UNDERSTANDING NON-CONSENSUAL DISSEMINATION OF INTIMATE IMAGES LAWS IN INDIA WITH FOCUS ON INTERMEDIARY LIABILITY

*Vaishnavi Sharma**

From the generally conservative and patriarchal approach of the courts towards pornography, to the paternalistic, welfare legislations enacted to 'protect' certain classes of the population, obscenity laws operate in and further churn an obscenity narrative that actively disables sexual autonomy, especially of women and minorities that often face the brunt of these exercises. This article argues that the extant legal regime relating to the non-consensual dissemination of intimate images is weak and non-developed in India, both, in terms of identification as an offence, and availability of remedies. Specifically, this article highlights the roles of certain sections of the Information Technology Act, 2000, that work in tandem to disable appropriate juridical and practical application of provisions that give due regard to privacy and consent concerns in matters concerning non-consensual dissemination of intimate images. Legislature and courts must give due regard to these concerns if they seek to curb the proliferation of cybercrimes online and build a more free and participative digital citizenship.

TABLE OF CONTENTS

I. INTRODUCTION

In this digital age, we have, through acquiescence, incarcerated ourselves in a digital surveillance system – our actions, our thoughts, our privacy, all infiltrated by unwanted, prying eyes. India has around 624 million internet users and about 448 million social media users, constituting forty-five percent and thirty-two percent of the country's total population,

* The author is a fourth-year law student at Maharashtra National Law University, Mumbai. She is grateful to the editors of the NUJS Law Review for their invaluable editorial assistance. For any comments or feedback, she may be contacted at vaisu09sharma@gmail.com.

respectively.[1] With this significant participation in cyber activities, there has been an alarming increase in cybercrimes. In fact, according to the statistics published by the National Crime Records Bureau, there was a sixty-three percent increase in cybercrimes from 2018 to 2019[2] (cybercrimes against women accounted for nearly one-fifth of all cybercrimes registered in 2019).[3]

One such technology-enabled crime is the non-consensual dissemination of intimate images,[4] which involves the distribution of sexually graphic images of individuals without their consent.[5] Non-consensual dissemination of intimate images via the internet as a medium had initially grabbed the media and legislature's attention when certain 'revenge porn' websites started popping up on the internet. The phenomenon gained even more attention later when celebrities became victims to it.[6] There has been a growing concern for non-consensual dissemination of intimate images in India, as is evident with the release of the new Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 ('IT Rules 2021')[7] that were enacted, *inter alia*, to curb the proliferation of 'revenge porn'.[8] Now, with the onslaught of Covid-19, gender, racial and social prejudices have only aggravated as women and minorities have been coerced into confinement with their partners and families, with far reaching and long-lasting ramifications, yet to be fully realised.[9]

Non-consensual dissemination has been known to cause anxiety, panic attacks, severe emotions of humiliation and shame, potential unemployment, lower self-esteem, verbal

---

[1] Simon Kemp, *Digital 2021: India*, DATAPORTAL, February 11, 2021, available at https://datareportal.com/reports/digital-2021-india (Last visited March 14, 2022).

[2] 27248 in 2018; NATIONAL CRIME RECORDS BUREAU, *Cyber Crime- IT Act Cases (Crime Head-wise & State/UT-wise) 2018*, available at https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.2.pdf (Last visited on March 14, 2022).

[3] 44546 in 2019; NATIONAL CRIME RECORDS BUREAU, *Cyber Crime- IT Act Cases (Crime Head-wise & State/UT-wise) 2019*, available at https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.2_0.pdf (Last visited on March 14, 2022) (Notably, §66E offences are categorised under 'violation of privacy', separate from the 'Publication/transmission of obscene/ sexually explicit act in electronic form' that includes only §67 offences. This exclusion of §66E from obscenity portrays a larger disregard of this section and its ingredients of privacy and consent, and the larger narrative with which obscenity. This has evolved in India that fixes its attention on regulating the production of women's bodies and absolutely discounts questions of consent, focusing on a distorted version of privacy).

[4] It must be noted that the phrase 'revenge pornography' is a subset of non-consensually dissemination of intimate images; it steals the attention away from the action of the perpetrator and fails to cover all scenarios. Furthermore, the usage of 'pornography' is again misleading for it assumes that the media was taken with consent, which is not the case here. *See* Miha Šepec, *Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence*, 13(2) INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY (2019).

[5] Danielle Keats Citron & Mary Anne Franks, *Criminalising Revenge Porn*, 49 WAKE FOREST L. REV. 102 (2014).

[6] *Id.*, at 120-121. One of the first prominent revenge porn websites was created in 2020 by Hunter Moore called 'Is Anyone Up?'. Moore gained substantial profits from the site and was later prosecuted, not for the content posted but for the violation of 'several federal laws'.

[7] Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021.

[8] THE HINDU, *Govt. announces new social media rules to curb its misuse*, February 26, 2021, available at https://www.thehindu.com/news/national/govt-announces-new-social-media-rules/article33931290.ece (Last visited December 22, 2021).

[9] *See* United Nations Human Rights Council, Special Rapporteur on Violence Against women, its Causes and Consequences, *Intersection between the coronavirus disease (COVID-19) pandemic and the pandemic of gender-based violence against women, with a focus on domestic violence and the "peace in the home" initiative*, U.N. Doc. A/HRC/38/47 (June 18, 2018).

and physical harassment, stalking, etc.[10] To alleviate such extreme feelings, victims have been known to have turned towards negative coping mechanisms leading to the manifestation of various extreme behaviours such as avoidance, denial, excessive drinking, obsessing over their victimisation, self-medication.[11] Often, personal details of the victim are posted online alongside the images, exacerbating these harms. This information can be anything – from social media usernames to mobile numbers to even home addresses, and carry with them the apprehension of physical stalking, targeted public humiliation, unemployment, etc.[12] Non-consensual dissemination is a veritable consequence and cause of violence against women, both online and offline – eerily similar to that of sexual assault.[13]

As shall be discussed in this paper, despite having both civil and criminal recourses, the legal system disables them for the victims by either making them infructuous or by making them inaccessible to an ordinary individual.[14] While there is considerable research on this topic globally, the present legal regime in India presents a unique situation that is quite distinct from other jurisdictions.

The primary issue this essay deals with is whether the law sufficiently anticipates and deals with the non-consensual dissemination of intimate images as a crime ex-ante and ex-post. The hypothesis with which this research essay will proceed is that the extant legal framework, while being juristically adequate from a consequentialist's point of view (at least for the violator), severely fails to be a viable avenue for victims due to the present legal deficits and defects in the administration of justice in this regard.

This essay is divided into four parts. Part II broadly addresses the constitutional challenges non-consensual dissemination laws have faced, and might still face; Part III addresses the legal concoction of laws that can be availed by the victim, and how the presence and application of these laws is rendered vain. Part IV deals with the larger obscenity argument surrounding sexually explicit photos in the context of non-consensual and consensual dissemination. Part V addresses the most effective recourses available to victims, with special focus on intermediary liability and the issues with the grievance redressal mechanism under the IT Rules 2021. Part VI will conclude.

[10] CITRON & FRANKS, *supra* note 5, at 105-106, 117; *See also* Samantha Bates, *Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors*, 12(1) FEMINIST CRIMINOLOGY (2017).

[11] *Id*, at 14.

[12] Zak Franklin, *Justice for Revenge Porn Victims: Legal Theories to Overcome Claims of Civil Immunity by Operators of Revenge Porn Websites*, 102(5) CALIFORNIA L. REV. 1303, 1308-1309 (2014).

[13] Jordan Fairborn, *Rape Threats and Revenge Porn: Defining Sexual Violence in the Digital Age* in eGIRLS, eCITIZENS 229-251 (Jane Bailey and Valerie Steeves, University of Ottawa Press); BATES, *supra* note 10 (the writer had conducted detailed interviews of 18 female revenge porn survivors to gauge the mental health effects of revenge porn and had concluded that non-consensual survivor reflects similar negative mental health outcomes that rape survivors' experiences).

[14] Consider the financial, emotional and social costs attached to rape trials, where the active disdain and disregard of the law enforcement and the courts not only discourages reporting, but also actively persecutes and exploits the victims further. *See generally* Preeti Pratishruti Dash, *Rape adjudication in India in the aftermath of Criminal Law Amendment Act, 2013: findings from trial courts of Delhi*, 4(2) INDIAN LAW REVIEW (June, 2020) (While rape trials are time-bound processes, the apparent lack of prescribed time limits in case of non-consensual dissemination, despite being recognised as violence against women, is alarming, to say the least).

II. UNDERSTANDING THE LEGAL BATTLES SURROUNDING NON-CONSENSUAL DISSEMINATION LAWS

Non-consensual dissemination of intimate images has gained momentum with the advent and progress of technology and social media.[15] It is a severe violation of an individual's online sexual privacy, a part of the more extensive online sexual surveillance and exploitation system that works primarily for material incentives.[16] Technology has provided a much more efficient and harmful method of disseminating non-consensual media.[17] The affordances of online activity allow for a unique, declarative form of monologue that enables a larger gender hegemony – majorly amplified extrapolations of offline heteronormative misogyny and sexism to online.[18] The dynamic and ever-evolving nature of online spaces perpetually keeps transforming our spatial sense of boundaries, in turn leading to material changes in social norms and resultant inter-personal relationships. Once non-consensual media is obtained and posted online, they get immortalised, migrating across websites, making them near impossible to remove. This entire practise, like most social media engagements, is heavily influenced by, and further influences, the set gendered prejudices.[19]

With cyberspace offering an alternate pane of communication and existence, the importance of defining the legal boundaries attached to non-consensual dissemination of intimate images/revenge porn provisions assumes great importance. These provisions tend to be controversial; they are either too narrow to be efficacious or too vague and overbroad to withstand constitutional challenges.[20] Internationally, many jurisdictions have taken active steps towards punishing non-consensual dissemination.[21]

It is primarily a content-based offense, in that it criminalises the content of the images that were distributed. As an offence, non-consensual dissemination of intimate images largely covers various scenarios. This includes the initial consensual capturing of the image with subsequent non-consented dissemination of that image,[22] a consensually captured image being stolen, or the non-consensual capturing of the image and its further non-consensual dissemination (this also includes instances rape).[23]

---

[15] CITRON & FRANKS, *supra* note 5, at 105.

[16] *See* Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62(6) William & Mary L. Rev. 24 (2020).

[17] Non-consensual pornography is not a modern concept and has simply found a newer and more efficient medium. Interestingly, however, the term 'revenge porn' entered the dictionary not long ago as opposed to non-consensual pornography.

[18] MATHEW HALL & JEFF HEARN, REVENGE PORNOGRAPHY: GENDER, SEXUALITIES AND MOTIVATIONS 124-131 (Routledge 2018).

[19] These prejudices, as has been noted, can be both subtle and aggressive – imagine the daily role of social media in objectifying, sexualising and commodifying women, to more hostile online engagements often found within 'manospheres'. *See* Stefanie E. Davis, *Objectification, sexualization, and Misrepresentation: Social Media and the College Experience*, SAGE SOCIAL MEDIA + SOCIETY (2018); Tracie Farrell et al., *Exploring Misogyny across the Manosphere in Reddit*, WEBSCI'19 PROCEEDINGS OF THE 10TH ACM CONFERENCE ON WEB SCIENCE (2019).

[20] *See* CITRON & FRANKS, *supra* note 5; K. Walker & E. Sleath, *A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media*, 36 AGGRESSION AND VIOLENT BEHAVIOUR 9 (2017).

[21] THE CENTRE FOR INTERNET AND SOCIETY, *Country-Wise Legislations on "Revenge Porn" Laws*, , available at https://cis-india.org/internet-governance/files/revenge-porn-laws-across-the-world/view (Last visited February 14, 2022).

[22] The Indian Penal Code, 1860, §354C, Explanation II (talks about the presence of initial consent).

[23] The offence is twofold here – that of rape on one count, and then of the non-consensual dissemination on the second. *See* Bishakha Datta, et. al., *Guavas and Genitals: A research study in Section 67 of the Information*

Non-consensual dissemination of intimate images has both civil and criminal law consequences.[24] It is challenging for victims to identify the person responsible for the publication of the incriminating material, and even if they do identify, they usually lack the means to prove it. Seeking civil action against the perpetrator may bring about heavy litigation costs and may prove to be futile especially considering that the perpetrator may be unable to adequately compensate the victim. While pursuing under criminal laws will unburden from those otherwise heavy civil litigation costs, there are still heavy costs attached to the criminal process that can't be ignored. These costs carry comparably greater social and mental health implications costs, especially considering that majority of victims are oftentimes women and other minorities.

There is a conspicuous dearth of research on non-consensual dissemination of intimate images specifically in India, considering the unsurprising scarcity in the cases registered and subsequently reported.[25] Even though India got its first 'revenge porn' conviction only in 2018,[26] in the form of *Animesh Boxi* v. *State of West Bengal*,[27] there have been several classic revenge porn cases previously noted but not recognised as such.[28]

Public disclosure of private information has an apparent chilling effect on private speech, and oftentimes the absence of public interest further makes questions of privacy much more prominent.[29] However, speech that is expressed online is susceptible to higher scrutiny; the State has a heavier burden to justify any curtailment on the rights to freedom of speech and expression. This essentially means that any legislative action regulating non-consensual dissemination shall have to necessarily pay heed to the perpetrator's freedoms of free speech and expression. In the United States of America, the early years of the 2010 decade saw great discussions regarding the criminalisation of non-consensual dissemination of intimate images, conversing vehement challenges on grounds of a potential criminal legislation being inconsistent with the First Amendment. Arguments generally agree that overbroad and vague legislation would not hold against a First Amendment challenge, and too narrow a

Technology Act, POINT OF VIEW INDIA, 2018, available at https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Smita_Vanniyar.pdf (Last visited on March 15, 2022). Here the activity itself is unlawful, where the consent is being abrogated thrice. There have been multiple cases where rape videos have been booked under §67. This completely transforms the question of consent which is central to rape cases to that of obscenity. Further, it becomes increasingly problematic when questions of consent in rape cases are determined based on the subjective viewing of the video, which is taken out of context and viewed and then non-consensually disseminated. The act of rape and non-consensual dissemination are not mutually exclusive.

[24] As shall be discussed later in the article, the criminal consequences would largely harp on §66E, §67, §67A of the IT Act, and may even include IPC provisions such as §§354A, §354C, §499 and §509 depending on the specific circumstances. The civil consequences, on the other hand, could ensue from breach of copyrights laws, defamation law, and torts law.

[25] One may also refer to the underreporting of rape cases generally, that carry a similar social stigma. *See* Pramit Bhattacharya & Tadit Kundu, *99% cases of sexual assaults go unreported, govt. data shows*, LIVEMINT, April 24, 2018, available at https://www.livemint.com/Object/141EnEHrj3MSsNLtT8BEaK/aboutus.html (Last visited December 22, 2021).

[26] GLOBAL FREEDOM OF EXPRESSION COLUMBIA UNIVERSITY, *State of West Bengal v. Boxi*, available at https://globalfreedomofexpression.columbia.edu/cases/state-of-west-bengal-v-boxi/ (Last visited December 22, 2021).

[27] State of West Bengal v. Animesh Boxi, CRM No. 11806/2017 (The case, as the article later discusses in detail, is a textbook revenge pornography case where the jilted lover had published the sexually explicit pictures of the victim on a pornographic website. The court had found him guilty under various sections of the IT Act, 2000 and IPC, 1860, including §66E, and sentenced him to five-years of imprisonment with a INR 9,000 fine).

[28] Manoj Dattatray Supekar v. State of Maharashtra 2016 SCC OnLine Bom 15449; State (NCT of Delhi) v. Mahesh 2017 SCC OnLine Del 7956.

[29] James T. Dawkins IV, *A Dish Served Cold: The Case for Criminalising Revenge Pornography*, 45(2) CUMBERLAND LAW REVIEW 395, 442 (2015); CITRON & FRANKS, *supra* note 5, at 136.

legislation would be redundant and not efficacious.[30] In the United States of America, scholars that have called for the criminalisation of non-consensual dissemination of intimate images usually agree that obscenity is the one unprotected form of speech that cannot stand the high protection of the First Amendment.[31]

However, the situation in India stands starkly against the one in the United States of America due to a distinct legal reading of the laws regulating freedom of speech and expression. While legal standards as regards obscenity and indecency and morality vary significantly between the two jurisdictions,[32] the argument here borrows from the larger foundational difference between the evolution of the right to free speech and expression in the two jurisdictions. In India, while freedom of speech and expression under Article 19(1) of the Indian Constitution is highly regarded by the courts and any restriction on the same invites greater scrutiny, the right is restricted via several explicitly listed 'reasonable restrictions' under Article 19(2). This practise is quite in line with even international conventions that similarly lists restrictions in cases where the right may be restricted.[33] Meanwhile, the First Amendment under the U.S. Constitution does not explicitly list the restrictions in the text of the Article, the acceptable restrictions have evolved over the course of centuries and judgments. This explicit absence of restrictions, while inviting rich discourse, has led to an idea of an absolute right as a solid foundation, notably distinct from the India's evolution of the right. And while the fight in the United States of America was to find an unprotected sphere that can stand the First Amendment challenges while contemplating criminalisation of non-consensual dissemination of intimate images, India already has ample provisions that punish non-consensual and privacy violative capturing, publication, and transmission of intimate images. There was no fight for criminalisation; cases in India have been known to have been registered under the sections that cover obscenity.

III. §§66E, 67, AND 67A OF IT ACT, 2000 - A MESH OF OVERLAPPING LAWS

In India, there is a combination of laws that can be utilised to address non-consensual dissemination. Notwithstanding the non-acknowledgment of a specific 'non-consensual dissemination of intimate images' provision in the statute books, it is primarily §66E of the Information Technology Act, 2000 ('IT Act') that is ostensibly designed as one. Titled 'punishment for violation of privacy', §66E punishes anyone who intentionally or knowingly captures, publishes, or transmits the image of a private area of any person without his or her consent, violating the privacy of the person, with an imprisonment sentence of up to three years and/or with fine up to two lakh INR. As the explanation to the section elucidates, the term 'capture' with respect to an image, means to videotape, photograph, film, or record by any means. The punishment of publication/transmission of such images extends to the public, as well as to one person, essentially meaning that even if the media is leaked to the employer or any family member, the person leaking shall be held liable.[34] Notably, §66E pays special

[30] *See* Reno v. ACLU 521 US 844 (1997) (the CDA was partly struck down on the ground of being vague and overbroad, going beyond the boundary set by the Miller test of obscenity).

[31] DAWKINS, *supra* note 29, at 445.

[32] *See* Siddharth S. Aatreya, *Obscenity and the Depiction of Women in Pornography: Revisiting the Kamlesh Vaswani Petition*, 13 NALSAR STUD. L. REV. 1 (2019).

[33] International Covenant on Civil and Political Rights, December 16, 1966, U.N. Treaty Series Vol. 999/171, Art.19; European Convention for the Protection of Human Rights and Fundamental Freedoms, November 4, 1950, ETS 5, Art.10.

[34] The definition for 'transmit' is "to electronically send a visual image with the intent that it be viewed by a person or persons".

heed to the 'privacy' violation of the victim, following suit of various other jurisdictions.[35] This recognition is material since it would make it a serious offence and presumably increase judicial scrutiny. However, this recognition of 'privacy' violation must not be categorised as only a privacy violation but also as a sexual offence.

At the outset, it is important to delineate the delicate workings of this provision and how it is different from the other seemingly similar statutes. While this section seems similar to voyeurism (in fact, while framing it was read as 'video voyeurism'),[36] it is not limited to merely 'capturing' of photos but also extends to their 'transmission' and 'publication'.[37] This widens the scope and removes fears of it being too narrow, by including within its scope 'selfies' that are taken by the victim where consent is apparently present when the victim clicked the image and transmitted it further, but consent is absent when the image is published/transmitted by the receiver.[38] In effect, we see that §66E is not merely a 'voyeurism' statute such as §354C of the Indian Penal Code, 1860 ('IPC') that punishes only 'viewing' and/or 'capturing' of images, which has an apparently narrower scope than §66E that punishes 'transmission' and 'publication' as well.

Further, as the explanation to §66E reads, it is applicable only to instances where the individual has a 'reasonable expectation of privacy'. A possible consequence of this is that an individual consensually sending an image of a private area would be allowed to do so and would not be caught under this section. However, it is here that other dragnet sections, particularly §67 and §67A of the IT Act, that come into play and criminalise even the consensual publication/transmission of sexually explicit images.

§67 punishes the transmission or publication of material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely to see, read or hear.[39] This section is the IT Act's version of obscenity, highly controversial due to its broad reading and irregular practical application.[40] On the other hand, §67A punishes the publication or transmission of material that contains any sexually explicit act or conduct. [41] This section largely criminalises instances of pornography.[42]

---

[35] The Penal Code of Spain, 2015, Chapter X, Paragraph 7, Art. 197 (Spain); The French Penal Code, Art. 226-232 (Spain); The Criminal Justice and Crime Act 2015, §33(1) (U.K.); The Cyberbullying Act, §162.1 (Canada); Anti-photo and Video Voyeurism Act of 2009 (Philippines); Crimes Act 1900, §91Q (New South Wales); Delaware Code, Title 11, §1335 (Delaware); Kansas State Act, §21-6101(a)(8) (Kansas).

[36] Ministry of Electronics and Information Technology, *Report of the Expert Committee on Amendments to IT Act 2000: Press Release*, August 29, 2005, available at https://www.meity.gov.in/content/report-expert-committee-amendments-it-act-2000 (Last visited December 22, 2021).

[37] This is similar to the law in Idaho, *see* Crime of Video Voyerism, H.B. 563, 2014 Idaho Sess. Laws Chapter 173 (U.S.A).

[38] *See* DAWKINS, *supra* note 29, at 435-436 (this question is relevant considering the problems with the New York 'revenge pornography law' that where the statute did not protect the unconsented dissemination of legally obtained images).

[39] The Information Technology Act, 2000, §67.

[40] *See* Sonali Verma, *Route 67: How the IT Act's Section on Obscenity is Being Misused to Violate Digital Freedom*, THE WIRE, November 29, 2017, available at, https://thewire.in/gender/victorian-censorship-research-finds-section-67-act-grossly-misused (Last visited December 22, 2021).

[41] The Information Technology Act, 2000, §67.

[42] Since §67A calls for 'sexually explicit' expression, it could be reasonably argued that the term does not cover media where the sexual organs or the genitals are covered. This is where §66E comes into focus and criminalises media that showcases even undergarments in non-consensually disseminated media.

Notably, Animesh Boxi was one of the rare cases where the courts had employed the use of §66E, albeit cursorily. It was a classic revenge porn case where the accused, Animesh Boxi, had demanded personal intimate images from his girlfriend and later acquired them by allegedly hacking into her phone. He subsequently used to pressure her into going for outings by threatening to publish the intimate images on social media. When the girlfriend resisted, he made good on his promise and non-consensually disseminated his girlfriend's intimate images on PornHub.[43] The court found him guilty and was accordingly sentenced to a total of 5 years' worth of imprisonment with a nine thousand INR fine.[44] To fit it into the IPC chapter relating to 'Of Criminal Force and Assault' and attract the application of the aforementioned IPC sections, the court read the harm done to the victim to come under the definition of 'injury', as provided under §44 of the IPC by reading the uploading of the non-consensual media as injuring the victim's mind and reputation. The court made an interesting, if crudely phrased, remark that the victim will be virtually raped every time someone views the content online, and considering that these photos are never really removed from online sources, the rape shall continue till she lives.[45] While sentencing the victim, the court's prime consideration was deterrence and the fact that such crimes against women have great impact on social order and public interest.[46]

The case is significant, firstly because of the inclusion of §66E in its list of charges, marking the court's attempt to acknowledge the privacy and consent violation; and secondly because of the observation that the victim is entitled to get compensation as a rape victim under the victim compensation scheme. This compensation was to be availed from the District Legal Services Authority under §357-A of the Code of Criminal Procedure, 1973,[47] which is one of the primary sections under which rape victims apply or are directed to apply for compensation.[48]

Thus, what we essentially see is a mesh of laws that can be employed to address non-consensual dissemination in the courts, however, they overlap in their scopes which leads to further problems as shall be discussed in the next portion. While all the three provisions – §66E, §67, and §67A, overlap in their scopes, their distinct language and ingredients significantly shapes the lens with which the judiciary views pornography, and by direct extrapolation, non-consensual dissemination. Interestingly, while there is the creation of an 'option' between these three sections, as any of these laws could be utilised to address non-consensual dissemination in courts, this option is rendered useless with their overlapping scope.

Operation of §67 and §67A effectively renders §66E infructuous. §67 (obscenity) and §67A (sexually explicit), read conjunctively or disjunctively, provide for a mechanism with which §66E is made useless. The scenario contemplated by §66E, to a huge extent, can squarely be covered under §67 and §67A due to their vague and otherwise dragnet nature. We see this in cases where despite being a proper 'revenge porn' case, the courts may

[43] State of West Bengal v. Animesh Boxi, CRM No. 11806/2017, at 94-95.

[44] The Indian Penal Code, 1860, §§354-A (sexual harassment and its punishment), §354C (voyeurism), §354D (stalking), §509 (insulting the modesty of a woman); The Information Technology Act, 2000, §§66E, §66C (preservation and retention of information by intermediaries), §67, §67A.

[45] State of West Bengal v. Animesh Boxi, CRM No. 11806/2017, at 127.

[46] *Id*, at 125-127.

[47] *Id*, at 128.

[48] Verma, *supra* note 40 (Interestingly, the Expert Committee's Report had recommended a compensation of up to 25 lakhs to the victim; however, the same was not added to the Information Technology Act, 2000, when it was amended).

still read §67 and §67A to punish, with heavy sentences.[49] The major issue here is that the operation of §67 and §67A subsumes the role of §66E and pointedly evades all privacy and consent violation questions and concerns. This swift evasion stands more starkly when considering the Puttaswamy judgment that formally upheld privacy to be a fundamental right under the Constitution.[50]

Not only is §66E frustrated legally, but also practically, largely due to the booking of non-consensual dissemination cases under §67 and §67A. The majority of the cases referred to in the essay are demonstrative of this practise, where despite of being argued as the victim's privacy violation (sometimes even consent), the focus of the case reverts to discussing/stating obscenity of such photos under §67 and §67A.

Moreover, as stated above, this redundancy of §66E also means that the courts do not need to delve into question of consent as well. The inevitable problem with provisions concerning consent is that they require the determination of that consent, a rather controversial aspect of such cases.[51] In the case of non-consensual dissemination, this determination of consent (as §66E requires) may be problematic when the court considers and determines this consent based on the victim's behaviour, which, as has been observed historically, often leads to victim blaming.[52] For reference, consider the alleged sextortion case of *State (NCT of Delhi)* v. *Mahesh*,[53] where the accused allegedly raped the victim, videotaped the act, threatened and blackmailed the victim for money, and subsequently attempted to sell that video in the village. Here, it is important to note that the Trial Court had apparently deduced the consent of the victim from the video, as is clear from the portion cited by the Delhi High Court's judgment –

> "The instant video was played before me. I found the prosecutrix behaving quite normal during the incident. No inference can be drawn from that video that she was under threat or she was forced to have such relations with the person. It appears to be a consented sex".[54]

The legal issues the court dealt with concerned the applicability of §67A and its ingredients. Since the accused's identity could not be established from the video, it did not satisfy the 'transmitted' ingredient of §67A and so the appeal was dismissed, and the accused was acquitted.

While Animesh Boxi is one of the rare examples where the case was booked under §66E, it must be noted that the punishment given to the convict under §66E was of four months, whereas the cumulative punishment given under §67 and §67A was of three years and four months.[55] This assignment of punishments clearly suggests that obscenity arguments carry

---

[49] For reference, *see* Manoj Dattatray Supekar v. State of Maharashtra 2016 SCC OnLine Bom 15449 (despite being a textbook revenge pornography case, it was booked under §67A instead of §66E. This case concerned a man who had videotaped sexual acts and non-consensually forwarded the clips to the victim's relatives and husband).

[50] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[51] *See* Anupriya Dhonchak, *Standard of Consent in Rape Law in India: Towards an Affirmative Standard*, 34 BERKELY JOURNAL OF GENDER, LAW & JUSTICE 29, 38-41 (2019).

[52] Consider this in the backdrop of the intense victim blaming witnessed in rape cases. *See* Fairbairn, *supra* 13, at 239.

[53] State (NCT of Delhi) v. Mahesh, 2017 SCC OnLine Del 7956.

[54] *Id*, at ¶10.

[55] The Indian Penal Code, 1860, §354-A (two months imprisonment), §354C (two months imprisonment), §354D (four months imprisonment), §509 (four months imprisonment); The Information Technology Act, 2000, §66E (four months imprisonment), §66C (four months imprisonment), §67 (four months imprisonment), §67A (three years imprisonment.

more weight in courts than privacy and consent violations. Partly, the blame can be put on the non-recognition of §66E as a 'revenge porn' section (despite having all the essentials of such laws), which may prompt the courts to consider other laws under which to fit such situations. Privacy and consent of the victim are then mere unfortunate corollaries of such 'obscene' actions. The concern then is not just limited to the wide intersecting scopes of multiple criminal provisions, the harm is much more far-reaching than what meets the eye.

IV. UNDERSTANDING THE OBSCENITY ARGUMENT HERE

Provisions prohibiting the transmission or publication of obscene/indecent material are universal and certainly not new. In absence of specific, tailored legislation for non-consensual dissemination, various jurisdictions take the help of obscene/indecent provisions to tackle this problem.

While revenge porn has been considered as obscenity unprotected, an ancillary concern that arises is whether all photos that are sexually explicit are obscene in nature, considering so especially in the case of consensual sharing. This is especially concerning in India, where watching pornography cannot be claimed as a matter of right to privacy.[56]

In other legislations, the portrayal of certain sexually explicit content evades the obscenity trap and is permitted when the right to freedom of speech and expression is considered.[57] In India, the harms of pornography are inherently presumed in all sexually explicit material; this is clear from §67 of the IT Act.

In *Jaykumar Bhagwanrao* v. *State of Maharshtra*,[58] the Bombay High Court defined the scope of §67A as "sexually explicit activity covered under §67A is necessarily to be lascivious or of prurient interest". A similar observation was made by the Delhi High Court in *X* v. *Union of India*,[59] that "§67A adds further specificity to the generic phrase 'obscene material' and refers to material which contains 'sexually explicit act or conduct' and makes publishing or transmitting of such material a more egregious offence, with enhanced punishment." These judgments essentially construct a twin test that the media disseminated will have to be – first, sexually explicit, and second, lascivious or of prurient interest.[60] Does the law then permit a separate space for sexually explicit material that is not obscene (as understood under §67) in nature? That can be a possible conclusion provided the sexually explicit media is able to escape the trap of obscenity, failing the conjunctive twin test.

One must note that there may be sexually explicit content that may not be obscene. Consider the United States of America's. judgment of *Reno* v. *American Civil Liberties Union*,[61] where the court observed that sexual expression that may be indecent or offensive to some may not inherently be obscene. This observation, building on the *Miller test* created in *Miller* v. *California*, was premised upon the idea that the First Amendment has

[56] *See* Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[57] *See* Siddharth S. Aatreya, *Obscenity and the Depiction of Women in Pornography: Revisiting the Kamlesh Vaswani Petition*, 13 NALSAR STUD. L. REV. 1 (2019) (the author outlines the various selective protections accorded to certain types of pornographic expression in America and Canada, while discussing the blanket implications of the Indian regime regarding pornography).

[58] Jaykumar Bhagwanrao v. State of Maharshtra, 2017 SCC OnLine Bom 7283.

[59] X v. Union of India, 2021 SCC OnLine Del 1788.

[60] *See* Arti Gupta, *The Uttarakhand High Court and Pornography*, INDIAN CONSTITUTIONAL LAW AND PHILOSOPHY, September 19, 2019, available at https://indconlawphil.wordpress.com/2019/09/19/the-uttarakhand-high-court-and-pornography/ (Last visited December 22, 2021).

[61] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997),

within itself a hierarchy of expressions when considering obscenity, and that phrases such as 'indecent' and 'patently offensive' are vague and overbroad.[62] Although similar observations as regards sexually explicit content have been entertained by some domestic courts (despite their considerable conservatism),[63] the same is generally not the case in India where pornography is considered an offence under §67A of the IT Act.

Accordingly, it is still pertinent to remark this uniform approach of the judiciary towards readily treating non-consensual dissemination as obscene. It is clear from the above cases and the recurring frequency at which the judges automatically label all sexually explicit media to be obscene in nature; their conservative approach leaves no space for latent interpretation of any sexually explicit content to not be obscene.[64] What then essentially follows from the plain reading of the law is that even consensually transmitted or published photos have the scope of the being caught in the obscenity trap. Although there is an apparent dearth of jurisprudence on the same, sexting which often involves the sending and receiving of sexually explicit images, is consequently considered a crime in India under the relevant sections discussed, even when done consensually.

Recently, the Delhi High Court dealt with the issue of intermediary liability and obscenity in *X* v. *Union of India*.[65] The case concerned the publication of the victim's images taken from her private social media accounts to a pornographic website called 'Xhamster' by an unknown entity, which were later reposted to other websites and online platforms. Though the case was not booked under §66E since the photos were not sexually explicit *per se*, this judgment is relevant for two major reasons. Firstly, the court categorically declared it to be a privacy violation.[66] Secondly, the court harped on the point of non-consensual dissemination of images, whereby the unique nature of internet enables the instant and endless distribution of such content, requiring immediate and efficient remedy for victims.

The court ruled that in cases where even the concerned image is not obscene in itself, the posting of the same on a pornographic site with the victim's name and/or their likeness, without consent or concurrence, would amount to an offence under §67.[67] This has seemingly expanded the scope of §67 in relation to non-consensual dissemination of images by penalising the publication or transmission of not only obscene material, but also by considering this publication and transmission as an obscene act. In the courts' opinion, the

[62] This position stands starkly against the Indian jurisprudence on obscenity, where though the term 'obscenity' is not mentioned in Art.19(2), it derives its authority from terms 'decency' and 'morality' that are explicit permissible restrictions under Art.19(2).

[63] For instance, in Ranjit Udeshi v. State of Maharashtra (1965) 1 SCR 65, the court had stated that sex and nudity may not ipso facto be considered obscene, it has to be supplied with 'something more'. The judgment is highly criticised for its approach of opting for most repressive obscenity test and its repressive outcome, however, this idea of there being a space for sexually explicit material that is not considered obscene is vaguely introduced by the courts. This idea is further stated more clearly over the course of several decades and judgments, with the adoption of different obscenity tests, and identifying certain specific areas where sexual explicitness shall not be obscene. However, this selective assignment of certain sexually explicit media to not be obscene (consider the Grihalakshmi obscenity case where breastfeeding image was not considered obscene) is problematic since it assumes obscenity and then carves out a space for acceptable media that may not be obscene. Every sexually explicit content is then deemed to be obscene right from its creation.

[64] See Caroline West, *Pornography and Censorship*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY FALL 2008 EDITION, May 5, 2004, available at http://plato.stanford.edu/archives/fall2008/entries/pornography-censorship/. (Last visited March 14, 2022).

[65] X v. Union of India, 2021 SCC OnLine Del 1788.

[66] *Id*, at ¶86.

[67] *Id*, (Justice Anup Bhamhani observed that "the only purpose of posting the petitioner's photograph on a pornographic website could be to use it to appeal to the prurient interests of those who are likely to see it").

victim's images had become 'offensive by association'.[68] Since this expanded reading was done in a set context, it would be difficult to extrapolate this logic to other situations, though certainly not impossible.

In essence, to combat the harms of non-consensual dissemination in cases where the images are not sexually explicit but the dissemination of those images results in similar harms as non-consensual dissemination of sexually explicit images would, the court has here enabled the application of obscenity law in favour of the victim.

V. MITIGATING THE HARM

Whilst it is important to hold a perpetrator accountable for such non-consensual dissemination, curbing the spread of one's intimate images non-consensually before it spreads any further may be a more urgent concern from a victim's perspective. Although technology has enabled this material harm as we have seen above, it has also provided certain technological tools via which this harm may be mitigated. While the harm has already happened and the victim has already suffered, these remedies, provided by technology and enabled by law, may prove to be a sturdy band-aid capable of staunching the blood flow.

A. CLAIMING COPYRIGHT INFRINGEMENT

One of the apparent remedies available for victims of non-consensual dissemination is to claim copyrights violation. However, copyrights law is usually not considered an appropriate redressal recourse majorly because most copyright ownership claims would be swiftly evaded in cases where the image is not taken by the victim.[69] Additionally, there is a problematic implication of labelling such photographs as an 'intellectual property' violation.[70] Copyrights law as a remedy will not apply where the images have been reposted at other sites, where a fresh claim will have to be pursued, with no guarantee of the sites responding since they're aware of the high litigation costs involved which the victims often times cannot afford.[71] Interestingly enough, since copyright infringement claims centre on questions of ownership and consent, such claims indirectly regard the consent of the victim, which, as we have discussed above is not the case when considering the domestic legal regime on non-consensual dissemination. This indirect regard of victim's consent and entitlement to their photos when they are the first owners, ultimately falls short of any positive result since for every upload online, the victim would have to go through the ordeal of challenging it.

However, due to the dynamic nature of internet, when photos that are uploaded online and then downloaded, further forwarded, or reposted on other sites, it becomes extremely difficult to completely remove such content. Third parties then continually aid in its distribution, further exacerbating the harm caused to the individual. It then becomes imperative to explore other remedies that directly target the media being disseminated without the trouble of claiming a copyright infringement.

---

[68] *Id*, at ¶2.

[69] Under §2(c) of the Copyright Act, 1957, photographs are protected as artistic work, and according to §25 the first owners are conferred protection for 60 years from the date of publication.

[70] CITRON AND FRANKS, *supra* note 5, at 114 (as the authors explain, pursuing copyright infringement relegates the suffering of the victim, a woman generally, to a mere property dispute).

[71] *Id*; Notably, in Animesh Boxi, in spite of the victim possessing ownership over the impugned images, she didn't approach the court for copyright infringement, and instead chose the criminal procedure.

B. MAKING THE INTERMEDIARIES LIABLE FOR ONLINE DISSEMINATION

There are several ways by which the transmission and publication of non-consensual intimate images can be curbed which significantly decreases the harm. One of the most effective ways for a victim is to approach the facilitators of such content online, either via the self-regulatory mechanisms set-up by the intermediaries,[72] or under statutory provisions that regulate online content.[73] The heart of enabling such provisions that interference with the intermediaries rights to host online lies primarily with the fundamental right to privacy which extends to information present online.[74] The right to privacy incorporates the individual's right to protect their personal conception of self. Right to control the dissemination of personal information online comes under the cloister of the right to privacy, whereby the individual is free to prevent others from using their image, name and other aspects of their personal life and identity to protect individual autonomy and personal dignity.[75] This includes the right to know for what the data is being used for with the ability to correct it and amend it; and while this right to control is not absolute, any restriction on it will have to be within the permissible limits laid down by the law.[76]

As has been noted, intermediaries such as telecommunications providers, search engines, social media platforms and network hosts have been identified as the central most effective way to curb the proliferation of these images.[77] Such intermediaries would prevent these images from being found on the internet, by not producing it in the search lists and keeping the victim's name and such from the most influential sites with a significant following.

However, intermediaries are largely exempt from liabilities arising from content-based offences. In India, §79 of the IT Act provides immunity to the intermediary from a broad range of potential liabilities. Intermediaries would enjoy the safe harbour under §79 so long as they observe due diligence while discharging their duties.[78] This requirement is not uncommon, like in the U.S., where §230 of the Communications Decency Act, whereby voluntary action on part of intermediaries is encouraged for restricting access to obscene or offensive material.[79] Hence, the primary issues that we need to consider when looking at non-consensual dissemination are, firstly, how to regulate such dissemination online and, secondly, who shall be made liable for that dissemination.

Due to internet exceptionalism, intermediaries receive preferential treatment and wider protection as compared to their offline counterparts, with the law expanding over

---

[72] *See* Ministry of Information and Broadcasting, *Self Regulatory Bodies*, January 4, 2022, available at https://mib.gov.in/self-regulatory-bodies (Last visited February 14, 2022).

[73] *See* THE CENTRE FOR INTERNET AND SOCIETY, *Country-Wise Legislations on "Revenge Porn" Laws*, available at https://cis-india.org/internet-governance/files/revenge-porn-laws-across-the-world/view (Last visited February 14, 2022).

[74] *See* Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[75] *Id*, ¶624-626.

[76] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1,¶620 (Though the court refers to this in the context of a professional fiduciary relationship, it can be generally extrapolated).

[77] *See* Nicolas Suzor et. al., *Non-consensual Porn and the Responsibilities of Online Intermediaries*, 40(3) Melbourne University L. Rev. 1057, 1066 (2017).

[78] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rules 3, 4.

[79] 47 U.S. Code §30 (c)(2)(A) (U.S.A); *See* Andrew Sevanian, *Section 230 of the Communications Decency Act: A "Good Samaritan" Law Without the Requirement of Acting as a "Good Samaritan"*, 21(1) UCLA ENTERTAINMENT LAW REVIEW (2014).

the years to accommodate the 'otherness' of the internet.[80] In cases concerning obscene content, it is required for the intermediaries who fall under §79 to have the 'actual knowledge' (a court order of competent jurisdiction or on being notified by the appropriate government or its agency) of the content that is circulated being obscene.[81] Consequently, the intermediaries are required to take down content only when they have been notified by the government or via court order.[82] Upon receipt of the court order or on being notified by the appropriate government or its agency, the intermediaries are required to block access to such obscene content within thirty-sex hours.[83]

Going after the intermediaries provides the victim with an alternative way to address the harm, especially when they are unable to track down the original uploaders.

1. THE NEW GRIEVANCE REDRESSAL MECHANISM AND ITS PROBLEMS

The 2011 IT Rules are superseded by the controversial Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('2021 IT Rules'), which introduced several significant additions. Rule 3 (applicable to all intermediaries) and Rule 4 (additional duties applicable for significant social media intermediary) of the 2021 IT Rules elaborate the due diligence that is to be observed by the intermediaries, whereby the intermediaries are, *inter alia*, required to inform users about rules and regulations, privacy policy, and terms and conditions for usage of its services.[84] Secondly, they are required to not host, store or publish any unlawful information, which is prohibited under any law for the time being in force, including the ones in relation to decency or morality.[85]

One of the prominent additions via the 2021 IT Rules is that on receipt of a complaint, by any individual or any on his behalf, concerning any content which is *prima facie* in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, the intermediary is required to take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it within twenty-four hours[86] (and within seventy-two hours in case

[80] *See generally* Mark Tushnet, *Internet Exceptionalism: An Overview from General Constitutional Law*, 56 WILLIAM & MARY LAW REVIEW (2015) (Internet spaces exists distinct from real spaces, however, as we have seen have a great hand in modelling tangible reality. Considering the topic of this article, imagine the circulation of pornographic magazines in person vis-à-vis the circulation of the same content online with the click of a button – this virtual presence that offered enables and exacerbates a lot of harms that might not have had similar impact offline. To this extent, though non-consensual dissemination may not be a 'new' offence, but it amplifies the anticipated effect and warrant special regulation keeping in mind the rights of the intermediaries and individuals. Hence, these new technologies are often regarded as separate panes of existence which must be regulated specifically and specially, though the offence committed online may not necessarily be unfamiliar, like identity fraud, cheating, obscenity, etc).

[81] This is as opposed to the 'strict liability' standard under §292 of the IPC that made booksellers liable irrespective of whether they possessed knowledge about the content being obscene. *See* Chinmayi Arun, *Gatekeeper Liability and Article 19(1)(A) of the Constitution of India*, 7 NUJS L. Rev. 73 (2014).

[82] Shreya Singhal v. Union of India, (2015) 5 SCC 1, ¶122.

[83] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rules 3(1)(d), Second Proviso.

[84] *Id*, Rule 3(1)(b) (this includes informing about obscene content policies as well).

[85] *Id*, Rule 3(1)(d).

[86] *Id*, Rule 3(2) (part of the Grievance Redressal Mechanism applicable to all intermediaries, including significant social media intermediaries).

of a court order or government notification).[87] The intermediaries are supposed to implement a mechanism for receipt of such complaints to provide details in relation to such content or communication link.[88] Further, a significant social media intermediary is required to publish a periodic compliance report every month detailing the complaints received and actions taken, including the number of links of information that the intermediary has removed or disabled access to.[89]

While the move to acknowledge non-consensual dissemination of intimate images by the legislator is welcome, there are several areas where the new law falls short of adequately addressing the core problem.

Firstly, the Rules require the assessment of the content being complained of by the intermediary to be strictly 'prima facie'.[90] However, the absence of the privacy and consent violation from the language of the law and the disregard for the consensual posting of images is resounding. Secondly, as was noted by the Centre for Internet and Society IT Rules 2021 Report, this grievance mechanism insofar as it permits 'any person on his behalf' to lodge a complaint is deeply problematic due to its wide scope, especially considering the several online spaces that exist for and cater to marginalised communities.[91] This wide phrasing allows for online abuse by enabling any random person to report these online spaces, leading to only suppression of expression and chilled speech. As is subsequently suggested, intermediaries must only entertain complaints from the concerned individual, or any individual legally authorised on their behalf.[92]

Thirdly, this situation is further muddled by the mandatory involvement of a 'Grievance Officer',[93] or a 'Resident Grievance Officer'.[94] They are appointed by the intermediaries themselves and their duties,[95] *inter alia*, is to essentially be the focal point of contact for receiving grievances and to dispose of the same.[96] While such appointments are welcomed since they provide a regulatory mechanism appointed specially for the resolution of complaints received,[97] the fact that the mechanism envisaged is absolutely self-regulatory, and does not involve an independent oversight at the crucial decision-making stage severely undermines the resolution process and paves way for arbitrariness.[98] The effect is that this regulation mechanism deludes the public by giving them a sense of safety because of its mere presence, but in fact, does little materially towards protecting the interest of the user.

---

[87] *Id*, Rule 3(1)(j).

[88] *Id*, Rule 3(2)(c).

[89] *Id*, Rule 4(1)(d).

[90] Presumably to limit any unfettered powers (adjudicatory powers, prior restraint, censorship powers) being accorded to the intermediaries which may be inconsistent with Article 19 of the Constitution.

[91] Torsha Sarkar, *On the legality and constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, THE CENTRE FOR INTERNET AND SOCIETY 19 (2021).

[92] *Id.*

[93] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(2).

[94] *Id*, Rule 4(1)(c).

[95] *Id*, Rule 2(k).

[96] *Id*, Rule 4(8).

[97] SUZOR, *supra* note 77, at 1086-1089 (Though he talks in the backdrop of a co-regulatory model which calls for an independent co-regulatory body that works with the executive towards adjudicating the value of the material reported, which is slightly different from the mechanism under the IT Rules 2021).

[98] *See* Suzor, *supra* note 77, at 1086-87 (The author explores the potential benefits of adopting a co-regulatory model where the intermediaries make decisions with an independent administrative body, premised on legitimate due process and transparent government practises).

2. RIGHT TO BE FORGOTTEN AND DE-LINKING

The right to be forgotten refers to the ability of individuals to limit, de-link, delete, or correct the disclosure of personal information on the internet which has become unlawful or unwanted.[99] The right to be forgotten requires the courts to carry out a balancing of the rights (consent, privacy) and interests of the individual as against the right to freedom of speech and expression.[100] For instance, the European Court of Justice's ('ECJ') decisions require the intermediaries to balance the right of privacy with freedom of expression while enabling right to be forgotten. Though the ECJ have found the measure to be justified, it has attracted criticism over whether it fits the proportionality test for its direct interference with the freedom of speech and expression, and a burden on private actors to adjudicate on complex legal matters.[101]

Additionally, this balancing often requires public interest considerations and the necessity of the same relies on the extent of the public interest involved.[102] As has been noted, the public interest is weak when considering non-consensually disseminated intimate images serve no real public interest.[103]

The right to be forgotten has been considered to be essentially towards alleviating some pain of the victim by preventing and limiting access to their non-consensually disseminated intimate images online.[104] This is particularly important considering how content is continually distributed and churned online. Preventing access at the outset goes a long way to prevent access to these images.

Presently, in India, there is no statutory recognition of this right,[105] though the Personal Data Protection Bill 2019, which is still in abeyance, specifically provides for it.[106] It must be noted that the right to be forgotten is used interchangeably with the right to erasure in the Indian context, especially considering the lack of statutory recognition.[107] Interestingly,

[99] BN SRI KRISHNA COMMITTEE, *Report of the Committee on Data Protection Framework* (July, 2017), at 75.

[100] *See* Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN L. REV. ONLINE (2012).

[101] SUZOR, *supra* note 77, at 1074-1077.

[102] *See* Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶635-636; BN SRI KRISHNA COMMITTEE, *Report of the Committee on Data Protection Framework* (July, 2017) (The PDP Bill balances these competing rights by stipulating a test inspired by Article 17 of the UK GDPR 'right to erasure').

[103] *See* CITRON & FRANKS, *supra* note 5, at 127.

[104] Aidan Forde, *Implications of the Right to Be Forgotten*, 18 TULANE JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 83, 119 (2015).

[105] *See* Rout v. State of Odisha, BLAPL No. 4592/2020 (a recent revenge pornography case where the woman was allegedly raped by the petitioner, who videotaped and photographed these acts and uploaded the contents to Facebook using a fake informant ID in the name of the woman. It was also alleged that he used to threaten, and blackmail using those photos and videos. The case was booked, *inter alia*, under §67 and §67A of the IT Act, and notedly, not under §66E. The Orissa High Court, while observing that there is no mechanism in the Indian legal system to remove the objectionable content from social media, explicitly mentioned Art.17 of the GDPR which provides for the right of erasure and laid special emphasis on the right to be forgotten. The court relied on various international judgments that speak of de-referencing material from search lists and directed the victim to seek appropriate orders).

[106] The Personal Data Protection Bill, 2019, §20.

[107] BN SRI KRISHNA COMMITTEE, *Report of the Committee on Data Protection Framework* (July, 2017); This right to control the dissemination of personal information online and offline doesn't equate to total erasure of information online but has to be balanced against other fundamental rights such freedom of expression, media and democratic society. This also includes important wider considerations for public interest'. Interestingly, the PDP Bill provides for the 'right of erasure' (clause 18) separately from the 'right to be forgotten' (clause 20). Since the Bill is still not passed, the substantive differences, apart from the procedural differences, would be clearer if and

Indian courts have time and again directed intermediaries to de-link certain information from the search engines, upholding the right to be forgotten in essence.[108] However, since there is no specific legislation that deals with the same, requesting a specific recourse becomes an issue for victims.

For instance, in *X* v. *Union of India*, the court had directed the search engines to make the offending content non-searchable by 'de-indexing' and 'de-referencing' it in their search results.[109] The court observed this to be consistent with an intermediary's obligation under the second proviso to Rule 3(1)(d) of the 2021 IT Rules. Although the court did not explicitly call out the right to be forgotten of the victim, it did essentially uphold it in a case that has all the markers of revenge pornography. The court further observed that since that search engines already possess and employ requisite automated tools to prevent generating links to child pornography, the same could be replicated to prevent link generation of the concerned pornographic site. This, as the court considered, would not impose "upon the website, online platform or search engine(s) any obligation to generally monitor content or to adjudicate the illegitimacy of any content or operate as a prior restraint or a blanket ban or censorship of content generally."[110]

It must be noted that this exercise of de-linking is the outcome of a full-fledged court case and may not necessarily extend to individual complaints sent to the intermediary. While this exercise can be read into the phrase 'take all reasonable and practicable measures to remove or disable access to such content',[111] the intermediary is not required to automatically de-link online search results upon the receipt of complaints. Furthermore, issues involving the dissemination of information online are extremely time-sensitive,[112] in a situation where there is a genuine case, it may become impossible to prevent the circulation online and hence be infructuous to even approach the court.

Besides, if de-linking is the best method possible to restrict rampant access to the concerned content, anything short of that would be blatantly unfair to the victim, a possibility which may probably arise with the use of the broad phrase 'take all reasonable and practicable measures to remove or disable access to such content' as mentioned in the IT Rules 2021.[113] While, understandably so, it is rational to not automatically de-link media on receipt of complaints, the legislature must provide an inclusive, non-exhaustive list of steps that may be taken by the intermediary on receipt of a complaint. It warrants a closer look and potentially, a specific definition from a technological perspective.

This brings us to the general criticism of takedown notices, considering that intermediaries have known to err on the side of caution, and remove, partially and often

---

when it comes in force, *see* Vinod Joseph & Protiti Basu, *Right of Erasure – Under the Personal Data Protection Bill 2019*, MONDAQ, December 23, 2019, available at https://www.mondaq.com/india/data-protection/877732/right-of-erasure--under-the-personal-data-protection-bill-2019 (Last visited on Feb. 14, 2022).

[108] *See* Sri Vasunathan v. The Registrar, General, 2017 SCC Karnataka 422 (this case upheld the right to be forgotten and directed the lady victim's name to be masked in the cause-title of the order passed to prevent her name from showing up on internet searches, damaging her reputation. The court further observed that this practise is in line with the Western trend where the same is followed as a matter of rule in sensitive matters concerning women generally, especially those that involve rape or affecting the modesty and reputation); S*ee also* Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd., 2019 (175) DRJ 660; Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶636.

[109] X v. Union of India, 2021 SCC OnLine Del 1788, ¶91.

[110] X v. Union of India, 2021 SCC OnLine Del 1788, ¶90.

[111] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(2)(b).

[112] *See* Shalini Harpalsingh Dugal v. State of Maharashtra, Criminal Application No. 481 of 2016.

[113] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(2)(b).

arbitrarily, content that is reported to them.[114] And as pointed above, even when the intermediaries are required to 'prima facie' assess the content reported, these intermediaries still are essentially evaluating the content complained of, leading to legitimate concerns of content that is not sexually explicit being removed on mere complaints. The fact that these decisions are usually made in an opaque manner with no transparency only exacerbates the situation.[115] Significant social media intermediaries would have little incentive towards locating and confirming the veracity of the complaint received and would rather veer towards over-blocking legitimate speech to evade any potential legal consequences.[116] This would undermine the fundamental right to freedom of speech and expression of legitimate posts that do not contain any sexually explicit content.

What we see is a fundamental problem associated with the way courts have read and explored available recourses such as de-linking and the right to be forgotten to mitigate the harm. Nonetheless, the resultant lack of uniformity is less an issue of the courts and more an issue of statutory non-recognition and arbitrariness, as we have seen above.

VI. CONCLUSION

This paper has identified the various lacunae present in the extant legal regime regarding non-consensual dissemination of intimate images that sidestep all privacy and consent concerns, essentially resulting in a weak and patriarchal legal framework. Although the remedies available against non-consensual dissemination of intimate images mentioned and discussed in this research paper mitigate the harm, they are not infallible, especially considering the unique and exceptional nature of internet that constantly distributes and churns media. The right to be forgotten emerges as a viable option that victims may pursue to slow down the reach of their intimate images, however, the lack of any statutory recognition results in an arbitrary situation where it may only be opted by the courts.

In India, media and obscenity legislations neatly reinforce the misogyny and patriarchy, where all questions concerning morality precipitate into a legislative answer that shrieks and harms the 'female body'. The production of female bodies has remained the focus of the legislature which has directly modelled the narrative of criminalisation in India, as can be witnessed in the obscenity laws generally and the larger argument this article addresses. Obscenity laws have been routinely employed in India to defend dominant patriarchal moral ideas at the expense of women's human rights when it comes to expressions of women's sexuality, with issues of consent either distorted or completely ignored.

What is perhaps required is a different approach to digital citizenship and cyberactivity that does not distort and taint women's voices.[117] Understanding the harm by factoring in the role of media that actively and passively influences this obscenity narrative,

---

[114] Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet 2011*, CENTRE FOR INTERNET & SOCIETY 29, April 27, 2012, available at https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf (Last visited March 19, 2022).

[115] Notedly, only significant social media intermediaries are required to publish a period compliance report every month mentioning the details of complaints received and action taken thereon, under Rule 4(d) of the 2021 IT Rules, excluding ordinary intermediaries from this compliance. Further, as Rule 4(6) states, the intermediaries are to provide for justification for any of its action taken/not taken to the complainant, however, only to 'to the extent reasonable', which essentially carves space for potential misuse.

[116] *Id*.

[117] Gurumurthy & Menon, *Violence against Women via Cyberspace*, 44(40) ECONOMIC AND POLITICAL WEEKLY, 19-21 (2009).

would then open a pathway to understanding the disproportionality of the harm this practise results in.[118]

[118] *See* Purnima Ojha, *Women's Issues in India: Role and Importance of Media*, 72(1) THE INDIAN JOURNAL OF POLITICAL SCIENCE, 87-102 (2011).