High Court in <i>Jorawer Singh Mundy v. Union of India and Ors.</i> , 2021	Plaintiff's Counsel	Printout	Printed from Court website	Plaintiff's counsel	12 - 13

	SCC Online Del 2306					
5.	Order of the Delhi High Court in <i>Zulfiqar Ahman Khan v. Quintillion Business Media Pvt Ltd and Ors.</i> , 2019 SCC Online Del 8494	Plaintiff's Counsel	Printout	Printed from Court website	Plaintiff's counsel	14 - 16
6.	Order of the Odisha High Court in <i>Subhranshu Rout v. State of Odisha</i> , 2020 SCC Online Ori 878	Plaintiff's Counsel	Printout	Printed from Court website	Plaintiff's counsel	17 - 24
7.	Order of Karnataka High Court in <i>Vasunathan v. Registrar General</i> , 2017 SCC Online Kar 424	Plaintiff's Counsel	Printout	Printed from Court website	Plaintiff's counsel	25 - 26
8.	Order of Madras High Court in WP(MD) No. 12015 of 2021	Plaintiff's Counsel	Printout	Printed from Court website	Plaintiff's counsel	27 - 32
9.	Judgment of the Delhi High Court in <i>UTV Software Communication Ltd. and Ors. v. 1337X.To and Others</i> , 2019 SCC Online Del 8002	Plaintiff's Counsel	Printout	Printed from Court website	Plaintiff's counsel	33 - 71

THROUGH



Abhishek Malhotra
Advocate

Abhishek Malhotra

TMT Law Practice

Counsel for the Plaintiff

C-2/39, Lower Ground Floor,

Safdarjung Development Area,

New Delhi - 110016

E-mail: amalhotra@tmtlaw.co.in

Phone# 9971053888, 9899597359

Place: New Delhi

Dated: August 16, 2021

List of URLs

1. <https://www.youtube.com/watch?v=iQ6K5Z3zyS0>
2. <https://www.youtube.com/watch?v=kLf5itQEC0M>
3. <https://www.youtube.com/watch?v=TYez5HliIkk>
4. <https://www.youtube.com/watch?v=bJ2gZA9MLr4>
5. <https://www.youtube.com/watch?v=8SNkrCM03B8>
6. <https://www.youtube.com/watch?v=H4BFZb2pBFk>
7. <https://www.youtube.com/watch?v=vKHa2UKGGrA>
8. <https://www.youtube.com/watch?v=sp8IsH2DK08>
9. https://www.youtube.com/watch?v=oiqvbrRf_B4
10. https://www.google.com/imgres?imgurl=https%3A%2F%2Fpbs.twimg.com%2Fmedia%2FCJXnIzLUAAAcLOX.jpg&imgrefurl=https%3A%2F%2Ftwitter.com%2Fonlinetollywood%2Fstatus%2F618654668130922497&tbnid=6-rlvu-PeiWa_M&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygCegQIARBa..i&docid=CsunT4DbPekRtM&w=594&h=402&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygCegQIARBa
11. https://www.google.com/imgres?imgurl=https%3A%2F%2Flookaside.fbsbx.com%2Flookaside%2Fcrawler%2Fmedia%2F%3Fmedia_id%3D935461176518216&imgrefurl=https%3A%2F%2Fwww.facebook.com%2FTilottama-Dutta-1436337886665570%2Flikes&tbnid=vKF_4yBfrP9O-M&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygBegQIARBY..i&docid=TS6VMycLrRJTBM&w=960&h=640&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygBegQIARBY
12. https://www.google.com/imgres?imgurl=https%3A%2F%2Flookaside.fbsbx.com%2Flookaside%2Fcrawler%2Fmedia%2F%3Fmedia_id%3D1436337886665570&imgrefurl=https%3A%2F%2Fm.facebook.com%2FTilottama-Dutta-1436337886665570%2F&tbnid=i4qL3SKJNFoXhM&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygDegQIARBC..i&docid=XmtyWGpHYgolfM&w=

724&h=724&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygDegQIARBc

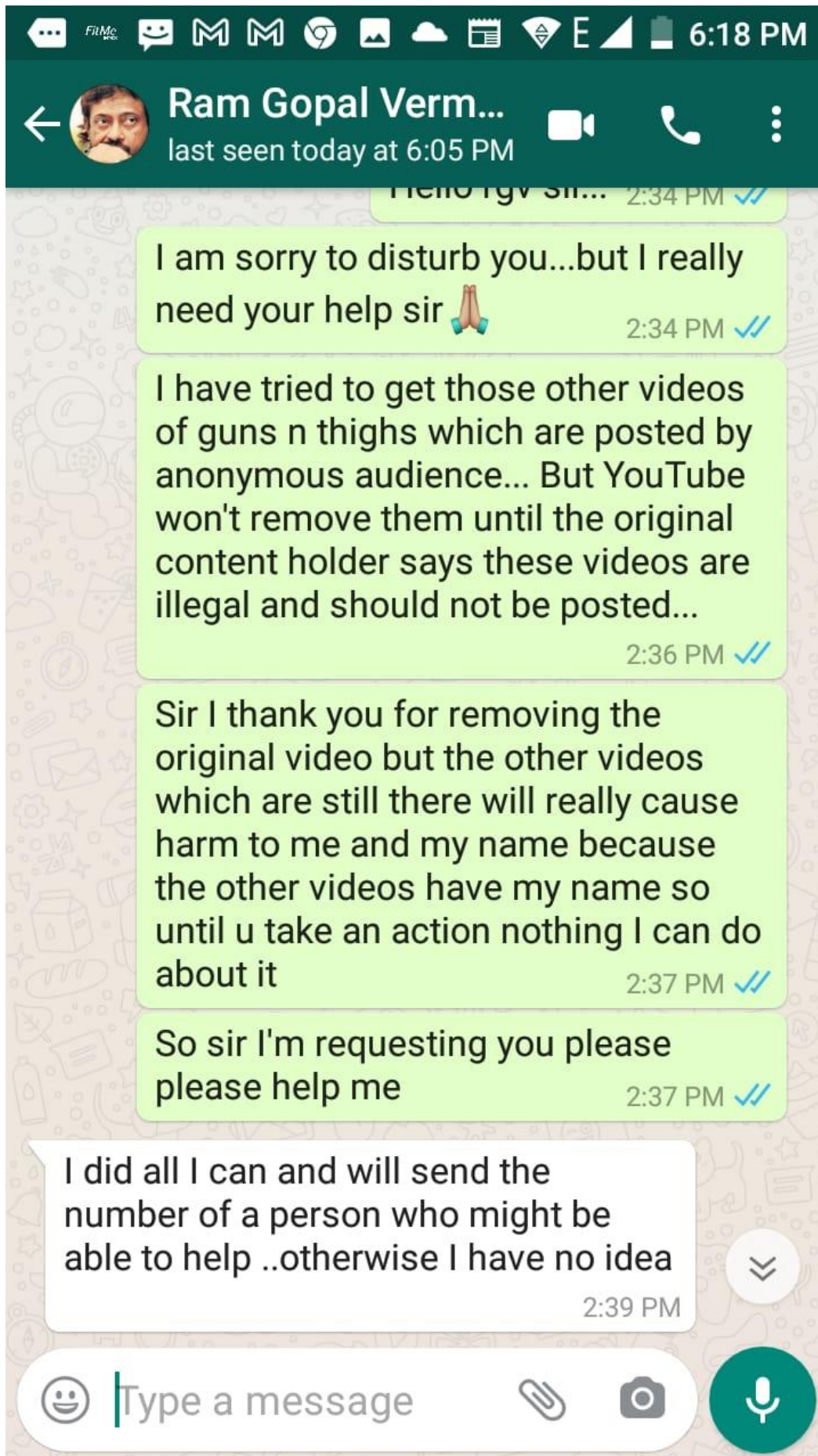
13. <https://www.google.com/imgres?imgurl=https%3A%2F%2Fwww.shorshe.com%2Fcelebrity%2Fposter%2F3%2F9%2F3981.jpg&imgrefurl=https%3A%2F%2Fwww.shorshe.com%2Fcelebrity%2Ftilottama-dutta-tilottoma-dutta.html&tbnid=HTZQOWM8iP2nzM&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygEegQIARBe..i&docid=e1GODwrjsaZPGM&w=150&h=231&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygEegQIARBe>
14. https://www.google.com/imgres?imgurl=https%3A%2F%2Flookaside.fbsbx.com%2Flookaside%2Fcrawler%2Fmedia%2F%3Fmedia_id%3D944938218903845&imgrefurl=https%3A%2F%2Fwww.facebook.com%2FTilottama-Dutta-1436337886665570%2Flikes&tbnid=Y64k3Y9c9Ew9YM&vet=12ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygJegQIARBq..i&docid=TS6VMycLrRJTBM&w=1800&h=1200&q=tilottama%20dutta&hl=en&authuser=1&ved=2ahUKEwiz26HU7sTxAhUKBrcAHfeBDVYQMygJegQIARBq
15. <https://mypornsnap.top/photos/tilottama-dutta>
16. <https://mypornsnap.top/photos/1/tilottama-dutta/hqdefault-jpg>
17. <https://mypornsnap.top/photos/2/tilottama-dutta/3981-jpg>
18. <https://mypornsnap.top/photos/3/tilottama-dutta/cjxnizluaaaclox-jpg>
19. <https://mypornsnap.top/photos/5/tilottama-dutta/maxresdefault-jpg>
20. <https://mypornsnap.top/photos/16/tilottama-dutta/hqdefault-jpg>
21. <https://www.fap.plus/content/indian-actress-tilottama-dutta-naked-in-guns-and-thighs-nsfw/1957912.shtml>
22. <https://xnxx.plus/ja/mov/indian-actress-tilottama-dutta-naked-in-guns-and-thighs-nsfw/109243.html>
23. <https://mobileporn4u.com/video/59922-indian-actress-tilottama-dutta-naked-in-guns-and-thighs-nsfw/>
24. <https://mobileporn4u.com/video/59923-indian-actress-tilottama-dutta-naked-in-guns-and-thighs-nsfw/>
25. https://daftsex.com/watch/-107646916_456248758

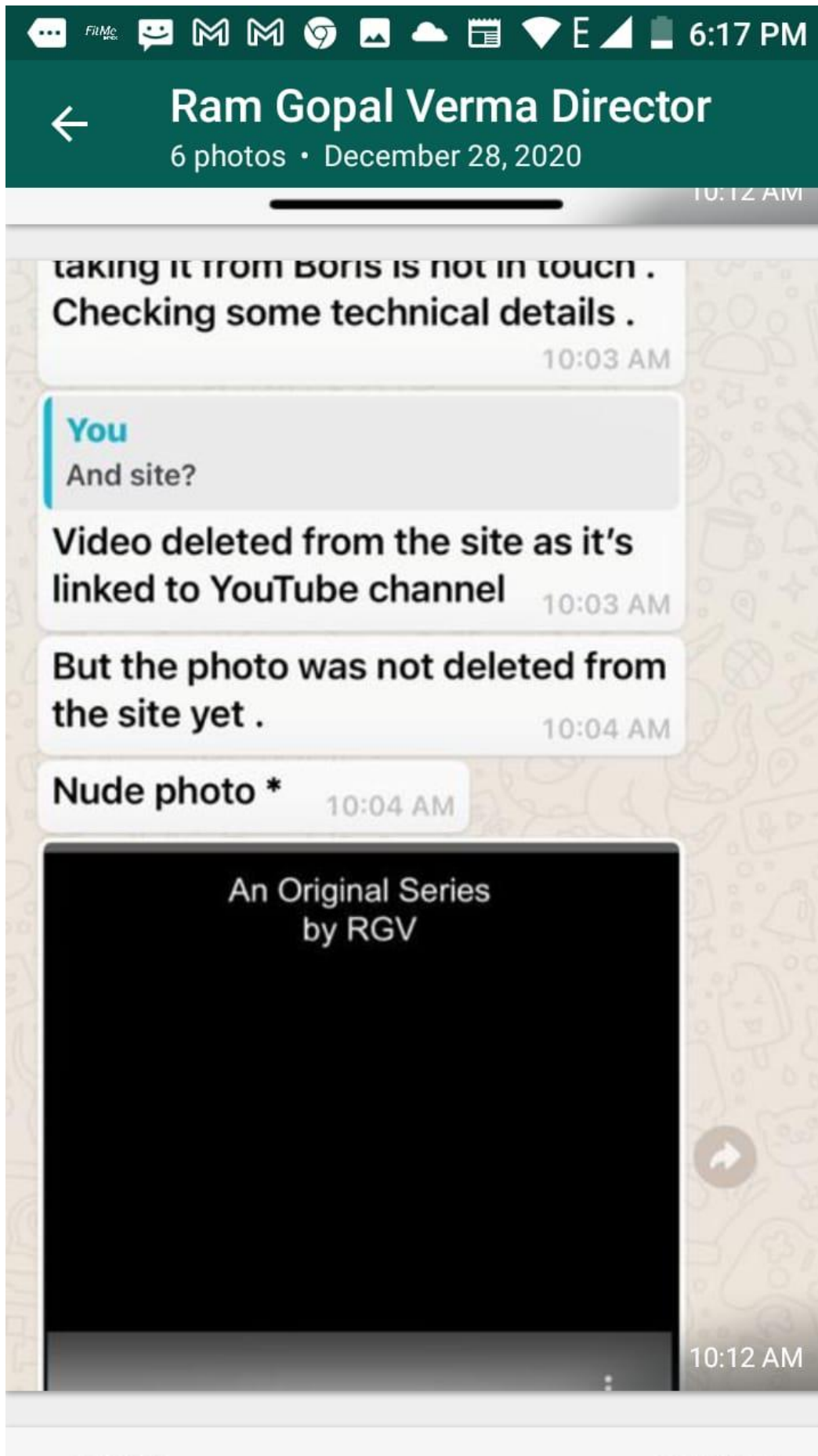
26. <https://hugetits.win/video/ViciousAmazingAfricanaugurbuzzard/>
 27. <https://www.reddit.tube/video/ff3554de124e31b7149f0ccb750ae36db2c20d5>

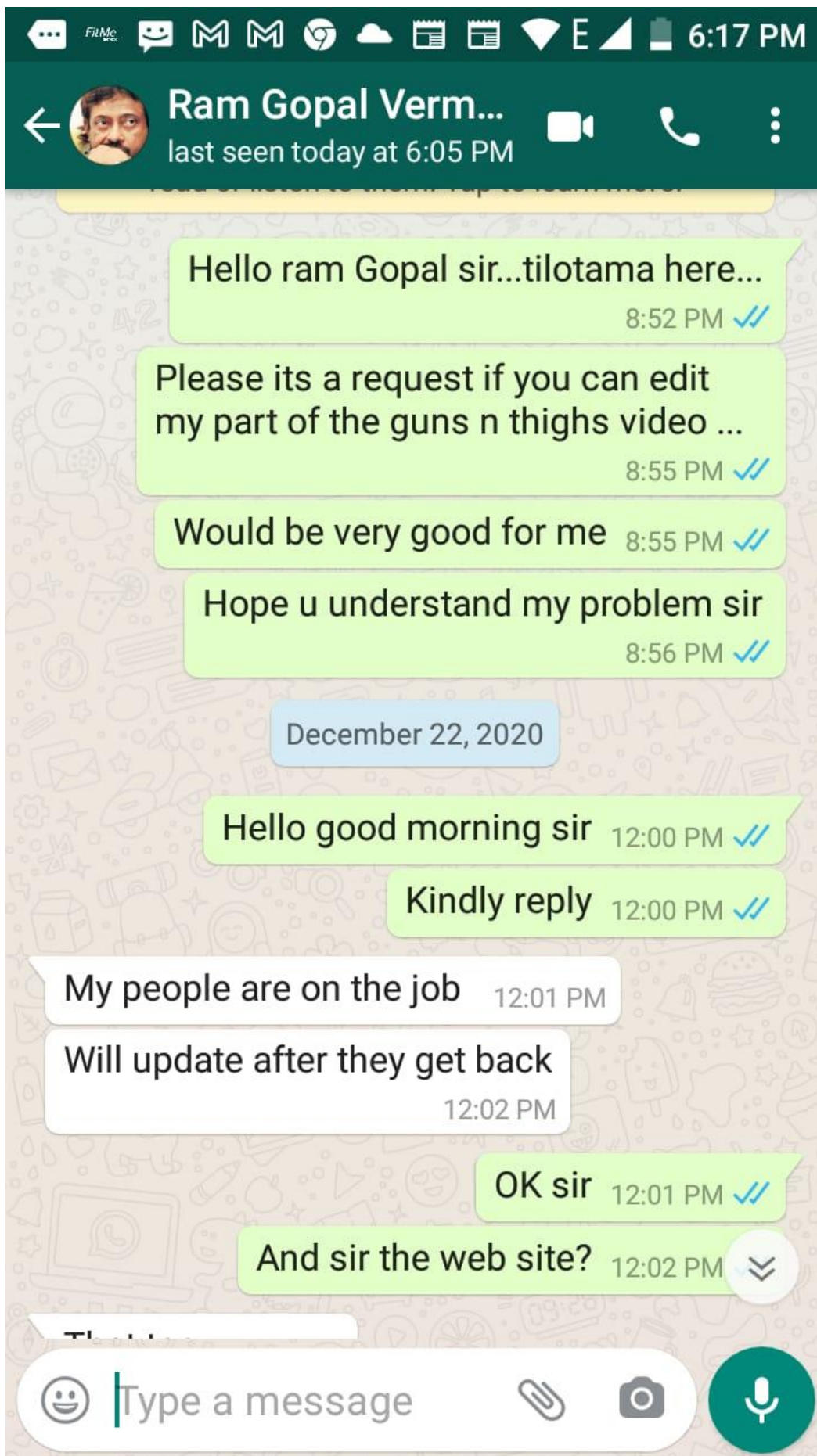
a

28. <https://greygif.com/tilotama-dutta-in-guns-amp-thighs>
 29. <https://pinkgif.com/tilotama-dutta-in-guns-amp-thighs>
 30. <https://xxxpornxvideos.com/xxxvid/ViciousAmazingAfricanaugurbuzzard/>
 31. <https://celegif.com/tilotama-dutta/>
 32. <https://adultseries.net/videos/tilotama-dutta-nude-guns-thighs-s01-trailer-2017/>
 33. <https://xxpdata.net/vid/ViciousAmazingAfricanaugurbuzzard/>
 34. <https://twitter.com/onlinetollywood/status/618654668130922497>
 35. <https://www.shorshe.com/celebrity/tilottama-dutta-tilottoma-dutta.html>
 36. <https://www.dailymotion.com/video/x68p5fa>











2021 SCC OnLine Del 2306

In the High Court of Delhi at New Delhi
(BEFORE PRATHIBA M. SINGH, J.)

Jorawar Singh Mundy ... Petitioner;

Versus

Union of India and Others ... Respondents.

W.P.(C) 3918/2021 & CM APPL. 11767/2021

Decided on April 12, 2021

Advocates who appeared in this case:

Mr. Sanjay Kumar, Advocate

Ms. Shiva Lakshmi, Advocate for R-1

The Order of the Court was delivered by

PRATHIBA M. SINGH, J.:— This hearing has been done through video conferencing.

2. The Petitioner prays for removal of the judgment in *Crl.A. No. 14/2013* titled *Custom v. Jorawar Singh Mundy* from the Respondents No. 2, 3, 4 and 5's platforms i.e. Google, Indian Kanoon and vLex.in.

3. The case of the Petitioner is that he is a professional of Indian origin but an American citizen by birth. He claims to be managing investments and dealing with portfolios of real estate etc. When he travelled in 2009 to India, a case under the Narcotics Drugs and Psychotropic Substances Act, 1985, was lodged against him. However, finally vide judgment dated 30th April, 2011, the trial court had acquitted him of all the charges. An appeal was filed challenging this order of the trial court, and vide judgment dated 29th January, 2013, a Id. Single Judge of this Court upheld his acquittal in *Crl.A. No. 14/2013* titled *Custom v. Jorawar Singh Mundy*.

4. Thereafter, the Petitioner is stated to have travelled back to the United States and pursued law at the University of San Diego School of Law. He then realised that he is facing a huge disadvantage due to the fact that the judgment rendered by this Court was available on a google search to any potential employer, who wanted to conduct his background verification before employing him. According to the Petitioner, despite him having had a good academic record, he is unable to get any employment to his expectations, and the reason for the same, according to him, is the availability of this judgment online.

5. The Petitioner then issued a legal notice to Respondent Nos. 2 to 5 i.e. Google India Private Ltd., Google LLC, Indian Kanoon and vLex.in. Respondent No. 5 i.e. vLex.in is stated to have removed the said judgment, however, the other platforms have not yet removed the same. The prayer in this writ petition is thus to direct the removal of the said judgment from all the Respondent platforms, recognizing the Right to Privacy of the Petitioner, under Article 21 of the Constitution.

6. Issue notice to the Respondents No. 1, 2, 3 and 4, returnable on 20th August, 2021.

7. Ms. Shivalakshi, Id. Counsel, accepts notice on behalf of Respondent No. 1, and submits that if this Court directs the removal of the said judgment, MEITY would accordingly issue directions to the said Respondents No. 2-4 platforms.

8. The question as to whether a Court order can be removed from online platforms is an issue which requires examination of both the Right to Privacy of the Petitioner on the one hand, and the Right to Information of the public and maintenance of transparency in judicial records on the other hand. The said legal issues would have to

be adjudicated by this Court.

9. The Right to Privacy is well recognized by the Supreme Court in the Constitution Bench judgment in *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1. In *Zulfiqar Ahman Khan v. Quintillion Businessman Media Pvt. Ltd.* this Court had examined this issue and while granting an interim order, this court had held as under:

"8. In fact, it is the submission of Id. counsel for the Plaintiff that the Plaintiff's personal and professional life has been hampered irreparably and further damage is likely to be caused if appropriate relief is not granted against the republication of these two articles. The original publisher having already agreed to pull down the same, this Court having directed that the same ought not to be republished, the Plaintiff, thus, has a right to ensure that the articles are not published on multiple electronic/digital platforms as that would create a permanent atmosphere of suspicion and animosity towards the Plaintiff and also severely prejudice his personal and professional life. The printouts of the articles from www.newsdogapp.com, which have been shown to the Court, leave no doubt in the mind of the Court that these are identical to the articles published on www.thequint.com, which have already been pulled down.

9. Accordingly, recognising the Plaintiff's Right to privacy, of which the 'Right to be forgotten' and the 'Right to be left alone' are inherent aspects, it is directed that any republication of the content of the originally impugned articles dated 12th October 2018 and 31st October 2018, or any extracts/or excerpts thereof, as also modified versions thereof, on any print or digital/electronic platform shall stand restrained during the pendency of the present suit.

10. The Plaintiff is permitted to communicate this order to any print or electronic platform including various search engines in order to ensure that the articles or any excerpts/search results thereof are not republished in any manner whatsoever. The Plaintiff is permitted to approach the grievance officers of the electronic platforms and portals to ensure immediate compliance of this order"

10. Recently, the Orissa High Court in *Subhranshu Rout v. State of Odisha* [BLAPL No. 4592/2020, decided on 23rd November, 2020], has also examined the aspect and applicability of the "Right to be forgotten" *qua* Right to Privacy, in a detailed manner including the international law on the subject.

11. It is the admitted position that the Petitioner was ultimately acquitted of the said charges in the case levelled against him. Owing to the irreparable prejudice which may be caused to the Petitioner, his social life and his career prospects, inspite of the Petitioner having ultimately been acquitted in the said case *via* the said judgment, *prima facie* this Court is of the opinion that the Petitioner is entitled to some interim protection, while the legal issues are pending adjudication by this Court.

12. Accordingly, Respondent Nos. 2 and 3 are directed to remove the said judgment dated 29th January 2013 in *CrI.A. No. 14/2013* titled *Custom v. Jorawar Singh Mundy* from their search results. Respondent No. 4 - Indian Kanoon is directed to block the said judgement from being accessed by using search engines such as Google/Yahoo etc., till the next date of hearing. Respondent No. 1 to ensure compliance of this order.

13. Let counter affidavit be filed by all the Respondents within four weeks. Rejoinder, thereto, if any, be filed within four weeks thereafter.

14. List on 20th August 2021.

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.

2019 SCC OnLine Del 8494 : (2019) 175 DRJ 660

In the High Court of Delhi at New Delhi
(BEFORE PRATHIBA M. SINGH, J.)

Zulfiqar Ahman Khan Plaintiff;
v.

Quintillion Business Media Pvt. Ltd. and Others Defendants.

CS (OS) 642/2018

Decided on May 9, 2019

Advocates who appeared in this case:

Mr. Abhishek Singh, Ms. Aayushi Mishra and Mr. Yatharth Kumar, Advocates. (M : 9910291290)

Mr. Prashant Kumar and Mr. Amit Singh, Advocates. (M : 9818934544)

The Judgment of the Court was delivered by

PRATHIBA M. SINGH, J. (Oral)

L.A. 17161/2018 (stay)

1. The present suit has been filed by the Plaintiff seeking permanent injunction against Defendant No. 1-Quintillion Business Media Pvt. Ltd., Defendant No. 2-its editor as also Defendant No. 3 - the author, who had written two articles against the Plaintiff on the basis of harassment complaints claimed to have been received by them, against the Plaintiff, as part of the #MeToo campaign. The three individuals, who made allegations against the Plaintiff, have remained anonymous and have not revealed their identity in the public domain. The stories, which had appeared on 12th October, 2018 as also on 31st October, 2018 were impugned in the present suit and an injunction was sought against the publication and re-publication of the said two articles.

2. The Plaintiff claims that he is a well-known personality in the media industry and he is currently the Managing Director of a media house. It is his case that due to publication of the stories on Defendant No. 1's digital/electronic platform www.quint.com, he underwent enormous torture and personal grief due to the baseless allegations made against him. The grievance of the Plaintiff was that he ought to have been given sufficient notice prior to the publication of the impugned articles and by not doing so, the defendants published one-sided accounts which resulted in tarnishment of his reputation.

3. The suit was listed on 14th December, 2018 on which date the Court had directed that the said two articles would not be republished till the next date. On 19th December, 2018, the Defendants had entered appearance and had submitted that without prejudice to the Defendants' rights, they would pull down/take down the two publications. The following order was then passed.

"CS (OS) 642/2018 & L.A. No. 1 7161/2018 (u/o XXXIX R 1 & 2 CPC)

The present suit has been filed by the Plaintiff seeking a permanent and mandatory injunction restraining the Defendants from continuing to publish two articles dated 12th October, 2018 and 31st October, 2018 on the website www.thequint.com.

The case of the Plaintiff is that two articles were published against him on the basis of harassment allegations claimed to have been received from individuals as part of the '#Me Too' campaign.

The suit was listed on 14th December, 2018 on which date the Defendants had

entered appearance after receiving an advance copy from the Plaintiff. On the said date, the counsel for the Defendants sought time to file a short affidavit explaining the position. The affidavit has been placed on record yesterday and both the parties have made their submissions partly.

Learned counsel for the Defendants, submits that without prejudice to the rights of the Defendants, while the matter is being heard and in view of the ensuing vacations, they are willing to pull down the said two publications against the plaintiff. Ld. Counsel submits that the first article dated 12th October, 2018 has already been pulled down and the second article dated 31st October, 2018 would be pulled down within 24 hours.

Taking the said statement on record, the matter is adjourned to 23rd January, 2019 for conclusion of arguments.

The order dated 14th December, 2018 that the contents of the said two articles which were published on the website www.thequint.com shall not be republished shall continue in the meantime.

The original interim reply which is stated to have been filed by the Defendants be placed on record by the Registry before the next date.

Any rejoinder, if the Plaintiff wishes to file, may be filed at least two days before the next date. Dasti."

4. Thereafter, the matter came up for hearing on 23rd January, 2019, whereby the Defendant submitted that it would adhere to the directions passed by this Court on 19th December, 2018. Further, liberty was granted to the Plaintiff to point out any further platforms where the article was published, and the Defendant was directed to apprise the said platforms of the order passed by the Court. Further, time was granted to the parties to complete their pleadings. Thereafter, vide order dated 15th April, 2019, time was given to the Plaintiff to seek instructions if he wished to press his claim for damages and the matter was listed for today.

5. It has been pointed today by Id. counsel for the Plaintiff that the contents of the said two articles, which were originally published on the Defendant No. 1's digital/electronic portal www.thequint.com, have now been picked up by another platform by the name www.newsdogapp.com and the same are being attributed to Defendant No. 1. The content on the said app www.newsdogapp.com is identical to the articles, which were published on the Defendant No. 1's website www.thequint.com and in fact, attributes the source as being www.thequint.com. Printouts of the same have been handed over to the Court and to Id. counsel for the Defendants.

6. The matter was initially passed over in order to enable the Defendants to seek instructions. Ld. counsel for the Defendants submits that the impugned articles have already been taken down from the portal www.thequint.com and whenever the Plaintiff has pointed out any other digital/electronic platform or website where the said articles have been reproduced, the Defendants have cooperated with the Plaintiff for pulling the same down.

7. The Defendants having been the original source of the said two publications and having already pulled down the said articles pursuant to the proceedings of this Court, the republication of the same, attributing it to any of the Defendants, would not be permissible. The allegations having been made as part of #MeToo campaign and the three individuals having chosen to remain anonymous and the publisher of the articles having already agreed to pull down the said two articles, further re-publication of the same is liable to be restrained. The campaign also ought not to become an unbridled and unending campaign against an individual with other electronic/digital portals or platforms picking up the pulled down content through archived material. The #MeToo campaign cannot become a 'Sullyng #UToo' campaign forever. If re-publication is permitted to go on continuously, the Plaintiff's rights would be severely jeopardised.

8. In fact, it is the submission of Id. counsel for the Plaintiff that the Plaintiff's personal and professional life has been hampered irreparably and further damage is likely to be caused if appropriate relief is not granted against the republication of these two articles. The original publisher having already agreed to pull down the same, this Court having directed that the same ought not to be republished, the Plaintiff, thus, has a right to ensure that the articles are not published on multiple electronic/digital platforms as that would create a permanent atmosphere of suspicion and animosity towards the Plaintiff and also severely prejudice his personal and professional life. The printouts of the articles from www.newsdogapp.com, which have been shown to the Court, leave no doubt in the mind of the Court that these are identical to the articles published on www.thequint.com, which have already been pulled down.

9. Accordingly, recognising the Plaintiff's Right to privacy, of which the '*Right to be forgotten*' and the '*Right to be left alone*' are inherent aspects, it is directed that any republication of the content of the originally impugned articles dated 12th October 2018 and 31st October 2018, or any extracts/or excerpts thereof, as also modified versions thereof, on any print or digital/electronic platform shall stand restrained during the pendency of the present suit.

10. The Plaintiff is permitted to communicate this order to any print or electronic platform including various search engines in order to ensure that the articles or any excerpts/search results thereof are not republished in any manner whatsoever. The Plaintiff is permitted to approach the grievance officers of the electronic platforms and portals to ensure immediate compliance of this order.

11. If the said search engines do not take down/remove the objectionable content from their platforms within a period of 36 hours after receiving communication from the Plaintiff with a copy of this order, the Plaintiff is also permitted to communicate with the Defendants so that the Defendants can also cooperate in the said pulling down, if required. If the said platforms do not, after being served by a copy of this order, take down the objectionable content, the Plaintiff is given liberty to approach this court forthwith - apart from approaching the appropriate authorities under the Information Technology Act.

CS (OS) 642/2018

12. List on 1st August, 2019 for further proceedings.

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.

2020 SCC OnLine Ori 878

In the High Court of Orissa at Cuttack
(BEFORE S.K. PANIGRAHI, J.)

Subhranshu Rout ... Petitioner;
Versus

State of Odisha ... Opposite Party.

BLAPL No. 4592 of 2020¹

Decided on November 23, 2020, [Date of Hearing : 20.10.2020]

Advocates who appeared in this case:

For petitioner : Shri Bibhuti Bhusan Behera and S. Bahadur, Advocates

For the Opp. Party : Shri Manoj Kumar Mohanty, Additional Standing Counsel

The Judgment of the Court was delivered by

S.K. PANIGRAHI, J.:— The present application is preferred under Section 439 of the Criminal Procedure Code, 1973 in connection with G.R. Case No. 171 of 2020 arising out of Rasol P.S. Case No. 62 of 2020, pending in the Court of learned SDJM, Hindol registered for the commission of offences punishable under Sections 376, 292, 465, 469, 509 of IPC read with Sections 66, 66(C), 67, 67(A) of the I.T. Act, 2000.

2. The factual conspectus as set forth in the F.I.R. is that on 03.05.2020 one Rupali Amanta, D/o. Raghunath Amanta of Village-Giridharprasad, P.S. Rasol, District-Dhenkanal alleged that for a period of about one year, she had been in love with the petitioner. Both the petitioner as well as the accused were village mates and classmates. On the day of last Kartika Puja, the petitioner went to the house of the informant and taking advantage of the fact that she was alone he committed rape on the informant and recorded the gruesome episode in his mobile phone. When the informant warned petitioner that she would apprise her parents of the brutal incident and its serious undertones, the petitioner threatened to kill her as well as to make viral the said photos/videos. Further, she has alleged that since 10.11.2019, the petitioner had maintained physical intimacy with the informant. Upon the informant narrating the incident to her parents, the petitioner opened a fake Facebook ID in the name of the informant and uploaded all the objectionable photos using the said ID in order to further traumatize her. Though the informant disclosed the said fact to the IIC, Rasol P.S. by way of a written complaint on 27.04.2020, the Police has failed to take any step on the said complaint and thereby portrayed unsoundness of the police system. After much difficulty, finally, the informant could get the present FIR lodged.

3. Learned counsel for the petitioner submits that both the victim and accused are adults and hence they know the best what is right or wrong. He submits that the petitioner is an ITI Diploma holder who is in search of a job and hence his detention will spoil his career. He further stated that the petitioner is interested to marry the victim girl unconditionally.

4. Per contra, learned counsel for the State submits that the petitioner had not only forcibly committed sexual intercourse with the victim girl, but he had also deviously recorded the intimate sojourn and uploaded the same on a fake Facebook account created by the Petitioner in the name of the victim girl. The allegation is very serious since there is specific allegation of forced sexual intercourse by the accused/petitioner against the will of the victim. Statement recorded under Section 161 of Cr. P.C. of the victim girl also clearly divulges the fact that the petitioner has been threatening and blackmailing her stating that if she discloses these facts to anybody, he would eliminate her and also make her intimate scenes viral on the social media. He further

submits that the investigation of the case has not yet been completed. The entire allegation in the FIR as well as the statement recorded under Section 161 of Cr.P.C read with other materials available on records are a pointer to the fact that the crime committed by the petitioner are serious in nature. The victim has been at the receiving end of an unabated mental torture due to the blackmailing tactics used by the petitioner.

5. While examining the pages of the case records, prima facie, it appears that the petitioner has uploaded the said photos/videos on a social media platform i.e. Facebook and with the intervention of the police, after some days, he deleted the said objectionable contents from the Facebook. In fact, the information in the public domain is like toothpaste, once it is out of the tube one can't get it back in and once the information is in the public domain it will never go away. Under the Indian Criminal Justice system a strong penal action is prescribed against the accused for such heinous crime but there is no mechanism available with respect to the right of the victim to get the objectionable photographs deleted from the server of the Facebook. The different types of harassment, threats and assaults that frighten citizens in regard to their online presence pose serious concerns for citizens. There is an unprecedented escalation of such insensitive behavior on the social media platforms and the victim like the present one could not get those photos deleted permanently from server of such social media platforms like facebook. Though the statute prescribes penal action for the accused for such crimes, the rights of the victim, especially, her right to privacy which is intricately linked to her right to get deleted in so far as those objectionable photos have been left unresolved. There is a widespread and seemingly consensual convergence towards an adoption and enshrinement of the right to get deleted or forgotten but hardly any effort has been undertaken in India till recently, towards adoption of such a right, despite such an issue has inexorably posed in the technology dominated world. Presently, there is no statute in India which provides for the right to be forgotten/getting the photos erased from the server of the social media platforms permanently. The legal possibilities of being forgotten on line or off line cries for a widespread debate. It is also an undeniable fact that the implementation of right to be forgotten is a thorny issue in terms of practicality and technological nuances. In fact, it cries for a clear cut demarcation of institutional boundaries and redressal of many delicate issues which hitherto remain unaddressed in Indian jurisdiction. The dynamics of hyper connectivity -the abundance, pervasiveness and accessibility of communication network have redefined the memory and the prescriptive mandate to include in the technological contours is of pressing importance.

6. However, this instant issue has attracted sufficient attention overseas in the European Union leading to framing of General Data Protection Regulation (GDPR) which governs the manner in which personal data can be collected, processed and erased. The aspect of right to be forgotten appears in Recitals 65 and 66 and in Article -17 of the GDPR¹, which vests in the victim a right to erasure of such material after due diligence by the controller expeditiously. In addition to this, Article 5 of the GDPR requires data controllers to take every reasonable step to ensure that data which is inaccurate is "erased or rectified without delay". Every single time, it cannot be expected that the victim shall approach the court to get the inaccurate data or information erased which is within the control of data controllers such as Facebook or Twitter or any other social media platforms.

7. A similar issue was raised in England in the Wales High Courts in *NT1 and NT2 v. Google LLC*² which ordered Google to delist search results referring to the spent conviction of a businessman known as NT2 but rejected a similar request made by a second businessman, NT1. The claimants therein had been convicted of certain criminal offences many years ago who complained that search results returned by

Google featured links to third-party reports about the convictions in the past which were either inaccurate and/or old, irrelevant and of no public interest or otherwise an illegitimate interference with their rights. The reliefs sought in those cases were based on the prevailing data protection laws and English Law principles affording protection in case of tortuous misuse of private information. The Court rejected NT1's request based on the fact that he was a public figure with a role in public life and thus the crime and its punishment could not be considered of a private nature. In contrast, the Court upheld NT2's delisting claim with the reasoning that his crime did not involve dishonesty. His punishment had been based on a plea of guilt, and information about the crime and its punishment had become out of date, irrelevant and of no sufficient legitimate interest to users of Google to justify its continued availability³.

8. In the case of *Google Spain SL v. Agencia Espanola de Protection de Datos (AEPD)*⁴ the European Court of Justice ruled that the European citizens have a right to request that commercial search engines, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant. The Court in that case ruled that the fundamental right to privacy is greater than the economic interest of the commercial firm and, in some circumstances; the same would even override the public interest in access to information. The European Court in the aforesaid case had affirmed the judgment of the Spanish Data Protection Agency (SPDA) in a case which concerned a proceeding relating to bankruptcy which had ordered removal of material from the offending website by recognizing a qualified right to be forgotten and held that an individual was entitled to have Google de-list information of which he complained.

9. Recently, the European Court of Justice, in *Google LLC v. CNIL*⁵ ruled that "currently there is no obligation under EU law, for a search engine operator to carry out such a de-referencing on all the versions of its search engine". The Court also said that the search operator must "take sufficiently effective measures" to prevent searches for differenced information from within the EU. The court specifically held as under:

"69. That regulatory framework thus provides the national supervisory authorities with the instruments and mechanisms necessary to reconcile a data subject's rights to privacy and the protection of personal data with the interest of the whole public throughout the Member States in accessing the information in question and, accordingly, to be able to adopt, where appropriate, a de-referencing decision which covers all searches conducted from the territory of the Union on the basis of that data subject's name.

70. In addition, it is for the search engine operator to take, if necessary, sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights. Those measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name (see, by analogy, judgments of 27 March 2014, UPC Telekabel Wien, C-314/12, EU : C : 2014 : 192, paragraph 62, and of 15 September 2016, McFadden, C-484/14, EU : C : 2016 : 689, paragraph 96).

71. It is for the referring court to ascertain whether, also having regard to the recent changes made to its search engine as set out in paragraph 42 above, the measures adopted or proposed by Google meet those requirements.

72. Lastly, it should be emphasized that, while, as noted in paragraph 64 above, EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of

fundamental rights (see, to that effect, judgments of 26 February 2013, Åkerberg Fransson, C-617/10, EU : C : 2013 : 105, paragraph 29, and of 26 February 2013, Melloni, C-399/11, EU : C : 2013 : 107, paragraph 60), a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine.

73. In the light of all of the foregoing, the answer to the questions referred is that, on a proper construction of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 and Article 17(1) of Regulation 2016/679, where a search engine operator grants a request for dereferencing pursuant to those provisions, that operator is not required to carry out that dereferencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request."

10. Presently, there is no statute which recognizes right to be forgotten but it is in sync with the right to privacy, which was hailed by the Apex Court as an integral part of Article 21 (right to life) in *K.S. Puttaswamy (Privacy-9J.)*⁴. However, the Ministry of Law and Justice, on recommendations of Justice B.N. Srikrishna Committee, has included the *Right to be forgotten* which refers to the ability of an individual to limit, delink, delete, or correct the disclosure of the personal information on the internet that is misleading, embarrassing, or irrelevant etc. as a statutory right in Personal Data Protection Bill, 2019. The Supreme Court in *K.S. Puttaswamy (Privacy-9J.)* has held right to be let alone as part of essential nature of privacy of an individual. The relevant paras of the judgment are as under:

"XXXXX

R. Essential nature of privacy

297. What, then, does privacy postulate? Privacy postulates the reservation of a private space for the individual, described as the right to be let alone. The concept is founded on the autonomy of the individual. The ability of an individual to make choices lies at the core of the human personality. The notion of privacy enables the individual to assert and control the human element which is inseparable from the personality of the individual. The inviolable nature of the human personality is manifested in the ability to make decisions on matters intimate to human life. The autonomy of the individual is associated over matters which can be kept private. These are concerns over which there is a legitimate expectation of privacy. The body and the mind are inseparable elements of the human personality. The integrity of the body and the sanctity of the mind can exist on the foundation that each individual possesses an inalienable ability and right to preserve a private space in which the human personality can develop. Without the ability to make choices, the inviolability of the personality would be in doubt. Recognizing a zone of privacy is but an acknowledgment that each individual must be entitled to chart and pursue the course of development of personality. Hence privacy is a postulate of human dignity itself. Thoughts and behavioural patterns which are intimate to an individual are entitled to a zone of privacy where one is free of social expectations. In that zone of privacy, an individual is not judged by others. Privacy enables each individual to take crucial decisions which find expression in the human personality. It enables individuals to preserve their beliefs, thoughts, expressions, ideas,

ideologies, preferences and choices against societal demands of homogeneity. Privacy is an intrinsic recognition of heterogeneity, of the right of the individual to be different and to stand against the tide of conformity in creating a zone of solitude. Privacy protects the individual from the searching glare of publicity in matters which are personal to his or her life. Privacy attaches to the person and not to the place where it is associated. Privacy constitutes the foundation of all liberty because it is in privacy that the individual can decide how liberty is best exercised. Individual dignity and privacy are inextricably linked in a pattern woven out of a thread of diversity into the fabric of a plural culture.

XXXXXXX

402. "Privacy" is "[t]he condition or state of being free from public attention to intrusion into or interference with one's acts or decisions" [Black's Law Dictionary (Bryan Garner Edition) 3783 (2004)]. The right to be in this condition has been described as "the right to be let alone" [Samuel D. Warren and Louis D. Brandeis, "The Right To Privacy", 4 Harv L Rev 193 (1890)]. What seems to be essential to privacy is the power to seclude oneself and keep others from intruding it in any way. These intrusions may be physical or visual, and may take any of several forms including peeping over one's shoulder to eavesdropping directly or through instruments, devices or technological aids.

XXXXXXX

479. Both the learned Attorney General and Shri Sundaram next argued that the right to privacy is so vague and amorphous a concept that it cannot be held to be a fundamental right. This again need not detain us. Mere absence of a definition which would encompass the many contours of the right to privacy need not deter us from recognising privacy interests when we see them. As this judgment will presently show, these interests are broadly classified into interests pertaining to the physical realm and interests pertaining to the mind. As case law, both in the US and India show, this concept has travelled far from the mere right to be let alone to recognition of a large number of privacy interests, which apart from privacy of one's home and protection from unreasonable searches and seizures have been extended to protecting an individual's interests in making vital personal choices such as the right to abort a foetus; rights of same sex couples-including the right to marry; rights as to procreation, contraception, general family relationships, child-bearing, education, data protection, etc. This argument again need not detain us any further and is rejected.

XXXXXXX

560. The most popular meaning of "right to privacy" is-"the right to be let alone". In *Gobind v. State of M.P.* [*Gobind v. State of M.P.*, (1975) 2 SCC 148 : 1975 SCC (Cri) 468], K.K. Mathew, J. noticed multiple facets of this right (paras 21 -25) and then gave a rule of caution while examining the contours of such right on case-to-case basis.

XXXXXXX

636. Thus, the European Union Regulation of 2016 [Regulation No. (EU) 2016/679 of the European Parliament and of the Council of 27-4-2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive No. 95/46/EC (General Data Protection Regulation).] has recognised what has been termed as "the right to be forgotten". This does not mean that all aspects of earlier existence are to be obliterated, as some may have a social ramification. If we were to recognise a similar right, it would only mean that an individual who is no longer desirous of his personal data to be processed or stored, should be able to remove it from the system where the personal data/information is no longer necessary, relevant, or is

incorrect and serves no legitimate interest. Such a right cannot be exercised where the information/data is necessary, for exercising the right of freedom of expression and information, for compliance with legal obligations, for the performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims. Such justifications would be valid in all cases of breach of privacy, including breaches of data privacy."

The Hon'ble Apex court while considering the issue of a conflict between the right to privacy of one person and the right to a healthy life of another person has held that, in such situations, the right that would advance public interest would take precedence."

(emphasis supplied)

11. The Hon'ble Supreme Court of India in the case of *Mr. 'X' v. Hospital 'Z'*² has recognized an individual's right to privacy as a facet Article 21 of the Constitution of India. It was also pertinently held that the right which would advance the public morality or public interest would alone be enforced through the process of court, for the reason that moral considerations cannot be kept at bay and the Judges are not expected to sit as mute structures of clay in the halls known as the courtroom, but have to be sensitive, "in the sense that they must keep their fingers firmly upon the pulse of the accepted morality of the day."

12. The Ld. Single Judge of High Court of Karnataka in the case of *Vasunathan v. The Registrar General, High Court of Karnataka*⁸ has acknowledged the right to be forgotten, keeping in line with the trend in the Western countries where it is followed as a matter of rule. The High Court of Delhi in its recent judgment in *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.*² has also recognized the "right to be forgotten" and 'Right to be left alone' as an integral to part of individual's existence. The Karnataka High Court in *(Name Redacted) v. The Registrar General*¹⁰ recognized "Right to be forgotten" explicitly, though in a limited sense. The petitioner's request to remove his daughter's name from a judgment involving claims of marriage and forgery was upheld by the Court. It held that recognizing right to be forgotten would parallel initiatives by 'western countries' which uphold this right when 'sensitive' cases concerning the 'modesty' or 'reputation' of people, especially women, were involved. However, the High Court of Gujarat in *Dharamraj Bhanushankar Dave v. State of Gujarat*¹¹, in a case involving the interpretation of the rules of the High Court has taken a contrary and narrow approach.

13. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, India's first legal framework recognized the need to protect the privacy of personal data, but it failed to capture the issue of the "Right to be forgotten". The Hon'ble Supreme Court of India in the case of *K.S. Puttaswamy v. Union of India* (supra) held that purpose limitation is integral for executive projects involving data collection - unless prior permission is provided, third parties cannot be provided access to personal data¹². This principle is embodied in S.5 of the yet-to-be-implemented Personal Data Protection Bill, 2019. Purpose Limitation enhances transparency in data processing and helps examine the proportionality of the mechanism used to collect data for a specific purpose. Moreover, it prevents the emergence of permanent data 'architectures' based on interlinking databases without consent. In the present case the proposition of purpose limitation is not applicable as the question of seeking consent does not arise at all. No person much less a woman would want to create and display gray shades of her character. In most of the cases, like the present one, the women are the victims. It is their right to enforce the right to be forgotten as a *right in rem*. Capturing the images and videos with consent of the

woman cannot justify the misuse of such content once the relation between the victim and accused gets strained as it happened in the present case. If the right to be forgotten is not recognized in matters like the present one, any accused will surreptitiously outrage the modesty of the woman and misuse the same in the cyber space unhindered. Undoubtedly, such an act will be contrary to the larger interest of the protection of the woman against exploitation and blackmailing, as has happened in the present case. The sloganeering of "betibachao" and women safety concerns will be trampled.

14. Section 27 of the draft Personal Data Protection Bill, 2018 contains the right to be forgotten. Under Section 27, a data principal (an individual) has the right to prevent continuing disclosure of personal data by a data fiduciary. The aforesaid provision which falls under Chapter VI (Data Principal Rights) of the Bill, distinctly carves out the "right to be forgotten" in no uncertain terms. In terms of this provision, every data principal shall have the right to restrict or prevent continuing disclosure of personal data (relating to such data principal) by any data fiduciary if such disclosure meets any one of the following three conditions, namely if the disclosure of personal data:

- (i) has served the purpose for which it was made or is no longer necessary; or
- (ii) was made on the basis of the data principal's consent and such consent has since been withdrawn; or (iii) was made contrary to the provisions of the bill or any other law in force.

15. In addition to this, Section 10 of the Bill provides that a data fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed. Further, it imposes an obligation on every data fiduciary to undertake periodic reviews in order to determine whether it is necessary to retain the personal data in its possession. If it is not necessary for personal data to be retained by a data fiduciary, then such personal data must be deleted in a manner as may be specified.

16. In the instant case, prima facie, it appears that the petitioner has not only committed forcible sexual intercourse with the victim girl, but has also deviously recorded the intimate sojourn and uploaded the same on a fake Facebook account. Statement recorded under Section 161 of Cr. P.C. of the victim girl is also clearly in sync with FIR version. Considering the heinousness of the crime, the petitioner does not deserve any consideration for bail at this stage. However, this Court is of the view that Indian Criminal Justice system is more of a sentence oriented system with little emphasis on the disgorgement of victim's loss and suffering, although the impact of crime on the victim may vary significantly for person(s) and case(s)-- for some the impact of crime is short and intense, for others the impact is long-lasting. Regardless, many victims find the criminal justice system complex, confusing and intimidating. Many do not know where to turn for help. As in the instant case, the rights of the victim to get those uploaded photos/videos erased from Facebook server still remain unaddressed for want of appropriate legislation. However, allowing such objectionable photos and videos to remain on a social media platform, without the consent of a woman, is a direct affront on a woman's modesty and, more importantly, her right to privacy. In such cases, either the victim herself or the prosecution may, if so advised, seek appropriate orders to protect the victim's fundamental right to privacy, by seeking appropriate orders to have such offensive posts erased from the public platform, irrespective of the ongoing criminal process.

17. In view of the foregoing discussion of the case, this Court is not inclined to enlarge the petitioner on bail. Hence, the present bail application stands dismissed.

[†] (In the matter of an application under Section 439, Criminal Procedure Code, 1973)

¹ The data subject shall have the right to obtain from the controller regarding the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.

² [2018] EWHC 799 (QB).

³ Para 223 of Judgment

⁴ C-131/12[2014] Q.B. 1022

⁵ Case C-507/17

⁶ (2017) 10 SCC 1

⁷ (1998) 8 SCC 296

⁸ 2017 SCC OnLine Kar 424

⁹ (2019) 175 DRJ 660

¹⁰ Writ Petition (Civil) Nos. 36554-36555/2017 decided on 4th January, 2018

¹¹ Special Civil Appln. No. 1854 of 2015, order dated 19-1-2017 (Guj)

¹² See Para 166 of K.S. Puttaswamy Judgment

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.

Writ Petition No. 62038 of 2016 (GM-RES)

Vasunathan v. Registrar General

2017 SCC OnLine Kar 424

In the High Court of Karnataka at Bengaluru
(BEFORE ANAND BYRAREDDY, J.)

Sri. Vasunathan, S/o V. Kandagang, Aged about 51 years,
Resident of No. 1/550, TPN Garden, K. Chettipalyam,
Dharapuram Road, Tirupur-641 608, Tamil Nadu Petitioner
Shri. Amar Correa, Advocate

v.

1. The Registrar General, High Court of Karnataka, Bengaluru-560 001.
2. State of Karnataka, By the Police Inspector, W & M Squad, CCB, N.T. Pet, Bengaluru-560 002.
3. Sri. Srinivas G., S/o Girithamaih, Aged about 28 years, Nataraja Gurukula, Somanahalli, III Block, Kanakapura Road, Bengaluru-560 062.
4. Kum. Pallavi Manohar, D/o late Manohar, Aged about 42 years, No. 136, O.B. Chodahalli, Udaypura Post, Bengaluru-560 082.
5. Kum. Swamini Mala, D/o R. Rudrappa, Aged about 45 years, Resident of Nataraja Gurukula, Somanahalli, III Block, Kanakapura Road, Bengaluru-560 062 Respondents
Shri. R Anitha, Government Pleader for Respondents 1 and 2

Writ Petition No. 62038 of 2016 (GM-RES)¹

Decided on January 23, 2017

ORDER

ANAND BYRAREDDY, J.:— Heard the learned counsel for the petitioner and the learned Government Advocate.

2. The present petition is filed in the following background:

On the basis of a First Information Report lodged by the daughter of this petitioner, a case in Crime No. 376/2014 was registered and investigation was taken up for offences punishable under Sections 463, 468, 469, 471, 366, 387 and 120B read with Section 34 of the Penal Code, 1860 and on conclusion of the investigation, a charge-sheet was filed.

3. In the meantime, the daughter of this petitioner had instituted a civil suit in O.S. No. 168/2014 on the file of the City Civil Judge, Bangalore, seeking a declaration that there was no marriage between her and the defendant in the said suit, and to annul the marriage certificate issued by the Sub-Registrar. There was also a prayer for grant of perpetual injunction restraining the defendant therein from claiming any marital rights on her on the basis of the said certificate of marriage.

4. The defendant therein had entered appearance and the parties ultimately entered into a compromise and the suit was decreed in terms of the compromise petition on 6.3.2015. One of the terms of the compromise was that the daughter of the petitioner should withdraw her complaint resulting in registration of the aforesaid criminal case and should also request to the police to close the case and that she had

undertaken not to pursue the said prosecution but extend all co-operation for termination of the complaint.

5. Pursuant to the said decree, the accused in the said Criminal case preferred a petition, i.e., CrI.P. 1599/2015 before this court under Section 482 Cr.P.C. seeking that the proceedings be quashed in respect of the criminal case in C.C. No. 6881/2015 on the file of the II Additional Chief Metropolitan Magistrate, Bangalore. The daughter of the petitioner herein was shown as Respondent No. 2 in the said petition before this court and her identity along with the address was specified in the causetitle as was required procedurally. The petitioner's daughter having appeared before this court along with the petitioner herein - her father, this court by its order dated 15.06.2015 after discussing the entire background, quashed the proceedings in C.C. No. 6881/2015 referred to above. The name of the petitioner's daughter and identity details are indicated in the cause-title to the said petition as Respondent No. 2.

6. It is the apprehension of the petitioner's daughter that if a name-wise search is carried on by any person through any of the internet service providers such as google and yahoo, this order may reflect in the results of such a search and therefore, it is to the grave apprehension of the petitioner's daughter that if her name should be reflected in such a search by chance on the public domain, it would have repercussions even affecting the relationship with her husband and her reputation that she has in the society and therefore is before this court with a special request that the Registry be directed to mask her name in the cause-title of the order passed in the petition filed by her husband - accused in Criminal Petition No. 1599/2015, disposed of on 15.06.2015. Further, if her name is reflected anywhere in the body of the order apart from the causetitle, the Registry shall take steps to mask her name before releasing the order for the benefit of any such oilier service provider who may seek a copy of the orders of this court.

7. However, it is made clear that insofar as the High Court website is concerned, there need not be any such steps taken. Therefore, if a certified copy of the order is applied for, the name of the petitioner's daughter would certainly be reflected in the copy of the order.

8. It should be the endeavour of the Registry to ensure that any internet search made in the public domain, ought not to reflect the petitioner's daughter's name in the causetitle of the order or in the body of the order of this court in CrI.P. No. 1599/2015 disposed of on 15.06.2015

9. This would be in line with the trend in the Western countries where they follow this as a matter of rule "Right to be forgotten" in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned. The petition is disposed of accordingly.

¹ This Writ Petition filed under Articles 226 and 227 of the Constitution of India praying to direct Respondent No. 1 to remove the name of the daughter of the petitioner, in the digital records maintained by the High Court, as indicated in the rank of Respondent No. 2 in order dated 15.06.2015 passed by this court in CrI.P. No. 1599/2015, to the extent of the same not being visible for the search engine including google or other search engines.

W.P.(MD).No.12015 of 2021

W.P.(MD).No.12015 of 2021

N.ANAND VENKATESH,J.

Mr.K.Samidurai, learned counsel takes notice for the respondents 1 to 3.

2. The petitioner faced criminal proceedings for an offence under Sections 417 and 376 of I.P.C., and he was convicted and sentenced by the Trial Court by Judgment dated 29.09.2011. The petitioner took this Judgment on appeal before this Court and this Court after dealing with the merits of the case and exhaustively dealing with the law governing the case, acquitted the petitioner from all charges in a Judgment made in Crl.A.(MD).No.321 of 2011, dated 30.04.2014. By virtue of this Judgment, the petitioner has been acquitted from all charges and the petitioner can no more be identified as an accused in the eye of law.

3. Today, the world is literally under the grips of social media. The background of a person is assessed by everyone by entering into the

Google search and collecting the information. There is no assurance that the information that is secured from the Google is authentic. However, it creates the first impression and depending upon the data that is provided, it will make or mar the characteristics of a person in the eyes of the Society. Therefore, in today's world everyone is trying to portray himself or herself in the best possible way, when it comes to social media. This is a new challenge faced by the World and already everyone is grappling to deal with this harbinger of further complexities awaiting mankind.

4. The petitioner is now facing a very peculiar problem. Even though the petitioner had been acquitted from all the charges, his name gets reflected in the Judgment rendered by this Court and unfortunately, whoever types the name of the petitioner in Google search is able to access the Judgment of this Court. In the entire Judgment, the petitioner is identified as an accused even though he has been ultimately acquitted from all charges. According to the petitioner, this causes a serious impact on the reputation of the petitioner in the eyes of the Society and therefore, the petitioner wants his name to be redacted from the Judgment of this Court.

W.P.(MD).No.12015 of 2021

5. It is brought to the notice of this Court that the Central Government is in the process of finalising the Data Protection Bill 2019 and it is yet to come into effect. This Act when brought into force will effectively protect the data and privacy of a person.

6. Till now, the Legislature has enacted laws protecting the identity of victims, who are women and children and their names are not reflected in any order passed by a Court. Therefore, automatically their names get redacted in the order and no one will be able to identify the person, who is a victim in a given case. This sufficiently protects the person and privacy of the person. This right has not been extended to an accused person, who ultimately is acquitted from all charges. In spite of an order of acquittal, the name of the accused person gets reflected in the order. Therefore, for the first time, a person, who was acquitted of all charges has approached this Court and sought for redacting his name from the Judgment passed by this Court.

7. For the present, this Court can act upon the request made by the petitioner only by placing reliance upon Article 21 of the Constitution

W.P.(MD).No.12015 of 2021

of India. After the historic Judgment of the Hon'ble Supreme Court in ***Puttasamy Vs. Union of India***, the Right of Privacy has now been held to be a fundamental right, which is traceable to Article 21 of the Constitution of India. If the essence of this Judgment is applied to the case on hand, obviously even a person, who was accused of committing an offence and who has been subsequently acquitted from all charges will be entitled for redacting his name from the order passed by the Court in order to protect his Right of Privacy. This Court finds that there is a *prima facie* case made out by the petitioner and he is entitled for redacting his name from the Judgment passed by this Court in Crl.A. (MD).No.321 of 2011. However, since the issue has come up for the first time before this Court, this Court wants to hear the learned counsel appearing on behalf of the respondents 1 to 3 and also the Members of the Bar and understand the various ramifications before writing a detailed Judgment on this issue.

8. It is also brought to the notice of this Court that when a similar issue came up before the Delhi High Court recently, interim orders were passed directing the concerned websites to redact the name

W.P.(MD).No.12015 of 2021

of the petitioner therein. It is also informed to this Court that a new Right called as Right to be Forgotten is sought to be included in the list of Rights that are already available under Article 21 of the Constitution of India.

9. The learned counsel for the respondents 1 to 3 shall take necessary instructions and file written submissions after serving a copy to the learned counsel appearing for the petitioner.

10. Registry is directed to post this case for final arguments on 28.07.2021 at 2.15 P.M.. Registry is further directed to publish this order in the Advocate Associations and Bar Associations both in the Principal Bench and Madurai Bench. The members of the Bar are requested to assist this Court in this issue.

16.07.2021

tsg

NOTE: In view of the present lock down owing to COVID-19 pandemic, a web copy of the order may be utilized for official purposes, but, ensuring that the copy of the order that is presented is the correct copy, shall be the responsibility of the advocate/litigant concerned.

W.P.(MD).No.12015 of 2021

N.ANAND VENKATESH,J.,

tsg

Order made in
W.P.(MD).No.12015 of 2021

16.07.2021

2019 SCC OnLine Del 8002 : (2019) 78 PTC 375

In the High Court of Delhi at New Delhi
(BEFORE MANMOHAN, J.)

CS(COMM) 724/2017 & I.As. 12269/2017, 12271/2017, 6985/2018, 8949/2018 AND
16781/2018

UTV Software Communication Ltd. and Others Plaintiffs.

v.

1337X.To and Others Defendants.

With

CS(COMM) 768/2018 & I.As. 4329/2018, 4331/2018, 10396/2018 AND 16782/2018

UTV Software Communications Ltd. and Others Plaintiffs.

v.

Bmovies. IS and Others Defendants.

And

CS(COMM) 770/2018 & I.As. 4358/2018, 4360/2018, 10402/2018 and 16785/2018

UTV Software Communications Ltd. and Others Plaintiffs.

v.

Fmovies. PE and Others Defendants.

And

CS(COMM) 776/2018 & I.As. 4546/2018, 4548/2018, 10404/2018 and 16779/2018

UTV Software Communications Ltd. and Others Plaintiffs.

v.

Rarbg. IS and Others Defendants.

And

CS(COMM) 777/2018 & I.As. 4549/2018, 4551/2018, 10405/2018 and 16786/2018

UTV Software Communications Ltd. and Others Plaintiffs.

v.

Thepiratebay. Org and Others Defendants.

And

CS(COMM) 778/2018 & I.As. 4552/2018, 4554/2018, 10406/2018 and 16783/2018

Twentieth Century Fox Film Corporation and Others Plaintiffs.

v.

YTS.AM and Others Defendants.

And

CS(COMM) 799/2018 & I.As. 4914/2018, 4916/2018, 10401/2018 and 16780/2018

UTV Software Communications Ltd. and Others Plaintiffs.

v.

Extratorrent. AG and Others Defendants.

And

CS(COMM) 800/2018 & I.As. 4917/2018, 4919/2018, 9732/2018 and 16784/2018

UTV Software Communications Ltd. and Others Plaintiffs.

v.

Torrentmovies. Co. and Others Defendants.

CS(COMM) 724/2017, I.As. 12269/2017, 12271/2017, 6985/2018, 8949/2018 and
16781/2018, CS(COMM) 768/2018, I.As. 4329/2018, 4331/2018, 10396/2018 and
16782/2018, CS(COMM) 770/2018, I.As. 4358/2018, 4360/2018, 10402/2018 and
16785/2018, CS(COMM) 776/2018, I.As. 4546/2018, 4548/2018, 10404/2018 and
16779/2018, CS(COMM) 777/2018, I.As. 4549/2018, 4551/2018, 10405/2018 and

16786/2018, CS(COMM) 778/2018, I.As. 4552/2018, 4554/2018, 10406/2018 and
16783/2018, CS(COMM) 799/2018, I.As. 4914/2018, 4916/2018, 10401/2018 and
16780/2018, CS(COMM) 800/2018 and I.As. 4917/2018, 4919/2018, 9732/2018 and
16784/2018

Decided on April 10, 2019, [Reserved on: 26th February, 2019]

Advocates who appeared in this case :

Mr. Saikrishna Rajagopal, Advocate with Ms. Suhasini Raina, Ms. Gitanjali Mathew and Ms. Disha Sharma, Advocates

Mr. Hemant Singh, Advocate as Amicus Curiae with Ms. Mamta Jha, Advocate.

Mr. Tanvir Nayar, Advocate with Mr. Ramnish Khanna, Advocate for D-8.

Mr. Abhishek Bakshi, Advocate for defendant No. 10.

Ms. Suruchi Thapar, Advocate with Mr. Ajay Kumar, Advocate for defendant No. 19.

Mr. K.R. Sasiprabhu, Advocate with Mr. Aditya Shandilya and Mr. Tushar Bhardwaj, Advocates for Reliance Jio Ltd.

Mr. Ruchir Mishra, Advocate with Mr. Mukesh Kr. Tiwari, Advocate for defendants No. 25 and 26.

Mr. Saikrishna Rajagopal, Advocate with Ms. Suhasini Raina, Ms. Gitanjali Mathew and Ms. Disha Sharma, Advocates

Mr. Hemant Singh, Advocate as Amicus with Ms. Mamta Jha, Advocate.

Mr. Ramnish Khanna, Advocate for Bharti Airtel Ltd.-D-6.

Mr. Tanvir Nayar, Advocate with Mr. Abhishek Bakshi, Advocate for defendant No. 11.

Mr. A.P. Sahay, CGSC with Mr. Suraj Kumar, Advocate for UOI. Mr. K.R. Sasiprabhu, Advocate with Mr. Aditya Shandilya and Mr. Tushar Bhardwaj, Advocates for Reliance Jio Ltd.

Mr. Vineet S. Shrivastawa, Advocate for defendant No. 20.

Mr. T.N. Durga Prasad, Advocate with Mr. Gagan Kumar, Advocate for Atria Convergence Technologies.

Mr. Saikrishna Rajagopal, Advocate with Ms. Suhasini Raina, Ms. Gitanjali Mathew and Ms. Disha Sharma, Advocates

Mr. Hemant Singh, Advocate as Amicus Curiae with Ms. Mamta Jha, Advocate.

Mr. Ramnish Khanna, Advocate for Bharti Airtel Ltd./D-6.

Mr. Ajay Dignpaul, CGSC with Ms. Madhuri Dhingra, Advocates for Union of India.

Mr. Tanvir Nayar, Advocate with Mr. Abhishek Bakshi, Advocate for defendant No. 9.

Mr. K.R. Sasiprabhu, Advocate with Mr. Aditya Shandilya and Mr. Tushar Bhardwaj, Advocates for Reliance Jio Ltd.

Mr. T.N. Durga Prasad, Advocate with Mr. Gagan Kumar, Advocate for Atria Convergence Technologies.

Mr. Vineet S. Shrivastawa, Advocate for defendant No. 18.

Mr. Saikrishna Rajagopal, Advocate with Ms. Suhasini Raina, Ms. Gitanjali Mathew and Ms. Disha Sharma, Advocates

Mr. Hemant Singh, Advocate as

Amicus Curiae with Ms. Mamta Jha, Advocate.

Mr. Ramnish Khanna, Advocate for Bharti Airtel Ltd./D-6.

Mr. Vivek Goyal, Advocate with Mr. Pawan Pathak, Advocate for UOI.

Mr. Tanvir Nayar, Advocate with Mr. Abhishek Bakshi, Advocate for defendant No. 9.

Mr. K.R. Sasiprabhu, Advocate with Mr. Aditya Shandilya and Mr. Tushar Bhardwaj, Advocates for Reliance Jio Ltd.

Mr. T.N. Durga Prasad, Advocate with Mr. Gagan Kumar, Advocate for Atria Convergence Technologies.

Mr. Vineet S. Shrivastawa, Advocate for defendant No. 18.

Mr. Saikrishna Rajagopal, Advocate with Ms. Suhasini Raina, Ms. Gitanjali Mathew and Ms. Disha Sharma, Advocates

Mr. Hemant Singh, Advocate as Amicus Curiae with Ms. Mamta Jha, Advocate.

Mr. Ramnish Khanna, Advocate for Bharti Airtel Ltd./D-6.

Mr. Tanvir Nayar, Advocate with Mr. Abhishek Bakshi, Advocate for defendant No. 9.

Mr. K.R. Sasiprabhu, Advocate with Mr. Aditya Shandilya and Mr. Tushar Bhardwaj, Advocates for

Reliance Jio Ltd.

Mr. T.N. Durga Prasad, Advocate with Mr. Gagan Kumar, Advocate for Atria Convergence Technologies.

Mr. Vineet S. Shrivastawa, Advocate for defendant No. 18.

Mr. Akshay Makhija, Advocate with Mr. Ankit Tyuagi, Advocate for defendants No. 24 and 25.

Mr. Saikrishna Rajagopal, Advocate with Ms. Suhasini Raina, Ms. Gitanjali Mathew and Ms. Disha Sharma, Advocates

Mr. Hemant Singh, Advocate as Amicus Curiae with Ms. Mamta Jha, Advocate.

Mr. Ramnish Khanna, Advocate for Bharti Airtel Ltd./D-6.

Mr. K.R. Sasiprabhu, Advocate with Mr. Aditya Shandilya and Mr. Tushar Bhardwaj, Advocates for Reliance Jio Ltd.

Mr. Tanvir Nayar, Advocate with Mr. Abhishek Bakshi, Advocate for defendant No. 10.

Mr. T.N. Durga Prasad, Advocate with Mr. Gagan Kumar, Advocate for Atria Convergence Technologies.

Mr. Vineet S. Shrivastawa, Advocate for defendant No. 20.

Mr. Saikrishna Rajagopal, Advocate with Ms. Suhasini Raina, Ms. Gitanjali Mathew and Ms. Disha Sharma, Advocates

Mr. Hemant Singh, Advocate as Amicus Curiae with Ms. Mamta Jha, Advocate.

Mr. Ramnish Khanna, Advocate for Bharti Airtel Ltd./D-6.

Mr. K.R. Sasiprabhu, Advocate with Mr. Aditya Shandilya and Mr. Tushar Bhardwaj, Advocates for Reliance Jio Ltd.

Mr. Tanvir Nayar, Advocate with Mr. Abhishek Bakshi, Advocate for defendant No. 9.

Mr. T.N. Durga Prasad, Advocate with Mr. Gagan Kumar, Advocate for Atria Convergence Technologies.

Mr. Vineet S. Shrivastawa, Advocate for defendant No. 18.

Ms. Shiva Lakshmi, CGSC with Mr. Siddharth Singh, Advocate for UOI.

Mr. Saikrishna Rajagopal, Advocate with Ms. Suhasini Raina, Ms. Gitanjali Mathew and Ms. Disha Sharma, Advocates

Mr. Hemant Singh, Advocate as Amicus Curiae with Ms. Mamta Jha, Advocate.

Mr. Ramnish Khanna, Advocate for Bharti Airtel Ltd.

Mr. Ajay Dignipaul, CGSC with Ms. Madhuri Dhingra, Advocates for Union of India.

Mr. Tanvir Nayar, Advocate with Mr. Abhishek Bakshi, Advocate for defendant No. 9.

Mr. K.R. Sasiprabhu, Advocate with Mr. Aditya Shandilya and Mr. Tushar Bhardwaj, Advocates for Reliance Jio Ltd.

Mr. Vineet S. Shrivastawa, Advocate for defendant No. 18.

Mr. T.N. Durga Prasad, Advocate with Mr. Gagan Kumar, Advocate for Atria Convergence Technologies.

The Judgment of the Court was delivered by

MANMOHAN, J.

"Whoops! The web is not the web we wanted in every respect"

Tim Berners-Lee, Inventor of Web.

1. It is rare that in an ex-parte matter questions of law of general public importance arise for consideration. However, in the present batch of ex-parte matters the following seminal issues arise for consideration:—

(A) Whether an infringer of copyright on the internet is to be treated differently from an infringer in the physical world?

(B) Whether seeking blocking of a website dedicated to piracy makes one an opponent of a free and open internet?

(C) What is a 'Rogue Website'?

(D) Whether the test for determining a 'Rogue Website' is a qualitative or a quantitative one?

(E) Whether the defendant-websites fall in the category of 'Rogue Websites'?

(F) Whether this Court would be justified to pass directions to block the 'Rogue Websites' in their entirety?

(G) How should the Court deal with the 'hydra headed' 'Rogue Websites' who on being blocked,

actually multiply and resurface as redirect or mirror or alphanumeric websites?

BRIEF FACTS

2. The present eight suits have been filed by the plaintiffs primarily seeking injunction restraining infringement of copyright on account of defendants communicating to the public the plaintiffs' original content/cinematographic works without authorization. The reliefs sought by the plaintiffs can broadly be classified as under: —

- a) Permanent injunction restraining the defendants from hosting, communicating, making available, etc. the original content of the plaintiffs on their website.
- b) Order directing Internet Service Providers (hereinafter referred to as "ISPs") to block access to the websites of the defendants.
- c) Order directing Registrars of the defendant-websites to disclose the contact details and other relevant details of the registrants.

3. The plaintiffs are companies, who are engaged in the business of creating content, producing and distributing cinematographic films around the world including in India.

4. Four classes of defendants have been impleaded in the present matters, namely: —

- i. Certain identifiable websites that are unauthorizedly publishing and communicating the Plaintiffs' copyrighted works. In the present batch of eight suits filed by the plaintiffs, thirty websites have been arrayed as defendants. The list of identifiable infringing websites arrayed as defendants in the present suits are: —

UTV Software Communications Ltd. v. 1337x.to CS(COMM) 724/2017

Domain	Uniform Resource Locator (URL)	Internet Protocol (IP) Address
1337x.to	http://1337x.to https://1337x.to	104.31.16.3. 104.31.17.3
Torrentz2.eu	https://torrentz2.eu	104.27.134.181 104.27.135.181

UTV Software Communications Ltd. v. Bmovies.is CS(COMM) 768/2018

Domain	URL	IP Address
bmovies.to	https://bmovies.to	104.31.86.38 104.31.87.38
bmovies.is	https://bmovies.is	104.24.98.151
fmovies.is	https://fmovies.is	87.120.36.22
fmovies.se	https://www1.fmovies.se/	104.31.17.3
fmovies.to	http://fmovies.to	87.120.36.22
bmovies.se	https://bmovies.se	104.24.112.4 104.24.113.4

UTV Software Communications Ltd. & Ors. Fmovies.pe and Ors. CS(COMM) 770/2018

Domain	URL	IP Address
fmovies.pe	https://fmovies.pe	104.24.18.88 104.24.19.88
fmovies.io	http://fmovies.io	192.162.138.17
fmovies.taxi	http://fmovies.taxi	104.27.143.24 104.27.142.24
bmovies.pro	https://bmovies.pro	104.31.71.201 104.31.70.201
bmovies.ru	http://bmovies.ru	104.24.108.89 104.24.109.89
fmovies.world	http://fmovies.world	104.27.131.168

UTV Software Communications Ltd. v. Rarbg.is CS(COMM) 776/2018

Domain	URL	IP Address
rarbg.is	https://rarbg.is	185.37.100.123
rarbg.com	http://rarbg.com	185.37.100.121
rarbg.to	https://rarbg.to	185.37.100.122
rarbgproxy.org	http://rarbgproxy.org	104.31.78.172

UTV Software Communications Ltd. v. thepiratebay.org CS(COMM) 777/2018'

Domain	URL	IP Address	
thepiratebay.org	https://thepiratebay.org	104.27.216.28	104.27.217.28
thepiratebay.se	http://thepiratebay.se	2002:6709:4c08::1	

UTV Software Communications Ltd. v. Yts.am CS(COMM) 778/2018

Domain	URL	IP Address
yts.am	https://yts.am	104.25.56.102 104.25.55.102
yts.ag	https://yts.ag	217.23.11.96
yts.tw	https://yts.tw	104.24.114.185 104.24.115.185
yts.altorrente.com	http://yts.altorrente.com	104.24.101.34 104.24.100.34
yts-yify.gold	http://yts-yify.gold	104.24.108.74 104.24.109.74
yts.gy	https://yts.gy	104.31.66.177 104.31.67.177
yify.is	http://yify.is	104.31.65.94 104.31.64.94

UTV Software Communications Ltd. v. Extratorrent.ag CS(COMM) 799/2018

Domain	URL	IP Address
extratorrent.ag	https://extratorrent.ag	104.27.186.160 104.27.187.160
torrentz.ht	http://torrentz.ht	104.28.14.154 104.28.15.154

UTV Software Communications Ltd. v. Torrentmovies.pe CS(COMM) 800/2018

Domain	URL	IP Address
torrentmovies.co	http://torrentmovies.co/	104.28.30.70

- ii. *John Doe Defendants* who are hitherto unknown parties engaged in the unauthorized communication of the plaintiffs' copyrighted works and include the registrants of the defendant-websites, uploaders, creators of the redirect/mirror/alphanumeric websites etc.
 - iii. *ISPs* that provide internet access, enabling users to visit any website online, including the defendant-websites.
 - iv. *Government Department/Agency*, namely Department of Telecommunication (hereinafter referred to as "DoT") and Ministry of Electronics & Information Technology (hereinafter referred to as "MEITY") who have been impleaded to assist in notifying ISPs to disable access to defendant-websites within India and implementing the orders passed by this Court.
5. Even according to the plaintiffs, the ISPs and the Government Agencies are not involved in committing any infringement but have been impleaded for the purpose of evolving an effective and balanced relief that adequately redresses the plaintiffs' concerns and also protects the public interest, if any.

6. Keeping in view the fact that the contesting defendants had been proceeded ex-parte and substantial question of law of general public importance arose for consideration, this Court deemed it appropriate to appoint Mr. Hemant Singh, who is a regular practitioner in IPRs cases, as the learned Amicus Curiae to assist the Court.

ARGUMENTS ON BEHALF OF LEARNED COUNSEL FOR PLAINTIFFS

7. Mr. Saikrishna Rajgopal, learned counsel for the plaintiffs stated that the infringing websites named in the present batch of matters allow 'streaming' and 'downloading' of copyrighted content of the plaintiffs, enabling the users to watch, download as well as share copies of such works. According to him, the defendants' business model is supported by revenue generated through advertisements, which are displayed on their websites.

8. Learned counsel for the plaintiffs pointed out that the plaintiffs had engaged the services of an investigator Mr. Manish Vaishampayan, who works as Manager of Content Protection at Motion Picture Distributors Association, Mumbai. The said investigator had filed affidavits in all the suits in which he stated that he had monitored the defendant-websites in respect of some of the

copyrighted movies of the plaintiffs. The evidence that had been collated in the form of screenshots and printouts from the infringing websites had been provided to the plaintiffs via a cloud link in conformity with Section 65B of the Indian Evidence Act, 1872. The investigator in his affidavit had further stated that the defendant-websites act in the following manner:—

- Allow direct download of the plaintiffs' copyrighted content and they provide searchable indexes along with curated lists of top movies, television shows etc.
- The plaintiffs' copyrighted content was available on the websites.
- The dates of upload of the content were unknown.
- Identities of the said websites were masked under the garb of privacy. o Indexes of hyperlinks redirect the end-user to the host site in order to facilitate streaming or downloading of copyrighted content of the plaintiffs.

9. Mr. Saikrishna Rajagopal, learned counsel for plaintiffs contended that the substantial purpose of the defendant-websites is to infringe or facilitate the infringement of copyright of the plaintiffs.

10. It is also the case of the plaintiffs that if one impugned websites is blocked, several other mirror websites are created which contain the infringing content. In some cases, the names of these websites are very similar to the blocked websites, enabling and encouraging easy identification and access. The details of registrants/operators of these websites are unknown and therefore the plaintiffs have arrayed them as 'John Doe' defendants.

11. He stated that in such circumstances courts in different jurisdictions have passed injunction orders blocking the primary website. Mr. Saikrishna handed over a Note on law prevalent in foreign jurisdictions in relation to website blocking. The Note handed over by him is reproduced hereinbelow:—

LAW RELATING TO WEBSITE BLOCKING PREVALENT IN FOREIGN JURISDICTIONS

Ø European Union

- Article 8.3 of 2001 Infosoc Directive (*Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*) provides rightsholders with a right to injunctive relief against intermediaries whose services are used by a third party to infringe copyright or related right.

- The preamble of the Infosoc Directive (recital 59) states that in the digital environment, the services of intermediaries may increasingly be used by third parties for infringing activities. In such cases intermediaries are best placed to bring such infringing activities to an end and therefore rightsholders should have the possibility of applying for an injunction against an intermediary who facilitates access to an infringing service. This is often referred to as the “no-fault based injunction”.

- Further, Section 5, Articles 9 and 11 of the Directive on the Enforcement of Intellectual Property Rights (*Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights*) support and are consistent with the goals as laid down in Article 8.3.

- Website blocking has been implemented across Europe and remedies both judicial (e.g. UK, Belgium, Spain, France, The Netherlands, Germany, Denmark, Norway, Ireland, Italy, Greece, Austria, Lithuania, Iceland and Sweden) and administrative (Italy, Spain, Portugal and Greece) are available in Europe.

- There are many European Court orders wherein websites have been ordered to be blocked by different methods. The precedent that blocking orders are proportionate and reasonable remedies has been established both at the national level and by the European Court of Justice (CJEU). The CJEU decisions constitute the highest legal precedent across all member states of the European Union and some of the relevant decisions are reproduced hereinbelow:—

(i) The CJEU in the 2014 *UPC Telekabel Wien v. Constantin Film Verleih* (Court of Justice of the European Union, Case C-314/12, March 27, 2014) case held:

- Providing link to copyright protected content, without the consent of the rightholder, constitutes an infringement.
- the ISP is an “inevitable actor in any transmission of an infringement over the internet” and that its services are therefore used to infringe copyright.
- the fundamental rights recognised by EU law must be interpreted as not precluding a court injunction prohibiting an internet access provider from allowing its customers access to a website placing protected subject-matter online without the agreement of the rightholders (...)

(ii) In a more recent judgment passed by the CJEU in the matter of *Stichting Brein v. Ziggo BV and XS4ALL Internet BV (C-610/15)*, it was held that the well known user submitted link/torrent Piratebay website directly infringes copyright in the EU. The Court found that Piratebay does communicate, goes beyond the mere provision of physical facilities, and plays an essential role in making the works available as, without the website, the sharing of works would be more complex. This was a key decision reiterating the validity of blocking of pirate websites throughout the EU.

Ø France

- Article L.336-2 of the French Intellectual Property Code: gives power to a regional first instance criminal Court, to order any measure to prevent an infringement of copyright or related rights against any person that can contribute to remedying the situation, on receiving an application for such order by the holders of the rights in the copyrighted works and subject-matters.
- This provision has been used by rightsholders to obtain blocking orders against illegal streaming websites in France. The Tribunal de Grandes Instances de Paris (TGI) issued a judgment requiring ISPs to block access to 16 unlicensed streaming sites. [28 November 2013, No. 11/60013]. The Court held that the injunction was compatible with fundamental freedom of expression. The Court of Appeal confirmed the findings and reiterated that the measures to block websites by ISPs do not violate rights of freedom of expression and are compliant with the principle of proportionality. [Paris Court of Appeal judgment of 15 March 2016 [No 040/2016].
- This decision by the Paris Court of Appeal was upheld by the French Supreme Court [15 March 2016 (RG No. 040/2016)] wherein it held that only in the instance where the blocking measure would compromise the viability of the business model of intermediaries, that the cost of such measure would be borne by the rightsholders.
- In *Société Française du Radiotéléphone et al. V Orange et al.*, Case No. 14/03236, France, Paris Court of First Instance (04 December, 2014) it was held that "while it is correct that any blocking measures can be circumvented by some internet users, on the one hand it has not been established that the large majority of internet users, who are attached to the free-of-charge nature of communications and numerous services on the internet, have the firm intention to participate in globalised and large-scale piracy and, on the other hand, the measures sought are aimed at the majority of users who do not necessarily have the time and skills to research means of circumventing the law, which specialists find and store in their memory."
- In *SFR v. Association of Cinema Producers*, Cour Cass, Civ 1, 6 July 2017, No 16-17.217, 16-18.298, 16-18.348, 16-18.595, ECLI:FR:CCASS: 2017:C100909 (Allostreaming) decided on July 6, 2017, by the French Supreme Court (Cour de cassation), established two very important precedents. The French Supreme Court confirmed the decision of the Paris Court of Appeal in March 2016 (RG No. 040/2016) which held that Internet intermediaries must bear the costs for implementing blocking measures against illegal streaming websites of copyright content; and confirmed that search engines qualify as intermediaries under Article 8.3 of the EU InfoSoc Directive, meaning they can be subject to orders to delist websites ordered for site blocking under Article 8.3.
- In *Federation Nationale Des Distributeurs De Films v. S.A. Orange*, 25 May 2018: On 25 May 2018, the Paris District Court ordered 6 new infringing streaming sites to be blocked and deindexed in France (including their future alternative domains). The case was filed by French right holders FNDF, SEVN, API and UPC - with the intervention of SPI and government body CNC - against search engine Google LLC and ISPs Bouygues Telecom, Free, Orange Numericable and SFR. The Court confirmed that costs have to be borne by the intermediaries provided that such imputation participates to the material and financial contribution to be made by the intermediaries whose services are used by a third party to infringe IP rights in order to remedy this infringement, and respects a fair balance between the copyright protection and the freedom of enterprise of the intermediaries. With regard to search engines, a de-indexing order is imposed for any result leading to the targeted sites, so not limited to currently known domains. Keys in the December 2017 judgment were: —
- Subsidiarity: No prior action is required against site operators, hosting providers or even registrars before seeking site blocking or delisting.

- **Proportionality:** Site blocking/deindexing measures are proportionate as they are targeted (target the infringing sites and French territory), limited in time (1 year) and implemented by the ISPs via the technical means of their choosing. They are also strictly necessary with respect to freedom of speech and communication - in accordance with French Constitutional Council decision nr. 2009-580 DC - as Internet users can still access the content through legal channels.
- **Search engines are intermediaries:** The Court confirmed that Google is an intermediary under Art.8.3 of Copyright Directive as its search engine is a means for Internet users to access infringing content.
- **Complementary nature of de-indexing to site blocking:** The Court confirmed that deindexing measures are complementary to blocking measures as they improve the effectiveness with respect to Internet users who may not know the direct links to the infringing sites.
- **De-indexing of entire sites:** The Court stated that if deindexing measure are not applied to the entire site, this would be an overly restrictive interpretation of Art.11 and Recital 24 of the Enforcement Directive.
- **Costs:** Referring to the objectives of the Copyright Directive (Recitals 4, 10, 16, 58, and 59), the Enforcement Directive (Recital 23, Artt. 3 and 11) and Art.12.3 of the E-Commerce Directive, the Court stated that the intent of those texts is to disconnect the safe harbor regime from the measures taken under Art.8.3 of the Copyright Directive, as a result rejecting the argument from the intermediaries that the safe harbor regime, the absence of causal role, or even their quality of third party, would exempt them from covering the implementation costs of the blocking measures.

Ø Germany

- **Third Act to Amend the Telemedia Act, Part 3, Section 7(4):** provides that in case a Telemedia service was used by a user to infringe the intellectual property right of a third party and if there is no other remedy against the infringement for the owner of this right, the owner of the right may request the service provider according to Section 8 sub-section 3, the blocking of information to prevent repetition of the rights infringement.

- **The German Court of Appeal in the case of *Constantin Film Verleih GmbH v. Vodafone Kabel Deutschland GmbH*, 29 U 732/18 (June 2018),** granted a blocking order against the Kinox.to site. The Court considered whether reasonable effort had been made by the rightsholder to effect legal action against the operator of the service and its service providers. The Court held in this case reasonable effort had been made and the rightsholder could not be expected to pursue even more time-consuming measures against the infringers that are often based in foreign countries and difficult to reach. The Court specifically noted that the blocking order will also apply to variances (additional domains, IP addresses, URLs) of the pirate service. The Court also clarified that the imposed site blocking measures “do not relate to the domain “Kinox.to” but to the overall service “Kinox.to”, which is offered under that company name, irrespective of the respective domain.” The appeal against this decision was rejected by the Court of Appeal of Munich (14 June 2018).

- **The German Federal Court of Justice laid down requirements to obtain injunctions against ISPs in order to make them block access to infringing websites.** (BGH, decisions dated 26 November 2015, case nos. I ZR 3/14 and I ZR 174/14). Although in this case injunction was not granted, it provided guidance on the requirements for obtaining blocking injunctions against ISPs. The Court accepted that ISPs can contribute to infringements of third parties but the blocking injunction against ISPs is to be considered as a last resort i.e. the interest of the rightsholders, access provider and the consumers must be well balanced.

- **The Court of Appeal summarily denied Vodafone's appeal in this case in June 2018.**

Ø United Kingdom

- **Section 97A of the Copyright, Designs and Patents Act, 1988 empowers the High Court to grant an injunction against the service provider once it is established that the service provider has actual knowledge of the infringement of copyright through its service. In terms of this provision, right owners have to establish that:**

- **Service providers have actual knowledge of infringement of copyright through its service.**
- **They had issued a notice with details such as the right owner, work in question, details of infringement.**

• Most importantly, Section 97A only entitles a right owner to get a no-fault injunction against a service provider. It does not entitle a right owner to allege liability for infringement itself. Section 97A provides the conditions under which such an injunction may be granted.

• Courts have interpreted “actual knowledge” as follows [20th *Century Fox v. British Telecommunication PLC* [2011] EWHC 1981 (Ch)]:

- Requirement of actual knowledge should not be interpreted restrictively.
- It means the service provider should have knowledge of use of the service to infringe, rather than have knowledge of the infringements thereby.
- What must be shown is that the service provider has knowledge of one or more persons using its service to infringe copyright.
- It is not essential to prove actual knowledge of a specific infringement of a specific copyright work by a specific individual.
- While granting orders for blocking of a website, Courts have taken the following factors into consideration:
 - Merely because granting of an injunction may open the floodgates for similar website blocking requests in the future, is not a sufficient ground to deny such block orders.
 - Because not all the content available on the website belonged to the plaintiffs.
 - And lastly, the Court considers the efficacy of passing the order i.e. the extent of users willing to circumvent the blocking.

Ø Singapore - Copyright Act, Section 193DDA, 193DDB and 193DDC

- Singapore amended its Copyright Act to enable Courts to make an order that would require ISPs whose services have been or are being used to access an online location to infringe copyright of rightsholders, to block access to a “flagrantly infringing online location”; thereby, giving rightsholders a more effective tool to disable access to pirate websites.
- Section 193DDA gives the High Court the power to disable access to flagrantly infringing online location. In order to determine a flagrantly infringing online location, the High Court is to consider the matters as listed out under Clause 2 of Section 193DDA:
 - the primary purpose of the online location being copyright infringement and whether the online location contains indexes or categories of the means to commit infringement;
 - whether the owner or operator of the online location demonstrates a disregard for copyright generally;
 - whether the online location has been blocked previously by any Court of any jurisdiction for copyright infringement and circumvention of such measure/Court orders by the online location;
 - the volume of traffic at or frequency of access to the online location.
- Before making an application for a Court order the owner of copyright must send a notice to the owner of the websites and also notify the ISPs of their intentions as per Section 193 DDB.
- The High Court may also vary the order made depending on material changes in the circumstances and on being satisfied on a few points as laid out under Clause 2 Section 193DDC.
- In 2016, at the request of the plaintiffs, the Singapore High Court ordered ISPs to disable access to Solarmovie.ph, finding the website to be flagrantly infringing intellectual property (*Developments in Site Blocking, Singapore Law Gazette, April 2017*).
- On 26 April 2018 the High Court in the case of *Disney Enterprises, Inc. v. M1 Limited*, HC/OS 95/2018,
 - rdered ISPs to block access to 53 piracy websites.
 - In furtherance of the above order, on July 12, the Court granted an order to block “variances” when the pirate services changes online location to evade the blocking order. This allows for flexible site blocking orders in Singapore for additional domains resolving to the same “online location” already ordered blocked. This precedent also bolsters flexible variance orders as an international best practice in site blocking, and mirrors the process that has been adopted in the United Kingdom, whereby rights holders periodically inform ISPs of additional domains, IP addresses, or URLs that resolve to the same online locations already ordered blocked. Ø Australia
 - Section 115A of the Copyright Act allows rightsholders to apply to the Federal Court for an injunction directing ISPs to block access to websites that infringe copyright content. The Court

considers the following factors before granting an injunction:

- the geographical origin of the website is located outside Australia; and the 'primary purpose' of the website is to infringe copyright.
- The law further provides that the owner of the copyright is to send notice to the ISPs and owner of website of the making of an application for injunction under this section.
- The Court considers certain factors to determine whether or not to grant an injunction such as ownership and subsistence of copyright, whether access has been provided outside Australia, infringement of copyright and primary purpose of website being infringement and discretionary factors where the Court feels there is blatant disregard for the rights of the copyright owners.
- In recent rulings by the Australian Federal Court, the ISPs have been ordered to block access to 59 websites and 127 web domains that carry pirated film and TV content on applications made by Roadshow Films and Foxtel. This was following a Federal Court decision in December 2016, *Roadshow Films v. Telstra Corporation Ltd.* [2016] FCA 1503, which were the first blocking injunctions in Australia.
- In a more recent decision, *Roadshow Films Pvt. Ltd. v. Telstra Corporation Ltd.* [2018] FCA 582, the facts were different being that the online locations did not host a website containing illegal content, rather they were specific online locations accessible via three apps installed and operated through the Android operating system on a TV smart box. The Federal Court granted the blocking injunctions against the illegal TV subscription services holding that the requirements under Section 115(A) were met as in the previous website blocking cases.
- The *Roadshow cases* also provide an avenue for quick applications to add additional domains, IP addresses and URLs used by the target online pirate service already ordered blocked, without the need for a further hearing.

Ø Legal Authorities and Statistics in Key Countries:

Countries Adopting (or Obligated to Adopt) Site Blocking, Legal Authorities, #of Sites Blocked, Efficacy Research (as of May 2018)			Sites Blocked (Approx)	Efficacy Research
	Country	Law		
1	Argentina	1933 Copyright Act; Unlawful enrichment civil law articles. Abuse of Rights doctrine.	1 site blocked	
2	Australia	Copyright Act, Section 115A	82 sites blocked	Incopro study finds significant drop in visitation to blocked sites (>50%) and 25% decrease in piracy overall. (<i>Incopro, Site Blocking Efficacy, Australia, December 2017</i>)
3	Austria	Copyright Act, Article 81	10 sites blocked	
4	Belgium	Code of Economic Law, Article XVII. 14	128 sites blocked	
5	Brazil	Article 195 of the Industrial Property Rights Act no. 9.279/96; Article 19, XIII and 162, Para 2 of the Organization of Telecommunication Services Act no. 9.472/97; Article	1 site blocked	

		300 of the New Code of Civil Procedure		
6	Denmark	Copyright Act Para 411 and Para 413; voluntary Code of Practice	128 sites blocked	
7	Finland	Copyright Act, Article 60c	2 sites blocked	
8	France	Intellectual Property Code, Article L 336-2	12 sites blocked	
9	Germany	Doctrine of Storerhaftung (derived from Articles 823 (liability in damages) and 1004 (claim for removal and injunction) of the German Civil Code (BGB))	1 site blocked (<i>Constantin Film Verleih GmbH v. Vodafone Kabel Deutschland GmbH</i> (2017) (Case Number: 7 O 17752/17)).	
10	Greece	Law 2121/1993 Copyright, Related Rights and Cultural Matters, Article 64A	2 sites blocked	
11	Iceland	Copyright Act No. 73/1972, Article 59 a	2 sites blocked	
12	Indonesia	Copyright Law No. 28 of 2014, Articles 54-56; Regs. Nos. 14 and 26 (2015)	444 sites blocked	MPA study found sharp reductions in piracy visitation due to four waves after site blocking implementation, with reductions in traffic of 74% - 94% at six months post-block. (<i>Motion Picture Association, Impact of Site Blocking in Indonesia (2017)</i>). This study also concludes that there was a 9 to 24% overall increase in piracy traffic due to the emergence of two piracy site groups: <i>Ik21</i> and <i>indoxxi</i> .)
13	Ireland	Copyright and Related Rights Act, 2000 Sections 40 (5A), 205. (9A)(a)	14 sites blocked	
14	Israel	Section 75 of the Courts Act	2 sites blocked	
15	Italy	Copyright Act, Article 156, 163 (1); AGCOM Regulation, Criminal Code	703 domains blocked (<i>Orders in Italy are issued on a</i>	

			per domain basis)	
16	South Korea	Act on the Establishment and Operation of Korea Communications Commission, Act No. 8867, Feb. 29, 2008 (2015), Art. 21; Act on Promotion of Information and Communication Network Utilization and Information Protection (2009), Art. 44-7	456 sites blocked	MPA studies demonstrate visits to blocked sites in South Korea declined over the 18 waves of site blocking between June 2015 and March 2017 by between 65% and 100% in the six months following each wave, with an average decline of 87% in the six months following site blocking (<i>Motion Picture Association, Impact of Site Blocking in South Korea (2017) (following up on MPA Study on Site Blocking Impact in South Korea (2016))</i>)
17	Lithuania	Law on Copyright and Related Rights, Article 78 (1)	1 site blocked	
18	Malaysia	Communications and Multimedia Act 1998, Section 263	198 sites blocked	MPA study found traffic to blocked sites was reduced in every wave of site blocking examined, ranging from reductions of 67% and 74% six months after waves 4, 5 and 6 of Malaysia site blocking. (<i>Motion Picture Association, Impact of Site Blocking in Malaysia (2017)</i>)
19	Mexico	Ley Federal del Derecho de Autor, Precepto 177	1 site blocked	
20	Netherlands	Dutch Copyright Act Section 26d and The Neighbouring Rights Act 1993, Section 15e	1 site blocked	
21	Norway	Copyright Act, Section 56c	21 sites blocked	
22	Portugal	Code of Copyright and Related Rights, Articles 210-G(1), 210-H (2), General Inspectorate of Cultural Activities ('IGAC') Competence Legislation	824 domains blocked (Orders in Portugal are issued on a per domain basis)	Research demonstrates site blocking in Portugal has resulted in an overall 69.7% drop in usage to the sites affected by the first 8 administrative blocking waves ordered in the country and resulted in a 9.3% decrease in piracy overall in Portugal to the top 250 piracy sites (blocked and unblocked). (<i>Incopro, Site Blocking Efficacy in Portugal September 2015 to October 2016 (2017)</i> , http://www.incoproip.com/wp

				<i>content/uploads/2017/07/Site-Blocking-and-Piracy-Landscape-in-Portugal-FINAL-pdf.)</i>
23	Russia	Civil Code, Article 1250, Internet Law	265 sites blocked	
24	Singapore	Copyright Act, Section 193A, DDA, DDB, and DDC	54 sites blocked	
25	Spain	Copyright Act, Article 138	16 sites blocked	
26	Sweden	Act on Copyright in Literary and Artistic Works Article 53b	2 sites blocked	
27	Thailand	Computer Crime Act (2016), Section 20(3)	1 site blocked	
28	Turkey	Law on Intellectual and Artistic Works 5846 Supplementary Item 4/3	22 sites blocked	
29	United Kingdom	Copyright, Designs and Patents Act, Section 97A	172 sites blocked	
30	Uruguay	Ley 9.739, art. 46 (a); Ley 17.616; Ley 17.520, arts. 1 and 2.	1 site blocked	
31	Bulgaria	Law on the Copyright and Related Rights, Article 96f	No case law to date	
32	Croatia	Copyright and Related Rights Act, Article 185	No case law to date	
33	Cyprus	Copyright Act, Article 13(4)	No case law to date	

Ø Other countries that have adopted site blocking:

- In Malaysia, the Malaysian Communications and Multimedia Commission (MCMC) may order its "licensee" to "prevent the network facilities that he owns or provides or the network service, applications service or content applications service that he provides from being used in, or in relation to, the commission of any offence" including copyright infringement.
- In Indonesia, the Minister Directorate General of Intellectual Property Rights (DGIPR) may, "[i]n case there is sufficient evidence to be found" of "copyright and/or related rights infringement through electronic systems for Commercial use"... "recommend to the Minister of Telecommunications and Informatics to block some or all of the content infringing the Copyright in the electronic system or make the electronic system service inaccessible."
- In Thailand, the Minister of Digital Economy "may submit a motion together with evidence to the competent Court to order discontinuation of dissemination or deletion of [computer data which is a criminal offense under the intellectual property laws] from the computer system."
- In Korea, the Korea Copyright Protection Agency (KCOPA), in consultation with the Ministry of Culture, Sports and Tourism (MCST)
- versees the blocking of sites which infringe copyright, based on organizing statutes including

the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.”

12. During the course of the arguments, Mr. Saikrishna extensively referred to an Article written “How Website Blocking Is Curbing Digital Piracy Without “Breaking the Internet” published in Information Technology & Innovation Foundation (ITIF) in August, 2016 by Mr. Nigel Cory, Associate Director, Trade Policy, ITIF. The relevant portion of the said Article is reproduced hereinbelow:—

“Many countries ask domestic Internet service providers (ISPs) to block access to websites engaged in illegal activities—such as those facilitating cybercrime, child pornography, or terrorism—because this is one of the few means available to respond to illegal materials hosted abroad. However, when it comes to addressing other legitimate public policy objectives, such as curbing digital piracy, some of these same countries are reluctant to ask ISPs to block websites dedicated to distributing illegal copies of movies, music, and other copyright-protected works. As a result, online piracy continues unabated. But where countries are using website blocking to fight digital piracy, the record shows it has been effective in driving users from illegal to legal sources of copyrighted material online…….

xxx xxx xxx

There are three key methods for website blocking: Internet Protocol (IP) address blocking, Domain Name Server (DNS) blocking, and Uniform Resource Locator (URL) blocking. While there may be ways for users and piracy site operators to circumvent these methods, it is important to remember that the aim of website blocking, like other online enforcement methods, is not to eliminate online piracy altogether, but to change consumers' behavior by raising the cost—in terms of time and willingness to find alternatives sites and circumvention tools—to make the legal sources of content more appealing.

Internet Protocol (IP) Address Blocking

Every computer has an IP address, similar to a street address or telephone number. When a user connects to the Internet, every packet of data sent or received over the Internet (e.g., for emails or to view websites) carries this IP address as does every destination on the Internet. Since ISPs act as central clearing houses for users' access to the Internet, they can modify their network settings equipment to discard user requests to access IP addresses for blocked sites. The costs of this process are low as the list of IP address is maintained centrally by the ISP. (Lukas Feiler, “Website Blocking Injunctions under EU and US Copyright Law: Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law” (working paper no. 13, Transatlantic Technology Law Forum (TTLF), Stanford University Law School and University of Vienna School of Law, 2012), http://law.stanford.edu/wp-content/uploads/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf.) Many ISPs and Internet backbone operators already use this process for security reasons (to fight malware) and to fight spam. (Lukas Feiler, “Website Blocking Injunctions under EU and US Copyright Law: Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law” (working paper no. 13, Transatlantic Technology Law Forum (TTLF), Stanford University Law School and University of Vienna School of Law, 2012), http://law.stanford.edu/wp-content/uploads/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf.)

There are a few ways that IP blocking can be circumvented, but these are cumbersome, and most Internet users do not have the sophisticated technical skills (and motivation) to sidestep blocking. Website operators can circumvent IP blocking by obtaining new IP addresses and reconfiguring their domain names so that users go to these new IP addresses, but this is also cumbersome, especially if it has to be done repeatedly. (Ofcom, “‘Site Blocking’ to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act” (London: Ofcom, May 27, 2010), <http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf>.) Users can circumvent IP address blocks by using software (such as an encrypted virtual private network) to relay their Internet connection via a server that is with a different ISP or via a different Internet backbone operator that is not affected by the block, but most users are not this sophisticated.

A disadvantage of IP blocking is that IP addresses can be quickly changed. IP blocking can also impact non-infringing websites, as a single IP address can host multiple websites. (Benjamin Edelman, “Web Sites Sharing IP Addresses: Prevalence and Significance,” Berkman Center for Internet and Society, Harvard Law School, last modified September 12, 2003). However, the focus of copyright enforcement and website blocking is on sites that facilitate large-scale

copyright infringement—such as those that have many full-length movies, TV shows, and songs—so even if the IP address used by a piracy site hosts non-infringing pages or files, the legitimate content that is blocked is small, and not reason enough to avoid shutting down the website. If The Pirate Bay or KickAssTorrents facilitated access to a small amount of content that had a creative commons license, and was therefore able to be shared, this would not change the fact that it is a piracy site worth shutting down.

Domain Name System (DNS) Blocking

DNS blocking targets the process that converts website domain names into a corresponding IP address, which is then used to communicate with other servers. The DNS system effectively serves as the phone book of the Internet and is used by virtually every piece of software or hardware on the Internet, from web browsers and email applications to game consoles and streaming video devices.

An ISP can block an entire domain by making configuration changes at its DNS server. When a user asks to access a particular website, such as www.maindomain.com, the DNS server of the customer's ISP recognizes the domain as a blocked site, does not allow it to be translated into an IP address, and responds to the user that the domain does not exist or redirects to an informational webpage. DNS blocking is quick to implement, as existing systems can be easily adapted, and would only require a modest incremental investment for ISPs. (Ofcom, "Site Blocking.")

Critics claim that DNS blocking, like IP blocking, will cause "collateral damage" due to the risk of over-blocking, as a single domain can host many websites through website extensions. (Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering" (Internet Society, May 30, 2012), 202, <http://www.internetsociety.org/internet-society-perspectives-domain-namesystem-dns-filtering-0>; Steve Crocker et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill" (technical white paper, May 2011), <https://stupid.domain.name/files/2011/05/PROTECT-IP-Technical-Whitepaper-Final.pdf>.)

However, this risk can be addressed by implementing DNS blocking at the subdomain level (e.g. www.piracysite.maindomain.com instead of www.maindomain.com). Furthermore, like IP blocking, if the main domain hosts a site that has the primary purpose of facilitating illegal access to copyrighted material, then it is a legitimate target for online enforcement.

A website operator that hosts copyright infringing material would only be able to circumvent the DNS block by using another domain name, but like IP blocking, this becomes cumbersome. Users are able to circumvent this process by using another domain name server (e.g., users could use a virtual private network to connect to an alternative DNS server not subject to the blocking orders). However, like IP blocking, it would be a mistake to assume that the average Internet user has the above-average technical skills necessary to do this. Many, if not most, consumers have low levels of computer literacy and certainly are not sophisticated enough to understand how to manipulate the DNS settings in the network configuration of their computers, mobile phones, and other Internet-connected devices. Furthermore, users who switch DNS servers can expose themselves to many security risks if they cannot trust the responses from these servers. For example, while the alternate servers may reliably return the correct IP address for a Russian file-sharing site, they might not return the correct address for Bank of America. (Paul Vixie, "DNS Changer," Circle ID, March 27, 2012, http://www.circleid.com/posts/20120327_dns_changer/; U.S. Attorney's Office, Federal Bureau of Investigation, "Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business," new release, November 9, 2011, <https://archives.fbi.gov/archives/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-inernet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business>). How many users are willing to risk their identity and financial information just to download a few songs?

Finally, circumvention software (such as encrypted virtual private networks) probably will not be adopted by many, as studies show that few users use these types of tools in countries where the government restricts access to certain websites. For example, a study by the Berkman Center for Internet and Society at Harvard University found that "no more than 3 percent of Internet users in countries that in engage in substantial filtering use circumvention tools. The actual number is likely considerably less." (Hal Roberts et al., "2010 Circumvention Tool Usage Report" (report, The Berkman Center for Internet & Society, Harvard Law School, Cambridge, MA,

October 2011),
https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf).

Uniform Resource Locator (URL) Blocking

URL blocking requires the ISP to examine both the headers of IP packets (which contain the source and destination IP addresses) and the contents of the IP packet. This is done through "shallow" or "deep" packet inspection (DPI) that examines the contents of the packet in transit, rather than simply the IP address of the source and destination devices. Shallow packet inspection is focused on IP addresses and technical specifications, such as port and protocol combinations. Deep packet inspection examines the packet for specific characteristics or values. When a packet matching the blocked site IP address, destination host, or even a particular keyword passes through a DPI device, the network connection can be terminated. These inspections can be performed by the ISP's router or a proxy that all traffic is forced through in order to access the Internet (such proxy servers are common in schools and businesses, as they cache content, block inappropriate sites, and provide some security).

This process can block specific websites (e.g., www.itif.org) or website addresses (e.g., www.itif.org/events/upcoming). Given this capability, URL blocking is the most precise method, thereby avoiding over-blocking. (Ofcom, "Site Blocking"). URL blocking combines the advantages of both DNS and IP blocking. (Feiler, "Website Blocking Injunctions Copyright Law."). To be effective, URL blocking needs to be designed so that it only targets specific types of network traffic, whether this is related to sites that actively facilitate terrorism, child pornography, or copyright infringement.

Network Functions Virtualization and Software-Defined Networks Can Make Blocking Cheaper, Easier, and More Effective

Software-Defined Networks (SDN) and Network Functions Virtualization (NFV) will fundamentally change how telecommunications carriers manage network operations and enable flexible new tools to block websites. (Fujitsu, "Technical Report: Carrier Software Defined Networking" (technical report for Ofcom, Fujitsu, Tokyo, March 2014), http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/SDN_Report.pdf.) These technologies, already used in many data centers, will eventually become key components of virtually all wide-area carrier networks for the simple reason that they offer powerful new tools and significant cost savings. (For example, Arthur Little and Bell Labs estimate operating expense savings of 30 to 50 percent. Arthur D. Little, "Reshaping the Future with NFV and SDN" (report, Bell Labs, Murray Hill, NJ, May 2015), 9, http://www.adlittle.com/downloads/tx_adlreports/ADL_BellLabs_2015_Reshapingthefuture.pdf).

These advantages are spurring surprisingly quick adoption of these techniques by industry. For example, AT&T plans for 30 percent of its network to use SDN and NFV by the end of 2016 and 75 percent by 2020. (Sean Michael Kerner, "AT&T to Virtualize 75 Percent of Its Network by 2020," Enterprise Networking Planet, March 15, 2016, <http://www.enterprisenetworkingplanet.com/netsp/att-pledges-to-virtualize-75-percent-of-its-network-by-2020.html>).

SDN separates the control of the network from the forwarding of information, offering network operators global control over switches and routers through software separate from the underlying hardware. This in turn allows networking applications, such as DNS, firewalling, and intrusion detection, to run in virtual systems installed on generic hardware whereas traditional network infrastructure relied on dedicated, fixed-function networking hardware. Combined, SDN and NFV allow greater network flexibility, easier introduction of new services, improved network manageability, and reduced costs. ("Data Plane Performance: A Key Enabler of SDN," 6Wind, accessed August 11, 2016, <http://www.6wind.com/software-defined-networking/6windgate-sdn/>.) In line with this, these changes in network management will make it much easier and cheaper to implement website-blocking mechanisms. For example, blocking could be achieved on the fly through software updates rather than individualized hardware configurations.

The Costs of Website Blocking

The costs of website blocking vary according to the type of blocks used and the country implementing them. More intensive processes, such as deep packet inspections, cost more. All website-blocking processes involve technical support costs for administering the blocking process within an ISP's network and in fielding calls from users about why they cannot access certain sites. There are hosting costs for the landing page that users trying to access blocked sites are redirected toward, as required in many countries. Cost estimates for initial website blocking

injunctions are likely to be high, given the legal costs involved in landmark court cases that a legal process for rights holders to use. However, once a website-blocking process is up and running, parts of it can be automated in order to minimize costs. For example, a centrally maintained register (with digitally signed lists of IP addresses) could be used by all ISPs in a country to update their settings to ensure that all necessary sites are blocked.

The United Kingdom's communications regulator, Ofcom, ranked the costs of different blocking techniques:

- IP address blocking: low cost;*
- DNS blocking: marginal incremental cost;*
- Shallow packet inspection: low cost if implemented only on routers, costly if implemented on firewall devices;*
- Deep packet inspection: relatively costly given the inspection of network traffic; and*
- URL blocking: potentially costly given hardware and software configurations, but this will change as ISPs move to software-defined networks. (Ofcom, "Site Blocking.").....*

Website Blocking Is Used as a Legitimate Tool by Many Countries

Many countries have turned to website blocking to apply existing and new legislation to a range of legitimate public policy goals that involve the Internet. Examples of the types of websites that are blocked:

- Child pornography (many countries)*
- Malware (e.g. Australia) (Claire Reilly, "AFP Using Site Blocking Laws to Target Malware," CNET, October 22, 2014, <http://www.cnet.com/au/news/afp-using-site-blocking-laws-to-target-malware/>.)*
- Investment fraud (e.g. Australia) (Josh Taylor, "FOI Reveals ASIC's IP-Blocking Requests," ZDNet, July 1, 2013, <http://www.zdnet.com/article/foi-reveals-asics-ip-blocking-requests/>.)*
- Online gambling (e.g. Singapore and Quebec, Canada) ("Approach to Regulating Content on the Internet," Media Development Authority Singapore, August 11, 2016, <http://www.mda.gov.sg/RegulationsAndLicensing/ContentStandardsAndClassification/Pages/Internet.aspx>.)*
- Pornography (e.g. India and others) ("Banned: Complete List of 857 Porn Websites Blocked in India," Deccan Chronicle, updated January 10, 2016, <http://www.deccanchronicle.com/150803/nation-current-affairs/article/porn-ban-complete-list-857-porn-websites-blocked-india>.)*
- Prostitution (e.g. India) ("174 Escort Services Websites to Be Blocked: State to Bombay High Court," dna India, April 21, 2016, <http://www.dnaindia.com/mumbai/report-174-escort-services-website-to-be-blocked-state-to-bombay-high-court-2204387>.)*
- Terrorism (the United Kingdom, Australia, France, and India) (For example, in 2015, France introduced a law that allows government agencies to order the blocking of websites that advocate acts of terrorism or contain images of child abuse. The legislation was brought in by revisions to the Loppsi Act, and an anti-terror bill passed by the French senate in 2014, but can now be used by the general directorate of the French police's cybercrime unit to force French internet service providers to block sites within 24 hours, without a court order. In the United Kingdom the government and ISPs have agreed to implement a system of blocks, similar to that used to keep child abuse material off the internet, for websites espousing terrorism related extremist views. Samuel Gibbs, "French law blocking terrorist and child abuse sites comes into effect," The Guardian, February 9, 2015, <https://www.theguardian.com/technology/2015/feb/09/french-law-blocking-terrorist-and-child-abuse-sites-comes-into-effect>. the United Kingdom.)*
- Copyright-infringing content (at least 25 nations).....*

SITE BLOCKING CAN HELP FIGHT ONLINE PIRACY

Some proponents of weak copyright argue that site blocking does no good, as content thieves will just find other sites to go to. In practice, this appears to be wrong. A new Carnegie Mellon University (CMU) study shows that the latest expansion of website blocking in the United Kingdom has been effective in fighting digital piracy. This study, released in April 2016, uses consumer data to analyze the impact of a court order for ISPs to block 53 websites in the United Kingdom in November 2014. This study shows that website blocking, when done on a large enough scale, can shift consumers from accessing copyright infringing material to consuming legal content online.....

The latest CMU study analyzed the impact that blocking 53 piracy websites in the United Kingdom in November 2014 had on the behavior of 58,809 users, comparing user visits three months before the blocks against user visits in the three months after the blocks (see Appendix B for the study's descriptive statistics). (Danaher, Smith, and Telang, "Website Blocking Revisited.") In both studies, the British Phonographic Industry (the trade association that represents the British record industry) was responsible for compiling and submitting to the court the list of websites for blocking. (Mark Sweney, "Record Labels Win ISP Blocks on 21 Filesharing Sites," *The Guardian*, October 29, 2013, <https://www.theguardian.com/business/2013/oct/29/record-labels-isp-piracy-block-music-filesharing>.) The court orders covered the six biggest ISPs, who collectively provide Internet services to over 90 percent of the United Kingdom. ("Facts and Figures," Ofcom, accessed August 11, 2016, <http://media.ofcom.org.uk/facts/>.).....

The results clearly showed that the website blocks were effective in changing consumer behavior. (Also see Appendix B.) To estimate the impact of the blocks, the study determined the difference between the observed activity by users after the blocks were enacted and the estimated counterfactual (as if the blocks had not been enacted) for these users' visits to piracy, ad-supported video, and subscription-based websites. The study found that:

- The blocking of these websites was effective, causing a 90 percent drop in visits to the blocked sites by users in the study sample (from 86,735 visits to blocked sites to 10,474), while causing no increase in usage of unblocked piracy websites. (The result was not 100 percent as some ISPs may have delayed enacting the blocks (into December), usage of virtual private networks to circumvent the blocks, and the order does not target some of the smaller ISPs.)
- The blocking of these websites had a significant impact on piracy, leading to a 22 percent decrease in total piracy for all users affected by the blocks (relative to the counterfactual estimate for how much they would have pirated if not for the blocks). The study is able to analyze the broader piracy universe as the 53 sites that were blocked were only a portion of the total piracy sites tracked in the study. (The causal change in total piracy was computed differently. The study assumes that the drop was a result of the blocks. Noting that the regression showed no causal increase in usage of unblocked piracy sites, the study calculated for each segment the total piracy before the blocks and assumed in the post-block period that, if nothing else changed except for the blocks, it would have been the same number less 90 percent, based on the study results. From this, the study calculated the causal change in piracy in each segment.)
- These blocks changed consumer behavior. The study estimated that the blocks caused a 10 percent increase in user visits to legal ad-supported streaming sites such as the United Kingdom's BBC and Channel 5. (The analysis of the results for access to ad-support and subscription video services was based on an analysis of coefficients from a regression analysis and showed that the estimate for the change in access to ad-supported video site was measured with 95 percent confidence, while the estimate for access to subscription services was measured with 75 percent confidence.) It also caused an estimated 6 percent increase in visits by users in the study to paid legal subscription-based streaming sites such as Netflix. This contrasts with the 12 percent increase in visits to subscription-based sites in the study of the 2013 blocks.....(The study into the website blocks of 2013 did not have data on visits to ad-supported legal content sites.)
- Relatively few users circumvented the website blocks. The study estimates that access to VPN sites increased 30 percent after the blocks, but this is likely off a relatively small base. The descriptive statistics show usage of VPN services is small relative to visits to other sites. For example, users in the study made 86,735 visits to the piracy sites before they were blocked, but only 1,688 to VPN sites (see descriptive statistics in Appendix B).
- The blocks had the biggest impact on the heaviest users of piracy sites. The study estimates that the blocks caused the heaviest piracy users in the study sample to reduce their use of pirated material by 28 percent, while leading to a respective 48.1 percent and 36.9 percent increase in their purchases of legal ad-supported and subscription services.

In summary, the study shows that while website blocking will not solve online piracy—no single tool, law, or practice will—it does reduce it while increasing the consumption of legal content. It then falls to other policies to target different parts of the piracy process and environment, which the United Kingdom does through a graduated response system for ISPs to

notify users of reported infringement, funding for education campaigns about accessing legal and illegal content, and a specialized Police Intellectual Property Crime Unit to investigate and tackle copyright infringement. All these measures, when combined with ongoing service and technology innovations, help tip the balance back toward the digital creators that rely on intellectual property to support and protect their creations and away from the rampant piracy that undermines their creativity.

Normal Rules Do Not Apply to the Internet

.....The CMU study also shows what other studies on the effectiveness of online enforcement have made clear—that the impact depends on public awareness and consistent and credible enforcement and implementation.....

Some opponents of website blocking have seized upon reports of governments misusing intellectual property enforcement measures for unrelated means, such as the Russian police raid on advocacy groups and opposition newspapers in the name of searching for pirated software. (Clifford J. Levy, "Russia Uses Microsoft to Suppress Dissent," *The New York Times*, September 11, 2010, <http://www.nytimes.com/2010/09/12/world/europe/12raids.html>.) However, such cases are rare and would not stand up to the type of scrutiny that is involved in the hundreds of cases where website blocking has been used to fight online piracy in recent years. Online intellectual property enforcement is far from alone in being a public policy that could be misused in order to pursue unrelated and illegitimate objectives. In each case, what matters is the actual intent and the integrity of the process involved in administering these policies.

Opponents of website blocking, including some ISPs, believe that the costs of website blocking are high enough to make the practice untenable. Internet exceptionalists fill the void created by the lack of detailed information about website blocking costs to paint the policy as unfeasible and unfair to both ISPs and consumers. However, these claims should not be taken at face value. The fact that we have not heard any uproar over the costs of website blocking of sites that actively facilitate child pornography or terrorism shows that enacting these blocks is not prohibitively expensive. In line with this, UK courts noted that ISPs have already made much of the necessary investment in relevant technology, processes, and staff in response to other law enforcement requirements.

As discussed above, website blocking costs look reasonable, especially when compared against total ISP operating revenue and investments. The UK government and judges presiding over website-blocking cases have stated that IP address-blocking would require ISPs to make additional investment in network hardware, but that these costs were not substantial, in many cases had already been made (to abide by other law enforcement decrees), and therefore would not present a barrier to IP blocking. Furthermore, in a similar process to what is required for website blocking, some DNS software vendors already offer customers an add-on to DNS systems that blocks malicious domains. (Ofcom, "Site Blocking."; Ron Moscona, "Website Blocking Orders - A New Tool in the Fight Against Online Trade in Counterfeit Goods," Dorsey, October 24, 2014, https://www.dorsey.com/newsresources/publications/2014/10/website-blocking-orders--a-new-tool-in-the-fight__.)

Critics claim that any measure to fight digital piracy will be abused by rights holders and that even the potential for such abuse is reason enough not to pursue online enforcement in the first place. This is why legislation and court orders in Australia, the United Kingdom, and elsewhere have built-in safeguards to ensure that only rights holders with high-quality cases—those involving websites that are dedicated to copyright infringement—are granted an injunction.....

CONCLUSION

As with any law-enforcement initiative, efforts to reduce digital piracy involve balancing costs and benefits. For example, while street crime could be reduced by doubling the number of police officers, communities seek an equilibrium where the marginal cost of an additional police officer does not outweigh the benefits from a corresponding reduction in crime. Regarding digital piracy, it is hard to argue that this equilibrium has been reached—there remains a lot of societal benefit to be gained through better efforts to stop digital piracy. The extent of digital piracy is so large, and the costs of additional enforcement are so reasonable, that it is clearly in the public interest to take more aggressive steps to fight digital piracy.

There is a reason why website blocking is being used in a growing number of countries: It can be a reasonable and useful tool to reduce piracy and encourage consumption of legal content. For it to be effective and workable, it needs to be predictable, transparent, accountable, low-cost, and quick to implement.....

Many opponents focus on the fact there are technical ways to circumvent website-blocking orders. However, the CMU study and others show that these users make up a relatively small proportion of total Internet users—certainly not enough to render website-blocking orders ineffective. Some critics would say that if blocking a website is not effective all of the time, then it should not be used at all. This is the same weak argument used against virtually every type of countermeasure. Why bother locking a door, when it is possible for sophisticated thieves to pick the lock? The answer, clearly, is that most thieves are not that sophisticated.

Complex problems with no single solution benefit from multilayered solutions. The standard for effectiveness should not be, as some opponents claim, elimination of all piracy. Reduction is an important goal, and on this point, the CMU study shows that website blocking can certainly help achieve this goal."

ARGUMENTS ON BEHALF OF LEARNED AMICUS CURIAE

13. Mr. Hemant Singh, learned Amicus Curiae stated that the first and foremost issue before this Court was to determine whether the websites complained of fell within the category of "*Flagrantly Infringing Online Locations*" (hereinafter referred to as 'FIOL'). He contended that the Court should not pass any orders against a website containing legitimate content and thus, the onus was on the plaintiff who was seeking site-wide blocking injunction to produce such evidence before the Court, which confirmed that the website complained of was only operating for sharing/downloading infringing/pirated content and was not limited to the plaintiffs' contents but also third parties' content.

14. He stated that caution had to be undertaken as there could be a website which could have both infringing content of plaintiff and legitimate content of third parties. According to him, the FIOL would be only such website where there was no legitimate content and if the evidence produced before Court was not of such nature, then prayers of wide ramification, interfering with legitimate content should not be granted.

15. Learned Amicus Curiae stated that upon assessing the enjoined and blocked website www.bmovies.pro, he had been redirected to www4.fmovies.to, a mirror website, which showed that 29,485 movies/TV series were arranged in an alphabetical manner. He stated that each alphabet depicted the total number of movies/TV series available e.g. under alphabet 'A', 1935 movies/TV Series were available, under alphabet 'B', 1913 movies/TV Series were available, under alphabet 'C', 1584 so on and so forth.

16. He pointed out that there were at least 122 other movies of the plaintiffs on www4.fmovies.to. Learned Amicus Curiae stated that the plaintiffs had not fully checked their own movies on the said website, let alone third-party content. He contended that the least due diligence expected of the plaintiffs was to provide evidence of at least all of their own movies, if not of third parties (though expected) that were illegally available on the impugned websites.

17. He submitted that the "three-step verification" test evolved by the Bombay High Court in *Eros International Media v. BSNL*, Suit No. 751 of 2016, which consisted of verification by an independent entity, extensive documents being placed on record and an affidavit on oath, was not satisfied in the present case. He contended that the evidence of the nature envisaged by courts was lacking in the present case. The relevant portion of the orders in *Eros International Media* (supra) relied upon by Mr. Hemant Singh are reproduced hereinbelow:—

a) Order dated 22nd July, 2016

"2. I am making it clear that I will not grant an injunction or order to block URLs that point to websites unless it is demonstrated that the entirety of the website contains, and contains only, illicit material. Without that being attested to and established on Affidavit, I will not consider an order that results in the blocking of an entire website."

b) Order dated 26th July, 2016

"14. Thus, what I have before me now is a three-step verification. First, a verification and an assessment by Aiplex (Plaintiff). This is accompanied by their letter in writing. There is then a second level of verification that is said to have been done by the deponent of the Affidavit along with the Plaintiffs' Advocates; and finally all of this material is placed on Affidavit and is now on oath. I think this is sufficient material on which to base an order."

18. However, Mr. Hemant Singh, learned Amicus Curiae admitted that online piracy was a menace. He stated that the problem was compounded due to high end technology that was used by FIOL. He pointed out that certain FIOLs like Torrents do not have a centralized server whereupon files are stored. Instead, users download freely available specialized software, which once connected

to the Internet, connects the user's computer into a Peer to Peer (P2P) network of other computers using the same software. He stated that a torrent is a file that allows a user to download bits and pieces of the content from several sources at the same time, which is assembled into the final complete copy onto the user's system. The content/data is stored on these systems (either completely or in bits or parts) and is made available for download through the specialized software. Given the scattered nature of the content as well as the inadvertent complicity of many persons, it becomes extremely difficult to pin-point the exact source of the content and for right-holders to take action. A helpful illustration of the P2P infrastructure, prepared by learned Amicus Curiae, is reproduced hereinbelow:

19. He pointed out that the courts across the world have grappled with devising appropriate mechanisms to prevent the menace of FIOL which largely included blocking of the specific URLs or the website in general. Some of the technical measures which had been employed to block, according to him, are reproduced hereinbelow:—

a. DNS Name Blocking:

The 'Domain Name System' [DNS] is the system which associates the colloquial name of a website (www.example.com) to the IP address of the site's web server, whereupon the website is hosted. DNS name blocking involves an ISP removing or modifying its records of the IP address for a particular Domain Name, thus ensuring that requests for such domain name are rendered void.

b. IP Address Blocking (IPB):

IP Address blocking involves ISPs discarding any traffic received from impugned IP address, as opposed to the website name. As several websites may be hosted on one server with a unique IP address, each of them, no matter what their name, would be blocked in case the IP address is blocked.

c. Deep Packet Inspection (DPI) based Blocking:

This technique involves examining the data received as part of the Internet traffic and filtering out specific content, patterns, or application types. DPI can be made on the basis of keywords or even image search. In case the data is found to contain the blocked content, the ISP shall block such content.

20. He admitted that the aforesaid measures of DNS, IPB and DPI blocking face challenges such as legitimate contents being blocked, invasion of privacy, high cost of deployment etc. He submitted that there was a serious concern associated with blocking orders that would prevent access to legitimate content in the cases of copyright.

21. According to him, Courts all over the world have considered the effect of over-blocking and have held that in order to ensure proper balance between the implementation of blocking injunctions and rights of the third-parties, it is essential to make sure that these blocking injunctions are proportionate. The proportionality principle, according to him, is designed to ensure that interferences with rights is justified as being no more than necessary to protect the rights or to achieve other legitimate goals. The learned Amicus Curiae relied upon the following case law:—

A) *Scarlet Extended SA v. Societe Belge des Auteurs Compositeurs et Editeurs SCRL*, [Case C 70/10]: *The ECJ, when talking about a proactive blocking order that would involve pre-filtering of content by ISPs for an indefinite period, held that such an injunction would be inconsistent with the prohibition on monitoring with respect to E-Commerce Directive and would be a disproportionate interference with the right to protection of personal data and freedom of Internet users to receive and impart knowledge, particularly considering the likelihood of over-blocking. It was also held that the costs involved in establishing a filtering system will fail to strike a fair balance between the rights of the copyright holders and the ISPs' freedom to conduct its business since an ISP is a mere connectivity provider as opposed to a hosting provider and thus has a passive, neutral role. Therefore, proactive blocking orders in the nature of pre-filtering were considered contrary to law.*

B) *UPC Telekabel v. Constantin Film*, [Case C-314/12]: *The ECJ addressed the proportionality of an injunction ordering an ISP to block access to an identified website, but the order failed to specify the measures to be taken by an ISP. The ECJ held that an injunction must be 'strictly targeted', so as to strike a balance between preventing third-party infringements and protecting freedom of information. The Court refuted the claim that an injunction can only be proportionate if it leads to a complete cessation of infringements. It was held that as blocking orders can always be circumvented, and as an injunction against one site cannot prevent*

infringing content from being available elsewhere, accepting an 'absolute effectiveness' standard would mean that an injunction could never be justified. Thus, targeted injunction is permissible even where it does not lead to complete cessation of copyright infringement, provided that there is no unnecessary deprivation of possibility of lawfully accessing information and it makes access difficult or seriously discourages internet users from accessing the targeted sites.

- C) Austria/CJEU (2014): UPC Telekabel Wien GmbH v. Constantin Film GmbH and Wegafilmproduktionsgesellschaft mbH (Telekabel), Case C-314/12, 27 March 2014: *This case decided in March 2014 established "no fault" site blocking injunctions under Article 8.3 of the EU InfoSoc Directive, opening the way for broader implementation of site blocking throughout the European Union.*
- *Specifically, questions were posed by the Higher Regional Court, Vienna, Austria, essentially as to: 1) whether Article 8(3) of the EU InfoSoc Directive is to be interpreted as meaning that a person who makes protected subject-matter available on the internet without the rightholder's consent is using the services of the Internet service providers, and therefore, the Internet service provider is an "intermediary" within the meaning of Article 8(3); and 2) whether it is compatible with EU law to prohibit an internet access provider from, allowing its customers access to a certain website when the material available on that website is provided exclusively or predominantly without the rightholder's consent.*
 - *The Court answered in the affirmative and the Court of Justice of the European Union laid the groundwork for national Courts to (as the Court had in Newzbin 2) issue a broad injunction against an Internet service provider to block websites. The CJEU found that an injunction would not infringe upon the fundamental right to conduct business because the ISP was free to decide upon the measure to be put in place to protect against this type of copyright infringement. The injunction would also allow Telekabel to avoid liability by showing that it has taken all necessary precautions, essentially confirming a "no fault" injunction approach in the EU.*
- D) Germany (2015): GEMA v. Deutsche Telekom, BGH, Urteile v. 26 (GEMA), November 2015 - I ZR 3/14 und I ZR 174/14: *Germany's Federal Constitutional Court (BGH) in late 2015 confirmed that site blocking does not breach privacy rights under both German and EU law, and is consistent with the German Constitution.*
- *In analyzing whether site blocking can be consistent with Article 10(1) of the German Constitution (right of privacy of telecommunications), the Court noted, "[t]he starting point for the protection in Art. 10 (1) ... is always the non-public exchange of specific communications of participants; in contrast, communications addressed to the general public are not covered by this provision."*
 - *The Court found, "a site providing links to downloads on the internet directed at an unspecific number of addressees does not constitute confidential individual communication; rather it is, a public offering, not covered by the scope of protection of Art. 10 (1)" The Court also concluded that DNS blocking "does not affect the confidentiality of communication protected under Art. 10 (1)...." The Court weaves a path for IP or URL blocking as well,[13] but is more emphatic about DNS blocking's conformity with the German Constitution, noting DNS blocks are inherently unproblematic in this basic point as the establishment of connections is simply prevented - without access to IP addresses. According to the Court, offering files for public download and accessing those files does not constitute an individual communication protected by Article 10 of the German Constitution.*
 - *Further, "[t]he fact that access to a public offer of a download occurs in each case through means of individual technical communications. connections does not justify a classification as communication within the meaning of Art. 10 (1) German Constitution, because a mere technical communication does not exhibit the specific risks for the privacy of the communication which that provision protects.... Such access actually constitutes a public form of communication comparable to the use of mass media...."*
 - *Importantly, and addressing one of the key objections to site blocking, the Court further concluded, "the (automated) obtaining of knowledge, on the part of the provider, of the circumstances of communication is limited to that necessary to interrupt the communication." This is consistent with prior rulings that there is no interference with the fundamental right to privacy "in the case of the recording of telecommunications events, provided they are recorded purely using technical means, anonymously and without trace*

and are immediately filtered out without any interests of the authorities in gaining knowledge, thereof." The Court also examined site blocking in light of the EU's strict privacy rights provisions, and the EU Charter of Fundamental Rights, finding site blocking to be consistent with both. Specifically, the Court concluded that site blocking does not breach Article 7 of the EU Charter of Fundamental Rights, since the purpose of the right - protecting "the confidentiality of communication which is directed at particular addressees and not at the public" - is not affected by the blocking of public offerings of downloads or access to them." This is consistent with site blocking decisions in other EU jurisdictions. While the case itself did not result in the first site block in Germany, it can be said the GEMA case paved the way for the Constantin decision to come. Germany (2018): Constantin Film Verleih GmbH v. Vodafone Kabel Deutschland GmbH (2018) (Case number: 7 O 17752/17) (Constantin): In this landmark decision handed down in February 2018, the Munich District Court ordered site blocking in Germany for the first time.

- The Court ruled that Vodafone had to bear the implementation costs (and had to pay rights holder Constantin's legal costs). In arriving at its decision, the Court applied the German Telemedia Act, and applied the secondary liability doctrine of Storerhaftung, and the Court's decision is consistent with Germany's obligations under Article 8.3 of the EU InfoSoc Directive.

E) • Vodafone appealed the decision in March, but on June 14, after an oral hearing before the Court of Appeal Munich, the three-judge panel denied the appeal unanimously.

22. Mr. Hemant Singh lastly contended that if the obligation of an ISP is limited to particular domain names, it would make the whole issue of granting blocking injunctions pointless, since there exists high likelihood of the infringers operating under a different domain name as soon as or even during the time the injunction is granted. He pointed out that recently, the Milan Court of First Instance [<http://ipkitten.blogspot.com/2018/08/milan-court-issues-dynamic-blocking.html>] ruled that Dynamic Injunctions are compatible with the E-commerce Directive. He submitted that this Court can exercise powers under Section 151 CPC to pass dynamic injunction limited to the mirror/redirected FIOL. He, however, stated that caution of supervision needed to be exercised to prevent misuse and overreach. He suggested that the Court should direct the plaintiffs to file detailed affidavits before the learned Joint Registrar who may examine whether the website sought to be included in the affidavit is a mirror FIOL or not. He stated that once the learned Joint Registrar is satisfied, such orders may be extended.

NEITHER THE ISPs OR DoT OR MEITY ADVANCED ANY ARGUMENTS

23. Neither the DoT nor MEITY advanced any arguments before the Court. Even the ISPs to maintain their neutrality did not advance any arguments. Learned counsel for ISPs as well as DoT and MEITY stated that they would abide by any order passed by this Court.

THOUGH THIS COURT IS SATISFIED THAT THERE IS NO FACT WHICH NEEDS TO BE PROVED IN VIEW OF THE DEEMED ADMISSION BY THE DEFENDANTS UNDER ORDER VIII RULE 10 CPC, YET KEEPING IN VIEW THE SEMINAL ISSUES THAT ARISE FOR CONSIDERATION, THIS COURT DECIDES TO PEN ITS OPINION

24. Despite being served through the contact information provided in the Whois details and/or other publicly available information, none of the defendant-websites have chosen to rebut or challenge till date any of the factual assertions or the evidence placed by plaintiffs in support of their claims. Though this Court is satisfied that there is no fact which needs to be proved in view of the deemed admission by the defendants under Order VIII Rule 10 CPC, yet keeping in view the seminal issues that arise for consideration, this Court decides to pen its opinion.

COURT'S REASONING

THE GENERAL INDUSTRY EVIDENCE APPEARS CONSISTENT WITH A HYPOTHESIS THAT DIGITAL PIRACY HAS HURT THE MOVIE INDUSTRY. IN FACT, ONLINE PIRACY HAS HAD A VERY REAL AND TANGIBLE IMPACT ON THE FILM INDUSTRY AND RIGHTS OF THE OWNERS.

25. According to the report 'The Economic Impacts of Counterfeiting and Piracy' prepared for BASCAP and INTA, the general industry evidence appears consistent with a hypothesis that digital piracy has hurt the movie industry. Revenues for sales and rentals of pre-recorded movies in the U.S. declined by more than 20% between 2005 and 2010 after having increased steadily until then. Box office revenues have remained relatively constant during the same period although a gradual 47% rise over the decade leading upto 2002 might have suggested an upward trend if it were to continue at the same pace.

26. In fact, the introduction of BitTorrent in 2003-04 has coincided with the turning point in the revenues of the film industry. This statement is based on the fact that the ease with which copyrighted material can be copied and shared online across jurisdictional borders makes it challenging for right holders to protect their works as they do in the offline world where customs agents can typically intercept physical goods, such as CDs and DVDs, that contain illegal copies of songs, movies, TV shows and other content. It is estimated that by the end of 2022 (See <https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICCBASCAP-Frontier-report-2016.pdf>), the loss of legitimate revenue on account of film piracy would reach \$289-644 billion.

27. Mr. Nigel Cory in his Article "How Website Blocking Is Curbing Digital Piracy Without 'Breaking the Internet'" (supra) points out that a 2016 study by the European Union's Intellectual Property Office highlights the size and scale of the piracy. It estimated that the European music industry lost €170 million in sales revenue in 2014 as a consequence of digital piracy. This equals a loss of 5.2 percent of its total annual sales (both physical and digital) to piracy. When indirect economic impacts are included, digital piracy is estimated to lead to €336 million in lost sales in the European Union, which leads to an estimated 2,155 lost jobs. This has real economic consequences, as approximately 39 percent of total economic activity and 26 percent of all employment in the European Union is in intellectual property-intensive industries, with another 9 percent of jobs supported by the economic activity of these industries.

28. It is estimated that in India, while the film industry earns around \$2 billion from legitimate sources such as screening at theaters, home videos and TV rights, piracy earns 35 per cent more at \$2.7 billion (See: home.kpmg.com/in/en/home/events/2017/03/kpmg-india-ficci-media-entertainment-report-2017.html). According to the Irdeto Global Consumer Piracy Threat Report 2018, India is one of the top five countries with the highest P2P downloads taking place, as close to 965 million P2P downloads took place in India between January 2017 and May 2018.

29. It is important to realise that piracy reduces jobs, exports and overall competitiveness in addition to standards of living for a nation and its citizens. More directly, online piracy harms the artists and creators, both the struggling as well as the rich and famous, who create content, as well as the technicians-sound engineers, editors, set designers, software and game designers-who produce it and those who support its marketing, distribution and end sales. Consequently, online piracy has had a very real and tangible impact on the film industry and rights of the owners.

THE INDIAN COPYRIGHT ACT CONFERS A BUNDLE OF EXCLUSIVE RIGHTS ON THE OWNER OF A "WORK" AND PROVIDES FOR REMEDIES IN CASE THE COPYRIGHT IS INFRINGED. THIS COURT IS OF THE OPINION THAT IT HAS AMPLE POWERS TO MOULD THE RELIEF TO ENSURE THAT THE PLAINTIFFS' RIGHTS ARE ADEQUATELY PROTECTED.

30. The Indian Copyright Act, 1957 ("the Copyright Act") confers a bundle of exclusive rights on the owner of a "work" and provides for remedies in case the copyright is infringed. The relevant portion of Statement of Objects and Reasons of the Copyright (Amendment) Act, 1994, is reproduced hereinbelow:—

"Effective copyright protection promotes and rewards human creativity and is, in modern society, an indispensable support for intellectual, cultural and economic activity. Copyright law promotes the creation of literary, artistic, dramatic and musical works, cinematograph films and sound recordings by providing certain exclusive rights to their authors and creators...."

31. Section 2(y) of the Copyright Act defines "work" as including a cinematograph film, which is defined under Section 2(f). The said sections read as under:—

"2(y) 'work' means any of the following works, namely:—

(i) a literary, dramatic, musical or artistic work;

(ii) a cinematograph film;

(iii) a sound recording;

2(f) 'cinematograph film' means any work of visual recording and includes a sound recording accompanying such visual recording and 'cinematograph' shall be construed as including any work produced by any process analogous to cinematography including video films;"

32. Section 14 specifies the exclusive rights of the owners. Section 14(d) provides that communication to the public of a cinematograph film or any substantial part thereof is one such exclusive right. The relevant portion of the said Section is reproduced hereinbelow:—

"14. Meaning of Copyright

For the purposes of this Act, 'copyright' means the exclusive right subject to the provisions of this Act, to do or authorise the doing of any of the following acts in respect of a

work or any substantial part thereof, namely:—

xxxx xxxx xxxx xxxx

(d) in the case of a cinematograph film,--

(i) to make a copy of the film, including-

(A) a photograph of any image forming part thereof; or

(B) storing of it in any medium by electronic or other means;

(ii) to sell or give on commercial rental or offer for sale or for such rental, any copy of the film;

(iii) to communicate the film to the public."

33. Section 2(ff) defines "communication to the public". It reads as follows:—

"2(ff) "communication to the public" means making any work or performance available for being seen or heard or otherwise enjoyed by the public directly or by any means of display or diffusion other than by issuing physical copies of it, whether simultaneously or at places and times chosen individually, regardless of whether any member of the public actually sees, hears or otherwise enjoys the work or performance so made available.

Explanation.— For the purposes of this clause, communication through satellite or cable or any other means of simultaneous communication to more than one household or place of residence including residential rooms of any hotel or hostel shall be deemed to be communication to the public;"

(emphasis supplied)

34. The above definitions make it clear that making any work available for being seen or heard by the public whether simultaneously or at places chosen individually, regardless of whether the public actually sees the film, will constitute communication of the film to the public. The intent was to include digital copies of works, which would include within its scope digital copies of works being made available online (as opposed to the physical world). Communication can be by various means such as directly or by display or diffusion. In this context, definition of "broadcast" is also relevant which identifies communication to public by wireless diffusion or by wire. Thus, making available of a film for streaming or downloads in the form of digital copies on the internet is within the scope of "communication to the public".

35. It is pertinent to note that the definition of "communication to the public" was first added in the Copyright Act by the 1983 Amendment and was as follows:—

"Communication to the public" means communication to the public in whatever manner, including communication through satellite".

36. Subsequently, as is evident from the Statement of Objects and Reasons of the 1994 Amendments, various amendments were brought to incorporate the technological advances. The 1994 Amendments substituted a more expansive definition of "communication to the public" in order to address various technological advances, which was as follows:—

2(ff) "communication to the public" means making any work available for being seen or heard or otherwise enjoyed by the public directly or by any means of display or diffusion other than by issuing copies of such work regardless of whether any member of the public actually sees, hears or otherwise enjoys the work so made available.

Explanation.— For the purposes of this clause, communication through satellite or cable or any other means of simultaneous communication to more than one household or place of residence including residential rooms of any hotel or hostel shall be deemed to be communication to the public;

37. The Copyright Act was further amended in 2012 to partially implement obligations under the 1996 WIPO Internet Treaties (WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty), in light of the substantial developments in technology with the aim of protecting copyright in the digital context.

38. Section 51(a)(i) provides that copyright is infringed when any person, without authorisation of the copyright owners, does anything of which the exclusive right lies with the owner of copyright. Thus, the defendants' websites, which are communicating the films to the public by making the films available for being seen or heard or enjoyed through their websites, are infringing the plaintiffs' copyrights in the film.

39. Additionally, Section 51(a)(ii) imposes liability on owner of a place when such owner permits his place to be used for communication of the film to the public for profit, without authorisation of

the copyright owner. Such liability can be avoided only if the owner of the place is able to establish that he was not aware and had reasonable ground to believe that the communication of the work in his place was not an infringement.

40. Section 52(1)(c) of the Copyright Act exempts from liability, any transient or incidental storage of a work for the purpose of providing access to content where such access has not been expressly prohibited by the copyright. Thus, ISPs are exempt from liability of copyright infringement under Section 52(1)(c) for any transient or incidental storage of a film. However, the proviso to this section mandates that if a complaint is received, an ISP shall restrain access to content for a period of twenty-one days or upon receiving a competent court order. Pertinently, if no such order is received by the ISP within twenty-one days, the proviso permits the ISP to reinstate access to the stored film.

41. In the present cases, no defendants' website has appeared before this Court or answered any notice claiming a limitation of liability under any provision including Section 52(1)(c) of the Copyright Act.

42. The Information Technology Act, 2000 ("IT Act") incorporates the defence of safe harbour for the intermediaries. It defines an intermediary under Section 2(1)(w), as including ISPs. The IT Act, under Section 79, creates a safe harbour for all intermediaries from liability for any third-party data, information or communication link that is made available by the ISP. Such exemption applies when the function of ISPs is limited to providing a communication system over which third party information is transmitted or temporarily stored. However, copyright is not included in the activities to be covered under the IT Act, so is generally inapplicable to this batch of matters.

43. Further, while dealing with Section 79 and the issue of extent of knowledge of an intermediary for it to act and take down content, the Supreme Court in *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 has held that the requisite knowledge which obligates an intermediary to act is when it receives a Court order directing the blocking of access. Mere receipt of notice does not obligate the intermediaries to act and take down content. The relevant portion of the judgment of *Shreya Singhal v. Union of India* (supra) is reproduced hereinbelow:—

"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)."

44. Subsequently, a Division Bench of this Court in *Myspace Inc. v. Super Cassettes Industries Ltd.*, 2016 SCC OnLine Del 6382 has held that though Section 79 grants a measured privilege to an intermediary, yet that does not mean that the rights guaranteed under the Copyright Act are curtailed in any manner. All that Section 79 does is to regulate the liability in respect of intermediaries, while the Copyright Act grants and controls rights of a copyright owner.

45. In any event, the plaintiffs herein do not seek to block Websites based on mere notices, although, with respect to mirrors and redirects (additional domain names, IP addresses, and URLs discovered to provide access to the same FIOL complained of), the plaintiffs contend that this Court may issue an order providing that plaintiffs may, by notification to the ISPs, add such additional means of accessing the FIOL's to the original orders.

46. Section 69A of the IT Act creates an administrative remedy empowering the Central

Government to block access to any information on the grounds of-

- (i) Interest of sovereignty and integrity of India
- (ii) Defence of India
- (iii) Security of State
- (iv) Friendly relations with foreign States, or
- (v) Public order

47. Copyright infringement does not fall within the suo motu powers of the Central Government to direct blocking. To be fair to the plaintiffs, they also did not seek to invoke the Government's powers under the IT Act. Rather the claim of the plaintiffs is based on this Court's jurisdiction to issue orders under the Copyright Act.

48. In the opinion of this Court, the defendant-websites are liable for copyright infringement under Section 51 of the Copyright Act. They cannot claim the exemption of Section 52(1)(c) as they are not entities that transiently and incidentally store the plaintiffs' films. They further cannot claim the exemption under Section 79 of the IT Act as they are not intermediaries.

49. Section 55 of the Copyright Act provides civil remedies to the rights holders which includes entitlement to an injunction order on approaching the Court. Consequently, the Court has ample inherent powers to mould the relief to ensure that the plaintiffs' rights as copyright owners are adequately protected.

WHETHER AN INFRINGER OF COPYRIGHT ON THE INTERNET IS TO BE TREATED DIFFERENTLY FROM AN INFRINGER IN THE PHYSICAL WORLD?

50. However, many believe that Internet is a unique highway or a separate space (i.e. Cyberspace) to be left totally free i.e. unrestricted. They believe that this space should be left free to be used by an infringer or by a law abiding individual simultaneously. Internet exceptionalists, such as the Electronic Frontier Foundation, are defined by the belief that because the Internet is exceptional, most rules that apply offline should not apply online. Followers of this school of thought believe that the Internet is first and foremost about individual freedom, not about collective responsibility. Their view is that the Internet's chief function is to liberate individuals from control by, or dependence on Government and Corporations. They believe in the maturity of the public. The followers of this school of thought acknowledge that online piracy comes at the cost of legal sales, but they rationalize this loss by saying that it only hurts the profits of content firms, implying that if the choice is between infringement that rewards consumers with free content legality that helps corporations, then the former is to be preferred.

51. However, this Court finds that the majority of piracy websites are in it not for any ideological reason but for one reason: to make money. Modern digital piracy is a multibillion-dollar international business. (Only a small fraction of sites are supported by ideologies which believe that piracy is a social good.) For example, the owners of The Pirate Bay were earning \$3 million a year, according to Swedish prosecutors. More recently, U.S. law enforcement stated that one of the world's most popular piracy sites—KickassTorrents—was making \$16 million annually in advertising.

52. Business models differ, but the majority of piracy sites make money via advertising, or to a lesser degree, through subscriptions that provide premium access to content without advertising. The Digital Citizens Alliance's Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business report showed that 589 of the largest piracy sites generated more than \$200 million in advertising-driven revenues in 2014. Another report showed that 80 percent of the top piracy websites (550 of 622) in Europe carried advertising, showing how easy it is for piracy sites to profit from online advertising and how profit-driven these sites are. Piracy sites take advantage of the fact that the online economy has become more complex and easier to exploit. There are many intermediaries that aggregate ad space—known as an ad exchange—from a range of websites (both legitimate and illegitimate) for advertisers to use. This makes it easy for websites hosting illegal content to gain advertising revenue, including from legitimate brands and businesses, which may be several steps and organizations removed from the host site.

53. Also should an infringer of the copyright on the Internet be treated differently from an infringer in the physical world? If the view of the aforesaid Internet exceptionalists school of thought is accepted, then all infringers would shift to the e-world and claim immunity!

54. A world without law is a lawless world. In fact, this Court is of the view that there is no logical reason why a crime in the physical world is not a crime in the digital world especially when the Copyright Act does not make any such distinction.

WHETHER SEEKING BLOCKING OF A WEBSITE DEDICATED TO PIRACY MAKES ONE AN OPPONENT

OF A FREE AND OPEN INTERNET?

55. If the views of Internet exceptionalists were to be accepted, then a boon like Cyberspace would turn into a disaster. Further, just as supporting bans on the import of ivory or cross-border human trafficking does not make one a protectionist, supporting website blocking for sites dedicated to piracy does not make one an opponent of a free and open Internet. Consequently, this Court is of the opinion that advocating limits on accessing illegal content online does not violate open Internet principles.

56. The key issue about Internet freedom, therefore, is not whether the Internet is and should be completely free or whether Governments should have unlimited censorship authority, but rather where the appropriate lines should be drawn, how they are drawn and how they are implemented.

WHAT IS A 'ROGUE WEBSITE'?

57. One of the key issues around digital piracy is the importance of distinguishing between accidental and intentional piracy. Some experts are apprehensive that anti-piracy orders can go too far, sweeping in the former when they should be more focused on the latter. There are risks that cleverly drafted plaintiffs could intentionally harm sites that are largely focused on legal material and that diligently work to limit infringing material. But one also knows that doing nothing contributes to further piracy. In the opinion of this Court, finding this balance does not mean abandoning efforts to go after international piracy.

58. Music and film piracy are primarily facilitated on the net by FIOs or Rogue Websites. They are those websites which primarily and predominantly share infringing/pirated content or illegal work (See: Para 2 of Order dated 29.07.2016 in *DEITY v. Star India Pvt. Ltd.*, FAO (OS) 57/2015). Either these websites, themselves allow streaming of content or provide a searchable database with links to third-party FIOs. The Registrant details of these websites are unknown and any or all contact information is masked/blocked. Even the Ad Networks employed on these websites are not run-of-the-mill popular networks, but obscure Ad Networks, with equally anonymized credentials. These websites invite consumers for watching free movies/contents. Although, some of these websites feebly claim to only provide links to third-party websites and not host content on their servers, yet their entire module/interface is premised on allowing users to watch pirated releases/movies by way of links, and which account for all the content available on their sites.

59. In the opinion of this Court, some of the factors to be considered for determining whether the website complained of is a FIO/Rogue Website are:—

- a. whether the primary purpose of the website is to commit or facilitate copyright infringement;
- b. the flagrancy of the infringement, or the flagrancy of the facilitation of the infringement;
- c. Whether the detail of the registrant is masked and no personal or traceable detail is available either of the Registrant or of the user.
- d. Whether there is silence or inaction by such website after receipt of take down notices pertaining to copyright infringement.
- e. Whether the online location makes available or contains directories, indexes or categories of the means to infringe, or facilitate an infringement of, copyright;
- f. Whether the owner or operator of the online location demonstrates a disregard for copyright generally;
- g. Whether access to the online location has been disabled by orders from any court of another country or territory on the ground of or related to copyright infringement;
- h. whether the website contains guides or instructions to circumvent measures, or any order of any court, that disables access to the website on the ground of or related to copyright infringement; and i. the volume of traffic at or frequency of access to the website;
- j. Any other relevant matter.

60. This Court clarifies that the aforementioned factors are illustrative and not exhaustive and do not apply to intermediaries as they are governed by IT Act, having statutory immunity and function in a wholly different manner.

WHETHER THE TEST FOR DETERMINING A ROGUE WEBSITE IS QUALITATIVE OR A QUANTITATIVE ONE?

61. This Court finds that globally, Courts examine whether the primary purpose and effect of the website is to facilitate infringement as opposed to examining purely the quantity of infringing content on the website.

62. Indeed, in the case of *Eros International Media Ltd. v. Bharat Sanchar Nigam Ltd.*, Suit No.

751/2016, as suggested by the learned Amicus Curiae, a learned Single Judge of the Bombay High Court held that for a blocking order to be passed against the entirety of a website, it must be shown by the plaintiffs that they have found the entire website to contain only illicit and infringing material with no legitimate content whatsoever. The Bombay High Court in the said case had raised certain doubts regarding the veracity of the evidence filed by the plaintiffs in that case because after a random check of the evidence, it was observed that some evidence was filed seeking blocking of resale of genuine CDs of a film as well. It was in this context that the Court formulated a three step verification process, which the Court directed ought to be followed in future matters where blocking orders are sought. The three-steps included:

- a. A verification and assessment by an external agency of the web links and URLs that are infringing, accompanied by a letter in writing;
- b. A second level of verification by the deponent of the Affidavit along with the Plaintiffs' Advocates; and c. The said Affidavit is on Oath.

63. However, in the case of *Department of Electronics and Information Technology v. Star India Pvt. Ltd.*, FAO(OS) 57/2015, a Division Bench of this Court followed a qualitative approach instead of the quantitative approach suggested by the Bombay High Court by observing that the rogue websites are overwhelmingly infringing and therefore prima facie the stringent measure to block the website as a whole was justified. It further held that blocking of specific URLs will not be sufficient due to the ease with which a URL can be changed. The task of continuously identifying each offending URL would be a gargantuan task and at the same time would be useless as the rogue websites could change these URLs within seconds. Relevant portion of the Division Bench judgment is reproduced hereinbelow: —

- "11. The steps to change a URL would require, to firstly access the source code of the infringing website and then change the alpha-numeric character string of the URL. This could be as easy as changing the password of one's e-mail ID. This would mean that if the URL of a rogue website is blocked, the operator can simply log into the website source code and change the URL akin to a person changing one's password. To give an example, a rogue website www.abc.com whose URL is www.abc.com/india-v-pakistan, can simply log into the website source code and insert the letter 's' after the letter 'v' and change the URL to www.abc.com/india-vs-pakistan. Thus, if the URL www.abc.com/inidia-v-pakistan is blocked, the infringer can start operating on the URL www.abc.om/india-vs-pakistan within a few seconds. But, if a domain name itself is blocked, to continue with the infringing activity becomes a cumbersome, time consuming and money spending exercise. A new domain name has to be created and purchased apart from purchase of a fresh hosting server space. The entire exercise of creating a website has to be undertaken.*
- 12. Suffice it to state that where infringement on the internet is not in dispute, a judicial response must factor in the comparative importance of the rights that are engaged because the very act of infringement is the justification for interfering with those rights. Therefore, the availability of alternative measures which are less onerous need to be considered. The cost associated with the measures which would include the cost of implementing the measures, also has to be taken into account. The efficacy of the measures which are ordered to be adopted by the ISPs have also to be kept in mind.*
- 13. Now, an ISP could argue that the lesser measure to block the URL would suffice. This argument stands to logic and reason, but would have no content where the offending activity by the rogue website is to carrying on hardly any lawful business and in its entirety or to a large extent, piracy is being resorted to.*
- 14. The respondent has placed enough material in the suit to show that the rogue websites are indulging in rank piracy and thus prima facie the stringent measure to block the website as a whole is justified because blocking a URL may not suffice due to the ease with which a URL can be changed, and as noted above, the number of URLs of the rogue websites range between 2 to 2026 and cumulatively would be approximately 20,000. It would be a gargantuan task for the respondent to keep on identifying each offending URL and especially keeping in view that as and when the respondent identifies the URL and it is blocked by the ISP, the rogue website, within seconds can change the URL thereby frustrating the very act of blocking the URL."*

64. The aforesaid Division Bench judgment, which is a binding judgment, is subsequent in time to the Bombay High Court order.

65. Moreover, the Bombay High Court order was passed in a *quia timet* action for an injunction order against the potential infringement of a movie that was yet to be released. The evidence that

was filed, related to past infringements connected with other films of the plaintiffs. In such an instance, the learned Single Judge felt it was imperative to strictly follow the above three-step verification. However, the present case is based on actual infringement and not *quia timet* action.

66. Further, in the opinion of this Court, if the standard of proof proposed by the learned Amicus Curiae were to be applied, the burden on every right owner would be disproportionate and onerous as it would have to first identify the owners of each of the content available on a website (which could be thousands in number) and thereafter, seek a declaration from each of the owners that the content being provided is illegal and unauthorised. Such a test would virtually ensure that no website would ever be eligible for a takedown/blocking order and would render the right owners remediless.

67. In fact, the analysis of the learned Amicus Curiae of the defendant-websites is based purely on alphanumeric variation website which became alive subsequent to the blocking order and which re-directed one to the primary infringing website - a fact itself shows the rogue nature of the website.

68. This Court is also of the opinion that if the test to declare a website as a rogue website is that it should contain only illicit or infringing material, then each and every rogue website would add a small percentage of legitimate content and pray that it be not declared an infringing website!

69. Consequently, the real test for examining whether a website is a Rogue Website is a qualitative approach and not a quantitative one.

WHETHER THE DEFENDANT-WEBSITES FALL IN THE CATEGORY OF ROGUE WEBSITES?

70. In the present batch of matters, there is sufficient evidence on record to show that the main purpose of each of the thirty websites (arrayed as defendants) is to commit or facilitate copyright infringement and the defendants' websites provide access to a large library of films, including films of the plaintiffs without their authorisation. The websites had been designed to facilitate easy access to cinematograph films, including the subject films, in breach of the copyright in those films. They contain indexes of the films, which are categorised including by quality, genre, viewership and ratings. Instructions to circumvent measures taken to disable access were also found on a number of these websites, as evidenced by screenshots of posts, which show the owner or operator of the websites informing users of a change of domain name for the websites. In fact, the infringing nature of the defendants' websites is apparent from the fact that their WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user; DMCA (Digital Millennium Copyright Act) declaration is an eyewash as despite receipt of legal notice from plaintiffs, infringing content is still being played and access to the online location had been disabled by orders of another country on the ground of copyright infringement. A chart showing the infringing nature of the defendant websites is reproduced hereinbelow:—

UTV Software Communications Ltd. v. Bmovies.is CS(COMM) 768/2018

S. No.	Criteria	Particulars	Page No.
1.	Primary purpose is copyright infringement	a) WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user. b) DMCA (Digital Millennium Copyright Act) declaration an eyewash as despite receipt of legal notice from plaintiffs, no action taken. c) Infringing content was still being played after receipt of legal notice	@4 @145 & 158 @72
2.	Index/directories	Indexes/categories	@60 (homepage)
3.	Disregard for copyright	DMCA declaration not given effect to	@145

4.	Court Orders (International)	a) Australia	@259 and @ 265 [@263 & 272 also websites in suit]
----	---------------------------------	--------------	--

UTV Software Communications Ltd. v. Rarbg.is CS(COMM) 776/2018

S. No.	Criteria	Particulars	Page No.
1.	Primary purpose is copyright infringement	a) WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user. b) Legal Notices c) Content Playing after Legal Notice	@5 @ 175 @58
2.	Index/directories	Indexes/categories	@46
3.	Disregard for copyright	a) Legal Notices b) Content Playing after Legal Notice	@175 @58
4.	Court Orders (International)	a) Portugal b) Australia	@142-154
5.	Circumvention of court orders	Advertisement to unblock blocked websites	@18

UTV Software Communications Ltd. v. Extratorrent.ag CS(COMM) 799/2018

S. No.	Criteria	Particulars	Page No.
1.	Primary purpose is copyright infringement	a) WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user. b) DMCA (Digital Millennium Copyright Act) declaration an eyewash as despite receipt of legal notice from plaintiffs, no action taken. c) Legal Notices d) Content Playing after Legal Notice	@5 @64 @158 @86
2.	Index/directories	Indexes/categories	@10
3.	Disregard for copyright	DMCA/VPN	@64
4.	Court Orders (International)	a) Portugal b) Australia	@168 to 175
5.	Circumvention of Court orders	DMCA/VPN	@64

UTV Software Communications Ltd. v. Yts.am (COMM) 778/2018

1.	Primary purpose is copyright infringement	a) WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user. b) Legal Notice c) Content available	@5 @190 @88
----	---	--	-------------------

		after legal notice	
2.	Index/directories	Indexes/categories	@ 23 (source page)
3.	Disregard for copyright	a) Legal Notice b) Content available after notice c) VPN	@190 @88 @161
4.	Court Orders (International)	a) Portugal b) Australia	@164 @166
5.	Circumvention of Court orders	VPN	@161

UTV Software Communications Ltd. v. thepiratebay.org CS(COMM) 777/2018

S. No.	Criteria	Particulars	Page No.
1.	Primary purpose is copyright infringement	a) WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user. b) Legal Notices c) Content Playing after Legal Notice	@5 @130 @71
2.	Index/directories	Indexes/categories	@10
3.	Disregard for copyright	a) Legal Notices b) Content Playing after Legal Notice	@130 @71
4.	Court Orders (International)	a) Portugal b) Denmark	@116-117 @118, 120
5.	Circumvention of Court orders	VPN	@112

UTV Software Communications Ltd. v. Fmovies.pe CS(COMM) 770/2018

S. No.	Criteria	Particulars	Page No.
1.	Primary purpose is copyright infringement	a) WHOIS detail is masked and no personal or traceable detail is available either of the Registrant or of the user. b) DMCA (Digital Millennium Copyright Act) declaration an eyewash as despite receipt of legal notice from plaintiffs, no action taken. c) Legal Notices d) Content Playing after Legal Notice	@4 @149 @152 @34
2.	Index/directories	Indexes/categories	@34 @102-103
3.	Disregard for copyright	a) DMCA b) Legal Notices c) Content Playing after Legal Notice d) VPN	@149 @152 @34 @64

UTV Software Communications Ltd. v. Torrentmovies.pe CS(COMM) 800/2018

S. No.	Criteria	Particulars	Page No.
1.	Primary purpose is	a) WHOIS detail is	@5

	copyright infringement	masked and no personal or traceable detail is available either of the Registrant or of the user. b) DMCA (Digital Millennium Copyright Act) declaration an eyewash as despite receipt of legal notice from plaintiffs, no action taken. c) Legal Notices d) Content Playing after Legal Notice	@130 @149 @53
2.	Index/directories	Indexes/categories	@53-54
3.	Disregard for copyright	a) DMCA a) Legal Notices b) Content Playing after Legal Notice	@130 @149 @53

UTV Software Communications Ltd. v. 1337x.to CS(COMM) 724/2017

S. No.	Criteria	Particulars	Page No.
1.	Primary purpose is copyright infringement Copyright Act) declaration an eyewash as despite receipt of legal notice from plaintiffs, no action taken.	a) DMCA (Digital Millennium b) Legal Notices c) Content Playing after Legal Notice	@182 @213 @517 (Vol.3)
2.	Index/directories	Indexes/categories	@230
3.	Disregard for copyright	a) DMCA b) Legal Notices c) Content Playing after Legal Notice	@182 @213 @517 (Vo.3)
4.	Court Orders (International)	a) Portugal	@171

71. Consequently, in the present cases, the aforesaid "qualitative test" is satisfied for the following reasons:—

- The rogue websites do not provide any legitimate contact details, they hide behind veil of secrecy and are located in safe-havens and rarely comply with requests for takedown.
- The rogue websites facilitate infringement by providing features such as indexing, detailed search functions, categorization, etc. which make it very convenient for a user to search and download illegal content.
- The sample evidence filed by the plaintiffs is consistent with the criterion adopted globally by various courts to direct blocking of such websites, such as in Singapore and in Australia.
- The rogue websites encourage a user to circumvent detection or blocking orders by providing detailed instructions on how to avoid detection or access a blocked website.
- The rogue nature of these websites has already been accepted by courts in other jurisdictions such as in Australia and the Plaintiffs have duly filed such orders before this Court. Consequently, the question of whether these websites are indeed rogue websites and deserving a blocking order have already been dealt with by competent courts in other jurisdictions.
- Sample evidence has been filed considering the volumes of content of the website and in order to avoid making it an impractical, costly, ineffective, non-fruitful and time consuming exercise.
- The list of movies provided in the Plaint are admittedly an illustrative list and not an exhaustive one.

h) The volume of traffic to these websites is also indicative of their rogue nature.

72. Accordingly, for the foregoing reasons, it is held that the defendant-websites are rogue websites.

IT IS VERY DIFFICULT FOR INDIA OR OTHER COUNTRIES TO BRING CASES AGAINST FOREIGN DIGITAL PIRACY SITES. ABSENT CHANGE IN ATTITUDE OF GOVERNMENTS OF SCOFFLAW NATIONS, INDIA LIKE OTHER COUNTRIES, WILL NEED TO WORK WITH INTERNET INTERMEDIARIES AS THE MAIN SOLUTION.

73. However, fighting digital piracy gets much harder at the international level. This is because many countries that are home to digital piracy sites have governments that will not or cannot shut them down, whether because there are weak or non-existent intellectual property protections or for geopolitical reasons. From a multilateral legal perspective, it is very difficult for India or others to bring cases against foreign digital piracy sites. To succeed, India requires the cooperation of the foreign governments where the site is hosted, and despite the fact that virtually every nation that acts as a haven for piracy sites is in the World Trade Organization and is a signatory to the multilateral agreement protecting intellectual property-the Trade related Aspects of Intellectual Property Rights (TRIPS) agreement-many nations refuse to address digital piracy in their own jurisdictions. But, does that mean that as IPR laws are territorial, they can be violated with impunity by an infringer/intellectual property infringer just because he has committed infringement through a server hosted abroad.

74. Governments across the world have grappled to find the most effective ways to address the issue of piracy of copyrighted works online. This Court is in agreement with Mr. Nigel Cory's view that absent changes to the WTO, or a change in attitude of governments of scofflaw nations, India like other countries will need to work with Internet intermediaries as the main solution.

WHETHER THIS COURT WOULD BE JUSTIFIED TO PASS DIRECTIONS TO BLOCK THE 'ROGUE WEBSITES' IN THEIR ENTIRETY?

75. Website blocking has emerged as one of the most successful, cost effective and proportionate means to address this issue. As pointed out by the learned Amicus Curiae, website blocking can be of various kinds namely, Internet Protocol (IP) Address Blocking, Domain Name System (DNS) Blocking and Uniform Resource Locator (URL) Blocking.

76. In the opinion of this Court, the extent of website blocking should be proportionate and commensurate with the extent and nature of the infringement. In fact, a Court should pass a website blocking order only if it is satisfied that the same is 'necessary' and 'proportionate'.

77. While 'necessary' means a particular measure is essential to achieve that aim, i.e. whether there are other less restrictive means capable of producing the same result; 'proportionate' means it must be established that the measures do not have an excessive effect on the defendant's interest.

78. The proportionality principle requires that a 'fair balance' be struck between competing fundamental rights, i.e., between the right to intellectual property on the one hand, and the right to trade and freedom of expression on the other. A Division Bench of this Court in *Myspace Inc. v. Super Cassettes Industries Ltd.* (supra) has observed as under:—

"... 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 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."

79. In fact, keeping in view the proportionality principle, the Courts have refrained from passing orders requiring pre-filtering and proactive monitoring of the Internet.

80. In the opinion of this Court, while blocking is antithetical to efforts to preserve a "free and open" Internet, it does not mean that every website should be freely accessible. Even the most vocal supporters of Internet freedom recognize that it is legitimate to remove or limit access to some materials online, such as sites that facilitate child pornography and terrorism. Undoubtedly, there is a serious concern associated with blocking orders that it may prevent access to legitimate content. There is need for a balance in approach and policies to avoid unnecessary cost or impact on other interests and rights. Consequently, the onus is on the right holders to prove to the satisfaction of the Court that each website they want to block is primarily facilitating wide spread copyright infringement.

81. It is pertinent to mention that this Court in *Dr. Shashi Tharoor v. Arnab Goswami*: 2017 SCC

OnLine Del 12049, has held that in India, the Courts have the power to pass the pre-publication or pre-broadcasting injunction, provided the two-pronged test of necessity and proportionality is satisfied.

82. One can easily see the appeal in passing a URL blocking order, which adequately addresses over-blocking. A URL specific order need not affect the remainder of the website. However, right-holders claim that approaching the Court or the ISPs again and again is cumbersome, particularly in the case of websites promoting rampant piracy.

83. This Court is of the view that to ask the plaintiffs to identify individual infringing URLs would not be proportionate or practicable as it would require the plaintiffs to expend considerable effort and cost in notifying long lists of URLs to ISPs on a daily basis. The position might have been different if defendants' websites had a substantial proportion of non-infringing content, but that is not the case.

84. This Court is of the view that while passing a website blocking injunction order, it would have to also consider whether disabling access to the online location is in the public interest and a proportionate response in the circumstances and the impact on any person or class of persons likely to be affected by the grant of injunction. The Court order must be effective, proportionate and dissuasive, but must not create barriers to legitimate trade. The measures must also be fair and not excessively costly (See: *Loreal v. Ebay*, [Case C 324/09]).

85. In *Cartier International AG v. British Sky Broadcasting Limited*, [2014] EWHC 3354 (Ch), it has been held by the Hon'ble Mr. Justice Arnold that alternate measures are not effective and not a complete answer to rampant piracy. The relevant portion of said judgment is reproduced hereinbelow:—

"Availability of alternative measures

197. *The ISPs' arguments and evidence in the present case focussed heavily on the availability of alternative measures...*

198. *Action against the operators. The first step which Richemont could take, and have taken, is to send cease and desist letters to the named registrants of the domain names as identified by a WHOIS search. Unsurprisingly, these letters were simply ignored.... Accordingly, I do not consider that this is a realistic alternative measure.*

199. *Notice and takedown by hosts. The second step which Richemont could take, but have not taken, is to send notices to the hosts of the Target Websites demanding that the Target Websites be taken down...*

xxx xxx xxx

201. *More importantly, Richemont contend that notice and takedown is ineffective because, as soon as an offending website is taken down by one host, the almost invariable response of the operator is to move the website to a different host.... Accordingly, I consider that, while Richemont are open to criticism for not even having attempted to use this measure, it is unlikely that it would be effective to achieve anything other than short-term disruption of the Target Websites.*

xxx xxx xxx

204. *I accept that website blocking has advantages over notice-and-takedown. Accordingly, I am not persuaded that, overall, notice-and-takedown is an equally effective, but less onerous, measure....*

205. *Payment freezing. A third measure which Richemont could adopt, but have not adopted, is to ask the payment processors used by the Target Websites, such as Visa, MasterCard and Western Union, to suspend the operators' merchant accounts.....*

206.*there are two problems with this approach. The first is that, although it may diminish the circulation of counterfeit goods, it leaves the offending website untouched. Thus at least the first category of infringement will continue until such time as the website is so starved of funds that it ceases operation, assuming that that time does come. The second is that, as with notice-and-takedown, the websites simply shift to alternative payment methods.....*

207. *My conclusion....it is unlikely that this would be effective to achieve more than some degree of disruption to the Target Websites. Again, therefore, I do not regard the availability of this alternative measure as a complete answer to Richemont's application.....*

208. *Domain name seizure. A fourth measure which Richemont could adopt, but have not adopted, is to seize the domain names of the Target Websites by invoking the dispute resolution procedures ("DRPs") of the registrar through which the domain names have been purchased.....*

Again, however, the problem is that the website operator can simply pick a new domain name and start again. Accordingly, I am not persuaded that this is a realistic alternative measure in general, although there may be particular cases where it has some value.

xxx xxx xxx

210. *De-indexing.* A fifth measure which the ISPs contend that Richemont could adopt, but have not adopted, is to send notices to search engine providers such as Google requesting them to “de-index” the Target Websites. This would have the effect of removing the website from the search engine’s search results....

xxx xxx xxx

212.there are three problems with this approach. The first is that search engine providers are not willing to de-index entire websites on the basis of alleged intellectual property infringements without a court order....

213. The second problem is that, whereas some search engine providers like Google.....do not have an equivalent policy for URLs which infringe third party trade marks.

214. The third problem is that, even if search engine providers de-index the URL or even the entire website, it will remain accessible on the internet. In particular, it would remain accessible to consumers who had previously visited the website and either had it bookmarked or could remember its domain name.....

215. Accordingly, I conclude that, as matters stand, this is not a realistic alternative measure for Richemont.

216. *Customs seizure.* A final measure is that of customs seizure.....The first is that it only tackles the imports of the counterfeit goods themselves. It does not affect the Target Websites. The second is that it is impossible for customs to inspect anything more than a small fraction of the large volume of small parcels.....

217. *Conclusion.....*I am not persuaded that there are alternative measures....which would be equally effective, but less burdensome.....Nevertheless, I do accept that the availability of some of the measures discussed above is a factor to be taken into account in assessing the proportionality of the orders sought by Richemont.”

(emphasis supplied)

86. Consequently, website blocking in the case of rogue websites, like the defendant-websites, strikes a balance between preserving the benefits of a free and open Internet and efforts to stop crimes such as digital piracy.

87. This Court is also of the opinion that it has the power to order ISPs and the DoT as well as MEITY to take measures to stop current infringements as well as if justified by the circumstances prevent future ones.

AT LEAST FORTY-FIVE COUNTRIES HAVE EITHER ADOPTED AND IMPLEMENTED, OR ARE LEGALLY OBLIGATED TO ADOPT AND IMPLEMENT MEASURES TO ENSURE THAT ISPS TAKE STEPS TO DISABLE ACCESS TO COPYRIGHT INFRINGING WEBSITES.

88. At least forty-five countries have either adopted and implemented, or are legally obligated to adopt and implement, measures to ensure that ISPs take steps to disable access to copyright infringing websites. These countries include the UK, Australia, Singapore, Portugal, France, Germany and India (*Site Blocking in the World, MPA Study on Site Blocking Impact in South Korea, June 2016*). Around the world, ISPs receive directions to block websites either from Courts or from administrative agencies/other competent authorities. The majority of governments where such relief is available have adopted the judicial approach, which involves ISPs blocking specific websites pursuant to criminal and civil Court orders, e.g. most EU Member States (including the UK), India, Singapore and Australia. A few additional countries like South Korea, Portugal, Italy, Malaysia and Indonesia have adopted an administrative approach where government agencies direct ISPs to block specific piracy services. In both these methods the approach is similar, whereby right owners establish that the target website provides access to infringing content. Courts and administrative agencies review the evidence to ensure that websites engaged in predominantly legal activities are not blocked. Following such assessment, directions are issued by the Court or administrative agency to ISPs to block specific infringing websites.

89. This Court is also of the view that it can take a cue from the years of experience of dozens of governments/jurisdictions that have successfully adopted website blocking regimes primarily by directing the ISPs to permanently block the identified websites. In the United Kingdom, blocking orders directed at 19 major online infringing sites in October/November 2013 not only led to

significant decrease in total piracy, but also led to significant increase in the usage of legal streaming sites. (Danaher, Brett and Smith, Michael D. and Telang, Rahul, *The Effect of Piracy Website Blocking on Consumer Behaviour* (November 2015), <https://ssrn.com/abstract=2612063>).

90. In the Asia-Pacific region, research results of South Korea's administrative site-blocking regime demonstrated the same positive impacts that the studies conducted in Europe showed. Visits to blocked sites declined significantly within three months of access being blocked. As website blocking in South Korea was heavily concentrated on peer-to-peer (P2P) sites, overall visits to infringing P2P sites (not just those sites blocked) showed a 51% decline three-months after the three rounds of website blocking. (Motion Picture Association, *MPA Study on Site Blocking Impact in South Korea* (2016) (http://www.mpa-i.org/wp-content/uploads/2018/01/MPAA_Impact_of_Site_Blocking_in_South_Korea2016.pdf)).

91. Most recently, research conducted by INCOPRO released in 2018 demonstrated that site-blocking in Australia had also had a significantly positive impact upon the usage of blocked infringing sites. Tracking Alexa data recorded usage reduction of 53.4% of blocked sites, usage of the top-50 infringing sites in Australia decreased by 35.1% since October 2016, usage of the top-250 infringing sites in Australia decreased by 25.4% from October 2016 to November 2017. (Incopro, *Site Blocking Efficacy-Key Findings-Australia* (February 2018) (https://www.creativecontentaustralia.org.au/_literature_210629/2018_Research_-_Incopro_Study)).

92. These studies demonstrate that site-blocking in those countries greatly contributed to: (1) reduction of usage of infringing websites to which access had been blocked; and (2) reduction of overall usage of infringing websites. As a consequence, there is every reason to believe that the same results of website blocking measures would hold true in India.

93. Undoubtedly, website blocking is 'no silver bullet' in the fight against digital piracy, but it should at least be one of the lead bullets, alongside other measures such as partnering with Internet ad companies, domain seizures, and other efforts to prosecute owners of pirate sites. *HOW SHOULD THE COURT DEAL WITH THE 'HYDRA HEADED' 'ROGUE WEBSITES WHO ON BEING BLOCKED, ACTUALLY MULTIPLY AND RESURFACE AS REDIRECT OR MIRROR OR ALPHANUMERIC WEBSITES?*

94. Now, the question that arises for consideration is how should courts deal with 'hydra headed' websites who on being blocked, actually multiply and resurface as alphanumeric or mirror websites. In the present batch of matters though this Court had injuncted the main website by way of the initial injunction order, yet the mirror/alphanumeric/redirect websites had been created subsequently to circumvent the injunction orders.

95. It is pertinent to mention that in Greek mythology the Hydra also called Lernaean Hydra is a serpent-like monster. The Hydra is a nine-headed serpent like snake. It was said that if you cut off one hydra head, two more would grow back.

96. Critics claim that website blocking is an exercise in futility as website operators shift sites-the so-called "whack-a-mole" effect.

97. Internationally, there has been some recent development to deal with the aforesaid menace in the form of a "Dynamic Injunction" though limited to mirror websites.

98. The High Court of Singapore in the case of *Disney Enterprise v. MI Ltd.*, (2018) SGHC 206 has after discussing the cases of *20th Century Fox v. British Telecommunications PLC*, (2012) 1 All ER 869 and *Cartier International AG v. British Sky Broadcasting* (supra), held that the applicant was not obligated to return to court for an order with respect to every single IP address of the infringing URLs already determined by the Court. The Court held as under:—

"38 I found that the court has the jurisdiction to issue a dynamic injunction given that such an injunction constitutes "reasonable steps to disable access to the flagrantly infringing online location". This is because the dynamic injunction does not require the defendants to block additional FIOs which have not been included in the main injunction. It only requires the defendants to block additional domain names, URLs and/or IP addresses that provide access to the same websites which are the subject of the main injunction and which I have found constitute FIOs (see [19] - [29] above). Therefore, the dynamic injunction merely blocks new means of accessing the same infringing websites, rather than blocking new infringing websites that have not been included in the main injunction.

39 In fact, under the dynamic injunction applied for in the present case, the plaintiffs would be required to show in its affidavit that the new FQDNs provide access to the same FIOs which are

the subject of the main injunction before the defendants would be required to block the new FQDNs (see

[6] above) ...

xxx xxx xxx

42. In relation to S 193DB(3)(d) of the Copyright Act, ie, the effectiveness of the proposed order, the dynamic injunction was necessary to ensure that the main injunction operated effectively to reduce further harm to the plaintiffs. This is due to the ease and speed at which circumventive measures may be taken by owners and operators of FQDNs to evade the main injunction, through for instance changing the primary domain name of the FQDN. Without a continuing obligation to block additional domain names, URLs and/or IP addresses upon being informed of such sites, it is unlikely that there would be effective disabling of access to the 53 FQDNs."

(emphasis supplied)

99. Though the dynamic Injunction was issued by the Singapore High Court under the provisions of Section 193 DDA of the Singapore Copyright Act, and no similar procedure exists in India, yet in order to meet the ends of justice and to address the menace of piracy, this Court in exercise of its inherent power under Section 151 CPC permits the plaintiffs to implead the mirror/redirect/alphanumeric websites under Order I Rule 10 CPC as these websites merely provide access to the same websites which are the subject of the main injunction.

100. It is desirable that the Court is freed from constantly monitoring and adjudicating the issue of mirror/redirect/alphanumeric websites and also that the plaintiffs are not burdened with filing fresh suits. However, it is not disputed that given the wide ramifications of site-wide blocking orders, there has to be judicial scrutiny of such directions and that ISPs ought not to be tasked with the role of arbiters, contrary to their strictly passive and neutral role as intermediaries.

101. Consequently, along with the Order I Rule 10 application for impleadment, the plaintiffs shall file an affidavit confirming that the newly impleaded website is a mirror/redirect/alphanumeric website with sufficient supporting evidence. On being satisfied that the impugned website is indeed a mirror/redirect/alphanumeric website of injuncted Rogue Website(s) and merely provides new means of accessing the same primary infringing website, the Joint Registrar shall issue directions to ISPs to disable access in India to such mirror/redirect/alphanumeric websites in terms of the orders passed.

102. It is pertinent to mention that this Court has delegated its power to the learned Joint Registrar for passing such orders under Section 7 of the Delhi High Court Act, 1966 read with Chapter II, Rule 3(61) read with Rule 6 of the Delhi High Court (Original Side) Rules 2018. The said provisions are reproduced hereinbelow:—

"3. Powers of the Registrar- The powers of the Court, including the power to impose costs in relation to the following matters, may be exercised by the registrar:

(61) Such other application, as by these Rules are directed to be so disposed of by the Registrar, but not included in this Rule and any other matter, which in accordance with orders or directions issued by Court, is required to be dealt with by the Registrar.

6. Delegation of the Registrar's Power - The Chief Justice and his companion Judges may assign or delegate to a Joint Registrar, Deputy Registrar or to any officer, any functions required by these Rules to be exercised by the Registrar.

103. In the event, any person is aggrieved by any order passed by the Registrar, the remedy for appeal is provided and may be availed of under Rule 5 of Chapter II of the Delhi High Court (Original Side) Rules, 2018 reproduced hereinbelow:—

"5. Appeal against the Registrar's orders.- Any persons aggrieved by any order made by the Registrar, under Rule 3 of this Chapter, may, within fifteen days of such order, appeal against the same to the Judge in Chambers. The appeal shall be in the form of a petition bearing court fees of Rs. 2.65."

SUGGESTION

104. This Court is of the view that since website blocking is a cumbersome exercise and majority of the viewers/subscribers who access, view and download infringing content are youngsters who do not have knowledge that the said content is infringing and/or pirated, it directs the MEITY/DOT to explore the possibility of framing a policy under which a warning is issued to the viewers of the infringing content, if technologically feasible in the form of e-mails, or pop-ups or such other modes cautioning the viewers to cease viewing/downloading the infringing material. In the event the

warning is not heeded to and the viewers/subscribers continue to view, access or download the infringing/pirated content, then a fine could be levied on the viewers/subscribers.

105. This measure, in the opinion of this Court, would go a long way in curbing the pirated content and the dark-net as well as in promoting the legal content and accelerating the pace of 'Digital India'.

THIS COURT PLACES ON RECORD ITS APPRECIATION FOR THE SERVICES RENDERED BY LEARNED AMICUS CURIAE AS WELL AS LEARNED COUNSEL FOR PLAINTIFFS

106. This Court places on record its appreciation for the services rendered by Mr. Hemant Singh, learned Amicus Curiae as well as Mr. Saikrishna Rajagopal and the team of Advocates assisting them. They not only handed over innumerable notes, charts and articles, but explained with great patience certain technologies that this Court was not familiar with.

RELIEF

107. Keeping in view the aforesaid findings, a decree of permanent injunction is passed restraining the defendant-websites (as mentioned in the chart in paragraph no. 4(i) of this judgment) their owners, partners, proprietors, officers, servants, employees, and all others in capacity of principal or agent acting for and on their behalf, or anyone claiming through, by or under it, from, in any manner hosting, streaming, reproducing, distributing, making available to the public and/or communicating to the public, or facilitating the same, on their websites, through the internet in any manner whatsoever, any cinematograph work/content/programme/show in relation to which plaintiffs have copyright. A decree is also passed directing the ISPs to block access to the said defendant-websites. DoT and MEITY are directed to issue a notification calling upon the various internet and telecom service providers registered under it to block access to the said defendant-websites. The plaintiffs are permitted to implead the mirror/redirect/alphanumeric websites under Order I Rule 10 CPC in the event they merely provide new means of accessing the same primary infringing websites that have been enjoined. The plaintiffs are also held entitled to actual costs of litigation. The costs shall amongst others include the lawyer's fees as well as the amount spent on Court-fees. The plaintiffs are given liberty to file on record the exact cost incurred by them in adjudication of the present suits. Registry is directed to prepare decree sheets accordingly.

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.