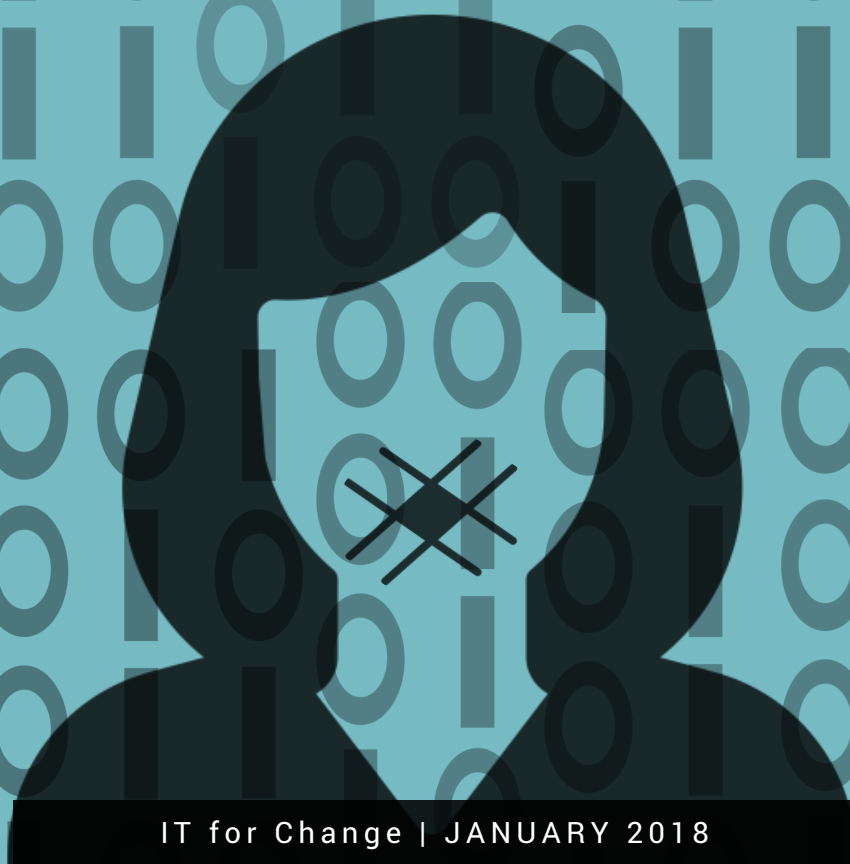
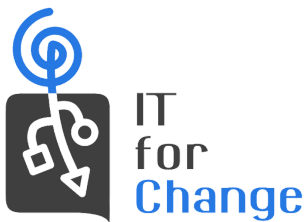


EXAMINING TECHNOLOGY-MEDIATED VIOLENCE AGAINST WOMEN THROUGH A FEMINIST FRAMEWORK

**TOWARDS APPROPRIATE
LEGAL-INSTITUTIONAL RESPONSES IN INDIA**

ANITA GURUMURTHY, AMRITA VASUDEVAN, NANDINI CHAMI





IT for Change is an NGO based in Bengaluru, India. We aim for a society in which digital technologies contribute to human rights, social justice and gender equality.

Authors: Anita Gurumurthy, Amrita Vasudevan and Nandini Chami
Design: Yatti Soni



Copyright: Research outputs from this project are licensed under a Creative Commons License Attribution NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4).

IT for Change | 2018

www.ITforChange.net

Examining Technology-mediated Violence against Women through a Feminist Framework

Towards appropriate legal-institutional responses in India

A discussion paper from IT for Change

Anita Gurumurthy, Amrita Vasudevan and Nandini Chami

January 2018

Table of Contents

Summary.....	2
1. Introduction: Understanding technology-mediated violence against women.....	4
2. Women’s movement and law reform in India.....	6
3. How does the law view technology-mediated violence against women? – Taking stock of existing legal provisions.....	7
3.1 Some gaps in existing provisions and interpretations of the law.....	8
3.1.1. Psychological violence is not accounted for.....	8
3.1.2. Provisions for privacy and confidentiality in the Information Technology Act do not adequately cover acts of ‘doxxing’.....	8
3.1.3. Online verbal harassment and abuse that is sexist, but not involving sexually explicit content, is not adequately addressed.....	9
3.1.4. Violence against women is not framed as violation of a woman’s bodily integrity and personal autonomy.....	9
3.1.5. Absence of a multi layered interpretation of consent.....	10
3.1.6 Dis-empowering interpretation of women’s sexual agency by courts.....	10
4. The legal paradigm of consent and why it is limited.....	11
5. Beyond consent: Developing a feminist framework of gender justice.....	14
6. Towards new laws on technology-mediated violence against women.....	16
6.1 Re-conceptualizing circulation of intimate images.....	16
6.2 Accounting for gender-based hate speech.....	18
6.3 Reformulating ‘outraging the modesty’ of women.....	19
7. Why the digital is different - the need for a new law.....	19
7.1. Intermediary liability.....	21
8. Enhancing the responsiveness of law enforcement agencies.....	25
9. Conclusion.....	26

Summary

The Internet has emancipated women and individuals with non-normative gender identity from their physical bodies, allowing exploration and adventure like never before. Unfortunately, by the paradox of the digital, features that allow speech-expression and facilitate community-solidarity are also used to silence, instill fear and create feelings of insecurity, especially amongst marginalized and vulnerable communities.

On the one hand, the offline-online continuum holds true, and so, it should come as no surprise that sexism, misogyny and violence against women are as much part of the virtual as they are of the real, hounding out women and anyone who is seen as threatening to prevailing gender norms. On the other hand, the techno-materiality of the digital re-orders violence in ways never imagined before, requiring that the digital receive a different treatment. Interactions online are invariably characterized by a disinhibition or lack of restraint, arising *inter alia*, from anonymity, invisibility and asynchronous communication. These subject positions result in a fluidity, fracturing the body from its humanness and normalizing violence against women in new ways.

The paper attempts to posit a feminist theoretical framework adequate to this complexity, as a signpost for progressive legal-institutional responses. It adopts the view that the paradigmatic shifts ushered in by the digital call for a new law in respect of technology-mediated violence against women (TMVAW), rather than piece-meal alterations to the existing law. For the purposes of the paper we have defined TMVAW as “acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of Information and Communication Technologies (ICTs), such as phones, the Internet, social media platforms, and email.” Crimes such as cyber stalking, morphing, doxxing, trolling, non-consensual circulation of intimate images etc. are all forms of TMVAW.

We examine current legal-institutional responses to the phenomenon of TMVAW as well as test if and how existing legislation has been able to hold up against the onslaught of violence. The paper pays heed to the skepticism expressed by home-grown feminist scholarship on law reform as a path to gender empowerment. At the same time, we recognize that dismissing the law or ignoring its role as a mediator of human interaction may be self-defeating. Therefore, while employing the feminist critique of the law and acknowledging the law’s androcentricity and epistemological bias, we turn to the wisdom of feminist jurisprudence to recommend foundational changes in legal approaches to TMVAW.

We map out the fault lines of the two primary laws that apply to TMVAW; the pre-digital Indian Penal Code (IPC) and the commercially oriented Information Technology Act (IT Act). The law, by and large, ignores psychological violence experienced by women, except when it occurs in familial settings. This is a serious lacuna given that victims of technology mediated violence often experience deep psychological trauma. Similarly, provisions in the Protection of Women from Domestic Violence Act, 2005, do not expressly recognize such violence that women in intimate partner relationships often face. Further, sexist speech that is not sexual in nature, and directed at women in general, is not punished. Most penal provisions do not recognize the breach of informational privacy, instead focusing mainly on acts that implicate women’s body. This protectionist approach of the law is also found in anti-obscenity laws whose application and interpretation often undermine and negate women’s sexual agency.

The paper takes cognizance of the improvements in the language of the law, especially in newer amendments to the IPC and IT Act that are centered on ‘consent’, rather than guarding womanly modesty and virtue. However, even here, the failure of the law and law enforcement to appreciate

the multi-layered nature of consent has been problematic. Ascription of essentialist gender roles by the judiciary has led to interpretations of consent that have often rolled back agency rather than promoting it. Recognizing this is important in order to remind ourselves that even seemingly progressive provisions that are centered on consent may not promote agency and autonomy.

The paper suggests looking beyond consent to uncover harm, understood as a violation of the right to privacy, equality and dignity. The right to privacy has been seen as an aggregation of the right to informational privacy, personal autonomy and bodily integrity. To elucidate the proposed framework and draw out its contours, the paper relies on judicial decisions from the country that have affirmed these rights in mutually reinforcing ways. Further, instead of a patriarchal public morality, which inevitably deems any sexual depiction of a woman as 'obscene', we argue the need for a feminist framework of constitutional morality. Using this framework as a litmus test, we suggest alternatives to current anti-obscenity, hate speech, and modesty based laws.

The digital's predisposition to virality necessitates a re-imaging of culpability (intent and knowledge) by invoking legally recognized principles of due diligence found in provisions that criminalize negligence and recklessness. This is vital in order to hold primary and secondary perpetrators liable, especially in cases of circulation of intimate images. Addressing TMVAW also requires tackling the role and responsibilities of Internet intermediaries and the changes needed for effective law enforcement.

To see like a feminist is to de-stabilize ideas, frames, practices and much more. Which is why the good fight against patriarchal legal institutions remains vital. Yet, the law can be an instrument of transformation, especially when the wheels of social change present a moment of flux.

1. Introduction: Understanding technology-mediated violence against women

The purpose of this discussion paper is to lay out the key social, legal and institutional issues concerning technology-mediated violence against women (TMVAW) from a feminist perspective. It draws upon secondary literature in this area, and inputs from Indian feminist scholars and practitioners working in the domains of gender-based violence, women's rights, digital rights and online violence.¹

Digital technologies have expanded informational and communicative capabilities of women and girls.² By making boundaries between the private and public more fluid, they have enabled greater opportunities for women's self expression and public-political engagement. For marginalized castes and communities, whose systems of knowledge creation are precluded from traditional formal spaces - the Internet has become an avenue for knowledge sharing.³ Ironically, the characteristics that make ICTs a strategic instrument for women's empowerment have also led to their persecution, with violence being a popular and effective weapon of choice. The cloak of online invisibility encourages patriarchal attitudes of entitlement over women, hounding out those women who are seen as threatening to prevailing gender norms.⁴ Women who write or speak about caste or religion are inevitably trolled.⁵ Media reports have also revealed politically motivated trolling and use of social media and social networking platforms to spread communally volatile misinformation against vulnerable minority groups.⁶ A *toxic dis-inhibition*⁷ is evident in the online public sphere, lowering thresholds for sexist and misogynistic speech and behavior.

TMVAW may be defined as, "*Acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of Information and Communication Technologies (ICTs), such as phones, the Internet, social media platforms, and email.*"⁸

Some common forms of TMVAW include⁹:

- i. Harassment on web and mobile platforms, whether sexual or not. This may escalate to cyber-bullying and trolling.
- ii. Stalking/monitoring an individual's movements through tracking her online behavior.
- iii. Hacking an individual's email and social media accounts to obtain personal information. Oftentimes, this is linked to 'doxxing' – the online publication of such information without the consent of the concerned individual.
- iv. Impersonation with the express intent of luring an individual to share private information, which can subsequently be used to exploit her or put her in a potentially violent situation.
- v. Creating fake profiles of women with the intent to harass – by discrediting, defaming and damaging their reputations.

1 We are grateful to Japleen Pasricha - FeminismInIndia; Swarna Rajagopalan, Prajnya; Shakun Mohini; Ritambhara Mehta, Nazariya, and Amelia Andrews for telephonic interviews. A meeting was convened on 19th January 2017 by IT for Change and included experts Bishakha Datta, Point of View; Donna Fernandes and Pushpa, Vimochana; Flavia Agnes, Majlis Legal Centre; Geeta Ramaseshan, Senior Lawyer, Madras High Court; and Namita Aavriti, APC's GenderIT.org. We are grateful to the participants for their inputs and contributions. Read the report of the meeting here - <https://itforchange.net/e-vaw/wp-content/uploads/2017/12/Report.pdf>

2 WWW Foundation (2015), Women' Rights Online, Translating Access into Empowerment, http://webfoundation.org/docs/2015/10/womens-rights-online_Report.pdf

3 Patil, M.A (2017), Debrahmanizing the online sphere: on larger questions of caste, gender and patriarchy, <http://www.genderit.org/articles/special-edition-debrahmanizing-online-sphere-larger-questions-caste-gender-and-patriarchy>

4 Datta, B (2016), Belling the trolls: free expression, online abuse and gender, <https://www.opendemocracy.net/bishakha-datta/belling-trolls-free-expression-online-abuse-and-gender>

5 Divya, A (2013), Why are Indian women being attacked on social media?, <http://www.bbc.com/news/world-asia-india-22378366>

6 Sanghvi, V (2016) I am a troll: Inside the secret world of BJP's digital army, http://www.business-standard.com/article/beyond-business/i-am-a-troll-inside-the-secret-world-of-bjp-s-digital-army-116122801182_1.html

7 Software Freedom Law Centre (2016), Online Harassment: A form of Censorship, http://sflc.in/wp-content/uploads/2016/11/OnlineHarassment_SFLCin.pdf

8 Association for Progressive Communication (2015), Technology-related Violence against Women: A Briefing Paper, https://www.apc.org/en/system/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015.pdf

9 Builds on the categories developed by the VAW learning network, cited in UN Women (2015), Cyber-violence against women and girls: A world-wide wake-up call, http://www.unwomen.org/~media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf

- vi. Non-consensual circulation and malicious distribution of private material, including intimate photographs and sexually explicit imagery/text.
- vii. Publishing or transmitting content that targets women based on their gender and is accompanied by misogynistic slurs, death threats, threats of sexual violence, etc.

Official statistics maintained by the National Crime Records Bureau (NCRB) about cybercrimes record very low levels of incidence of TMVAW. The 2016 Crimes in India report records 868 cases under the motive of insulting the modesty of women, and 569 cases under the motive of sexual exploitation. For the first time, the NCRB also listed cases filed under section 67A (dealing with the publication and transmission of sexually explicit content) under crimes against women. 930 cases were filed under this anti-obscenity provision.¹⁰ In 2014-15, according to NCRB, only about 10% of cybercrimes reported for this period pertain to offenses against women/ offenses of a sexual nature.¹¹ Similarly, between 2014-15, the National Commission of Women registered a mere 178 complaints of cybercrimes against women.¹² However, considering that the majority of victims of TMVAW prefer not to seek legal recourse due to prevailing cultures of victim-blaming and shaming, these statistics must be recognized for what they reveal – just the tip of the iceberg. This assessment is corroborated by research. A 2016 survey on *Violence Online in India* conducted by the FeminismInIndia portal on 500 individuals (97% women and 3% trans-genders) found that 58 percent of respondents “had faced some kind of online aggression in the form of trolling, bullying, abuse or harassment”. But 38% of those who faced such violence did not take any action.¹³

Contrary to popular imagination, TMVAW, is not largely ‘stranger violence’. Many a time, these acts are committed by intimate partners or former partners. For example, a 2014 study conducted by the *Association for Progressive Communications* on 500 cases of TMVAW across 7 countries¹⁴ found that the perpetrator was known to the victim in 40% of cases. Also, in many of these cases, women experienced violence as a continuum stretching from offline to online spaces.¹⁵ In India too, this is emerging as a key issue – as revealed by even a quick study of proceedings and judgments of family courts on intimate partner violence.¹⁶

TMVAW has a chilling effect on women’s free expression. The fact that violence in online platforms is an extremely powerful force of social censorship of women’s speech is not to be treated lightly. The pervasiveness of TMVAW and its increasing normalization thus requires transformative social action.

The paper seeks to engage with the current legal framework in India, as well as emerging feminist thought - exploring the adequacy and appropriateness of the law in addressing TMVAW. We examine the feminist critique of law, its default standards, and consequently, the biases and exclusions it generates, analyzing judicial decisions (which have, at various points, affirmed and denied women’s rights) in light of the changing circumstances brought on by the digital.

The paper is divided into seven parts. Part one observes the back and forth of feminist debate regarding legal reform as route to women’s empowerment. Part two explains the current legal provisions as they would apply to TMVAW and also points to their fundamental failings. Part three

10 National Crime Record Bureau, Crimes in India 2016, <http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf>

11 From 2015 NCRB stats: 5.2 % (606 cases) of all cybercrimes reported this year deal with insult to the modesty of women and 5.1 % (588 cases) of all cybercrimes reported deal with sexual exploitation. See <http://ncrb.nic.in/StatPublications/CII/CII2015/chapters/Chapter%2018-15.11.16.pdf>

12 National Commission for Women (2015), Annual Report 2014-15, http://ncw.nic.in/pdfReports/Annual_Report_2014-15_English_Full.pdf

13 Pasricha, Japleen (2016), ‘Violence’ online in India: Cybercrimes against women and minorities on social media, http://feminismindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf

14 Pakistan, Philippines, Bosnia and Herzegovina, Mexico, Colombia, Kenya, and Democratic Republic of Congo

15 Plou, D.S (2014) Mapping as a strategy to disclose online violence against women, <http://www.genderit.org/node/4214>

16 IT For Change (2017), Report of the meeting on technology-mediated violence against women in India, <https://itforchange.net/e-vaw/wp-content/uploads/2017/12/Report.pdf>

interrogates the use and interpretation of 'consent' in law, drawing from legal definitions and interpretation of 'consent' from rape law and theorization of alternatives to 'consent' emanating from the area of data protection. Part four articulates an alternate legal framework to TMVAW that respects certain inherent rights of women, which are privacy (understood as informational privacy, personal autonomy and bodily integrity), substantive equality, and dignity, supported by constitutional morality. Part five operationalizes this framework against the gaps in the law with respect to hate speech, anti-obscenity and 'outraging the modesty'. Part six explains why digital demands a fresh epistemological approach through discussions on techno-materiality and how it shapes human behavior, and on Internet intermediaries and their liability for TMVAW. , Part seven undertakes a brief analysis of the responses by law enforcement agencies to TMVAW

2. Women's movement and law reform in India

The role of legal reform for women's empowerment has been a polarizing theme in the feminist movements, with broadly, two schools of thought – the 'empowerment' school and the 'rights' school. The former has placed more emphasis on self-driven empowerment of women while the latter on petitioning the state for legislative reform.¹⁷ Scholars of the former view believe that the law and consequently the language of rights is a patriarchal construct that cannot accommodate a feminist framework; that social transformation as legal reform reduces the many identities and experiences of women to a singular fixed and universal prototype. They contend that since state focused reform is inherently patriarchal, it will inadvertently impinge upon women's agency, especially with regard to their sexuality.¹⁸ Kapur and Cossman attest to this fact, drawing out the thread of the self-sacrificing wife who is economically dependent that runs through the Indian legal framework.¹⁹ However they also argue that legal reform can be sites of subversion where feminist norm-making can be taken up.²⁰ Other scholars argue that the law reform skeptics have little to offer in terms of next steps for the women's movement and ignore the fact that women of varying degrees of marginalization do seek out the law for redress. They reject the conception of justice and rights as static concepts.²¹

This paper posits a mix of the two positions. We do subscribe to the critique of the empowerment position, acknowledging that law as a social institution is entrenched in patriarchal norms and that resistance to violence and modes of justice that women seek are contingent, depending on the available choices and individual trade-offs that women make. However, we also recognize that the material-discursive structures of the online impinge upon and define gender identities in particular ways. Even though technologically mediated space is contiguous with offline space, its ontological and relational axes are vastly different. Identity online is not merely a function of individual agency. It is co-constructed by particular interventions - patriarchal, statist and market based – of actors dominating the Internet. We are bound by the architectures of the Internet much the same way as we are constrained by the offline world and its norms and rules. A productive engagement for transformative change that promotes agency, equality and dignity of women must grapple afresh with social theories adequate to the time-space wrought by the Internet. This would imply taking cognizance of the limits of the criminal legal system *and* engagement with institutions of the law. An important opportunity in this moment of flux is in the possibility to articulate the principles of feminist jurisprudence adequate to current conjuncture and challenge anachronistic and patriarchal laws that define and deny women's agency. As Menon observes, "The option of

17 Calman,L (1992), Towards Empowerment: Women and Movement Politics in India, Boulder. Cited in Mazumdar,V, 2000, Political Ideology of the women's movement's engagement with law, <http://www.cwds.ac.in/wp-content/uploads/2016/09/PoliticalIdeology.pdf>

18 Menon,N (1998), Rights, Law and Feminist Politics: Rethinking our Practice. In the name of justice: women and law in society

19<http://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1571&context=ohlj>

20 S.P. Sathe (1996), Law and Women, <http://www.epw.in/journal/1996/41-42/reviews-uncategorised/law-and-women.html>

21 Mazumdar,V (2000), Political Ideology of the women's movement's engagement with law, <http://www.cwds.ac.in/wp-content/uploads/2016/09/PoliticalIdeology.pdf>

abdication of the law is not a viable one, for the law will not abdicate us – the only permissible identities in modern democracies are those put in place by the law. We are inextricably implicated in state and legal procedures.”²²

3. How does the law view technology-mediated violence against women? – Taking stock of existing legal provisions

The primary Acts that deal with TMVAW in India are the IT Act, 2000 and IT (Amendment) Act, 2008 (hereinafter collectively referred to as the ‘IT Act’); and the Indian Penal Code and Criminal Laws (Amendment) Act, 2013 (hereinafter collectively referred to as ‘IPC’).

The key legal provisions from these legislations that may be invoked to charge perpetrators of TMVAW are detailed in **Table 1** below. This is followed by a critical evaluation of these provisions that highlights the gaps/ lacunae in the law.

Table 1. Key legal provisions that can be invoked to address online VAW

Act	Clause	Details of the offense this provision addresses	What forms of online VAW can this provision help in challenging?
IT Act ²³	Section 66E	The capture and electronic transmission of images of private parts of a person, without his/her consent.	- Voyeurism: videotaping women in changing rooms or in public without their knowledge. However, it is limited to when the capture is of ‘private parts’, viz. ‘naked or undergarment clad genitals, pubic area, buttocks or female breasts’.
	Section 67	The publishing or transmission of obscene material in electronic form.	- Graphic sexual abuse on social media and blog platforms, including trolling. - Sending emails/social media messages with sexually explicit content and images to an individual, against his/her will. - Circulation of videos of rape - Morphing pictures/ videos and uploading them online.
	Section 67A	The publishing or transmission of sexually explicit content in electronic form.	- This section is used interchangeably with section 67 ²⁴
	Section 67B	The electronic publishing or transmission of material in electronic form that depicts children in obscene or indecent or sexually explicit manner.	- Circulation of child pornography
IPC	Section 354 A	Sexual harassment, including by showing pornography against the will of a woman.	- Sending video and pictures with sexually explicit content and images to a woman, against her will. - Making sexually coloured remarks over mail, text etc. to a woman. This can include trolling that is sexual in nature
	Section 354 C	Voyeurism, including watching or capturing the image of a woman engaging in a private	- Non-consensual production, circulation and malicious distribution of sexually explicit

²² Krishnan, S (2015), Nivedita Menon: on feminism and feminist conundrums, <http://www.tarshi.net/inplainspeak/interview-nivedita-menon/>

²³ The IT Act is a gender neutral legislation

²⁴ Point of View (2017), Guavas and genitals: A research study, https://www.apc.org/sites/default/files/Erotics_1_FIND.pdf

Act	Clause	Details of the offense this provision addresses	What forms of online VAW can this provision help in challenging?
		act in circumstances where she would have a reasonable expectation of not being observed; and dissemination of images of a woman engaging in a private act under circumstances where she has agreed to the capture of the images but not to their dissemination.	photographic and video material about a woman.
	Section 354D	Following a woman, contacting/ attempting to contact her to foster personal interaction repeatedly despite a clear indication of disinterest by such woman, or monitoring the use by a woman of the Internet, email, or any other form of electronic communication.	- Cyber-stalking of women by monitoring use of mobile/e-mail/ social media, including repeatedly trying to contact her through electronic communication. Only women are recognized as potential victims by the law.
	Section 499	Criminal defamation that leads to reputational harm.	- Though this is a gender neutral provision, it could be invoked by women bloggers and women on social media fighting slander and libel.
	Section 507	Criminal intimidation by anonymous communication.	- Though this is a gender neutral provision, it could be invoked by women fighting trolls issuing threats, whose identities are often anonymous.
	Section 509	Word, gesture, act or exhibition of an object intended to insult the modesty of a woman.	- Though this provision does not explicitly address online sexual harassment and abuse, it could be invoked in such cases.

3.1 Some gaps in existing provisions and interpretations of the law

3.1.1. Psychological violence is not accounted for

TMVAW has a number of detrimental impacts on women's well-being. It causes severe emotional and psychological distress.²⁵ Psychological violence resulting from violation of informational privacy - such as unauthorized access to, and circulation of, personal information that is not sexually explicit in nature - is not acknowledged.

There is no recognition in the law of gender based psychological violence against women outside the familial setting.²⁶ Further, laws that focus on psychological violence within the home and in intimate partner relations, such as the Protection of Women from Domestic Violence Act, 2005, lack provisions that explicitly deal with technologically-mediated forms of such violence.

3.1.2. Provisions for privacy and confidentiality in the Information Technology Act do not adequately cover acts of 'doxing'

The act of doxing involves hunting down personally identifiable information (name, address, mobile number, place of work etc), usually from public databases and subsequently posting that information on public forums with invitation usually to harass the person virtually or even

²⁵ Association for Progressive Communications (2015), End violence: Women's rights and safety online From impunity to justice: Domestic legal remedies for cases of technology-related violence against women, https://www.genderit.org/sites/default/upload/flow_domestic_legal_remedies.pdf#page=20

²⁶ Malhotra, N. (2014), Good questions on Technology-mediated Violence, http://www.genderit.org/sites/default/upload/end_violence_malhotra_dig.pdf

physically.²⁷ Women who are doxxed are usually bombarded with rape and death threats.²⁸ The act is a breach of privacy of the individual. Note that even though identity information/knowledge may be in public records, the context in which it is used can be violative.²⁹

While the harassment faced after being doxxed may well be covered by Sections of the IPC, such as Section 507 (anonymous criminal intimidation), the preceding breach of privacy to discredit, target or de-anonymize an individual has not been dealt with in the IPC or the IT Act. Section 72 of the IT Act which deals with 'breach of confidentiality and privacy' only holds those who misuse powers drawn from the Act or its rules that results in a breach' culpable. Section 66A that dealt with 'sending offensive messages through communication service' could have punished doxxing but was struck down by the Supreme Court in the *Shreya Singhal* case for its wide ambit and vague wording.³⁰ Though the IT Act does have a provision which criminalizes hacking (Section 66), it does not explicitly mention hacking for the purpose of doxxing. Sections 67 and 67A dealing with obscenity are also not suitable to such a crime. This has been detailed in part 6 of the paper. Further, a breach of privacy and confidentiality (Section 72) and data theft (Section 43 read with Section 66) in the IT Act is seen as an economic offense, and not in social or gendered terms.

3.1.3. Online verbal harassment and abuse that is sexist, but not involving sexually explicit content, is not adequately addressed

Sections 499 and Section 507 of the IPC pertaining to criminal defamation and anonymous criminal intimidation cover only those acts of trolling that contain personal threats, and fail to address generalized, misogynistic abuse. The Penal Code's hate speech provision - Section 153A, in its current form, does not cover hate speech based on gender identity and sexual orientation.³¹

The Sections of the IPC construct (online and offline) verbal harassment, abuse and trolling against women as "*isolated and individualised crimes*".³² They fail to recognize that such acts of violence are systemic in nature, and are "*directed at a woman because she is a woman and affect women disproportionately*".³³ In specific, they fail to adequately address acts of verbal abuse targeting women's social identity and location.

Section 6 of the paper will elaborate on how hate speech law in the country ignores sex, gender identity and sexual orientation as markers of identity of collective discrimination and harm to persons belonging to those groups.

3.1.4. Violence against women is not framed as violation of a woman's bodily integrity and personal autonomy

Under the IT Act and IPC, except for a few exceptions, viz., Section 66E of the IT Act and Sections 354C of the IPC, the framing of violence ignores a breach of women's bodily integrity

27 Software Freedom Law Centre (2016), Online Harassment: A form of Censorship, http://sflc.in/wp-content/uploads/2016/11/OnlineHarassment_SFLCin.pdf

28 Jens,K.(2015) Looking for evidence of gender inequality in sexual harassment on Twitter, <https://www.genderit.org/resources/looking-evidence-gender-inequality-sexual-harassment-twitter>

29 Douglas,D.M (2016) Doxing: a conceptual analysis, <https://link.springer.com/content/pdf/10.1007/s10676-016-9406-0.pdf>

30 Shreya Singhal v. Union of India AIR 2015 SC 1523

31 Padte, R.K. (2013), Keeping Women Sade, <https://internetdemocracy.in/wp-content/uploads/2013/04/Internet-Democracy-Project-Gender-Online-Harassment-and-Indian-Law.pdf>

32 Padte, R.K. (2013), Keeping Women Sade, <https://internetdemocracy.in/wp-content/uploads/2013/04/Internet-Democracy-Project-Gender-Online-Harassment-and-Indian-Law.pdf>

33 In line with General Recommendation 19 of the CEDAW that traces the roots of violence against women to structures of gender discrimination; and its acknowledgement of mental suffering as a form of violence.

and personal autonomy. Even these exceptions have only a narrow focus, in that they allude to privacy of 'private areas' of the body, ignoring acts where the face of the victim may be morphed with the body in sexually explicit ways and circulated online.³⁴ Further the Sections are limited to physical privacy, thereby excluding violations occurring through a breach of informational privacy.³⁵ For instance, acts of doxxing that put out a woman's address with an explicit mention that she is 'soliciting', cannot be booked under these Sections.

Also, while Section 509 of the IPC mentions the word 'privacy', it equates intrusion of privacy with the violation of womanly modesty. Invariably, the interpretation of modesty by the courts tends to veer towards patriarchal protectionism.³⁶

3.1.5. Absence of a multi layered interpretation of consent

Feminists have highlighted that 'consent' must be interpreted as a multi-layered act, whereby a woman can withdraw at any point, consent that was previously given. Section 66E of the IT Act and 354C of the IPC, which deals with acts of voyeurism are framed in terms of non-consent. Section 354C also accounts for cases where a woman allows her image to be captured, but does not consent to its circulation/ dissemination. Section 66E however, does not make this leap, failing to recognize women's active sexual agency (such as in sharing intimate images) and accounting for how consent may pan out between acquaintances. Neither of the Sections talks about cases where the woman voluntarily shared the image but did not consent to it being viewed by a third party.

3.1.6 Dis-empowering interpretation of women's sexual agency by courts

Often used to book non-consensual circulation of intimate images, anti-obscenity law in the country, such as Section 292 of the IPC and Sections 67 and 67A of the IT Act, imagine sex to be an immoral act of corrupting influence that society is to be cleansed of.³⁷ The male gaze and the policing of the female body is encoded in the law. A classic example of this is the Indecent Representation of Women's (Prohibition) Act. The Act defines 'indecent representation' as

Publication or distribution in any manner, of any material depicting a woman as a sexual object or which is lascivious or appeals to the prurient interests; or depiction, publication or distribution in any manner, of the figure of a woman, her form or body or any part thereof in such a way as to have the effect of being indecent.

The accompanying judicial history of suppressing sexual expression is source of apprehension, especially in an era where women have looked to the Internet as a source of sexual liberation. Consequently, the need to address sexual violence is conflated with the need to regulate the enactment and representation of sexuality. This ends up reinforcing prevailing gender norms and controls over women's sexuality rather than protecting women's bodily integrity and/ or their informational or decisional privacy.

34 Cybercrimes involving morphed photos rising (2015), <https://timesofindia.indiatimes.com/city/jaipur/Cyber-crimes-involving-morphed-photos-rising/articleshow/47861480.cms>

35 Privacy has broadly been seen in scholarship as comprising physical, informational and decisional dimensions. Information privacy, or data privacy (or data protection), concerns personally identifiable information or other sensitive information and how it is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. In relation to technology, it pertains to the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.

36 Baxi, P, Sexual harassment, http://www.undp.org/content/dam/india/docs/sexual_harassment.pdf

37 Point of View (2017), Guavas and genitals: A research study, https://www.apc.org/sites/default/files/Erotics_1_FIND.pdf

A hyper focus on women's sexuality is also seen in Sections that seek to protect women from her modesty from being outraged (Section 354 and 509 of the IPC). In *Ramkripal S/O Shyamlal Charmakar*³⁸, the bench noted,

The essence of a woman's modesty is her sex. The reaction of the woman is very relevant, but its absence is not always decisive. Modesty in this Section is an attribute associated with female human beings as a class. It is a virtue which attaches to a female owing to her sex.

Furthermore, it is only when a sexual advance is spurned can modesty be outraged. Whether this would cover cases where the women initiated or did not protest sexual advances at first but later objected to them is unclear

The following section explores how the courts in India have interpreted consent, offering theoretical underpinnings of consent in the law and a feminist critique of the same.

4. The legal paradigm of consent and why it is limited

Consent based criminal provisions like Section 66E of the IT Act are a progressive step from blatantly patriarchal provisions that refer to modesty. However, women's experiences in courts reflects the tyranny of patriarchal morality. Unable to acknowledge women's sexual agency, courts often perpetuate essentialist interpretations of 'victimhood'. Even seemingly progressive judgments are underwritten by protectionism and an androcentric analysis. In the *State of Punjab v. Gurmeet Singh*³⁹, the court backed the dismissal for the need of corroborative evidence in cases of rape, arguing "the inherent bashfulness of the females(sic)". Judges may also deconstruct consent in their investigations, but they often slot victims into 'good' and 'bad' women. Only 'good' women are seen as 'genuine' victims. Thus, violence against women is addressed without acknowledging and engaging with gender-based power imbalances in society.

Interpretations of rape provisions (which follow a consent framework) help us understand the fundamental quarrel courts have with consent. Referring to the sexual history of the victim is a standard method used to counter the prosecution's assertion of lack of consent. The provision of the evidence law that allowed for such character assessment was struck down in 2003. Nevertheless, medical tests to determine 'habituation to sex' continue to be conducted on the victim.⁴⁰ In *Mahmood Farooqui v. State (Govt of NCT of Delhi)*⁴¹, the Delhi High Court proceeded to demonstrate that the victim's prior relationship and proximity to the accused 'may have given an impression to the appellant of 'consent' and that 'an expression of disinclination alone, that also a feeble one, may not be sufficient to constitute rape.'

Employing the trope of 'modern woman' the court goes on to observe:

If one of the parties to the act is a conservative person and is not exposed to the various ways and systems of the world, mere reluctance would also amount to negation of any consent. But same would not be the situation when parties are known to each other, are persons of letters and are intellectually/academically proficient, and if, in the past, there have been physical contacts. In such cases, it

38 *Ramkripal S/O Shyamlal Charmakar v. State Of Madhya Pradesh Appeal (cri.) 370 of 2007*

39 *State of Punjab v. Gurmeet Singh* (1996) 2 SCC 384

40 Mitra, D (2014), Testing Chastity, Evidencing Rape-Impact of Medical Jurisprudence on Rape Adjudication in India, <http://www.epw.in/journal/2014/41/special-articles/testing-chastity-evidencing-rape.html>

41 *Mahmood Farooqui v. State (Govt of NCT of Delhi)* CRL.A. 944/2016

would be really difficult to decipher whether little or no resistance and a feeble “no”, was actually a denial of consent.

On appeal before the Supreme court, the bench upheld the High Court's rationale that - not only should there be a lack of consent, but the accused must be aware of such a lacking.⁴² This implicit demand for signs of resistance by the victim (to make the aggressor 'aware' of her lack of consent), especially where parties are known to each other and consent is complicated, makes it an uphill task for the victim to prove rape.

In *Vikas Garg, Karan Chhabra and Hardik Sikri v. State of Haryana*, the Punjab and Haryana High Court, referring to the complainant's 'promiscuous attitude' and irrelevant details like her alleged substance abuse, dismissed the conviction. The three were accused of blackmailing and raping a female classmate, and threatening to release her intimate images. The absence of "gut wrenching violence", the court concluded, meant that the sexual relationship with the complainant had been consensual. Blaming the victim directly, the court also lamented "the degenerative mindset of the youth".⁴³

The consideration of a prior relationship between the parties as a contaminant of consent is a serious cause of concern especially with regard to non-consensual circulation of intimate images, where the victim and the accused may have at some point shared a cordial relationship. Given that physical force may be missing altogether in such cases, the question is ultimately about whether or not there was consent. The woman may have volunteered the image at the first instance but not consented to its publication or circulation. The multiple 'consents' involved here may go unheeded by the accused, and unfortunately, the legal machinery as well. Citron and Franks note that permission once given is wrongly utilized in wide-ranging contexts even if that was not the intent when permission was given. Consent is thus not seen as purpose and use specific,⁴⁴ and the fact that privacy is contextually implicated each time in a series of interrelated events is either not understood or disregarded.⁴⁵

The determination of consent and non-consent in the judicial process needs some unpacking. Turning to the 'no means no' framework, which women's rights advocates find appealing, firstly, the absence of a 'no' requires to be interrogated. For instance, women who encounter of sexual violence are often paralyzed with fear to resist physically or verbally and hence be unable to say 'no'. Further, Schulhofer explains the difficulty in cases of rape where the initial 'no', may be followed by an eventual 'yes'. In these cases, courts inevitably look for the use of force. Schulhofer notes that the content of "meaningful choice" must be constructed from conceptions of human dignity.⁴⁶ Therefore a 'yes' in such instances may not be a real 'yes'.

Law is premised upon the homo economicus, or economic man, depicting human beings as consistently rational and narrowly self-interested agents who usually pursue their subjectively-defined ends optimally. All actions are judged against this masculine ideal of the rational, knowing subject. Rational choice theory may hold for commodity transactions where motivations are straightforward,⁴⁷ but where social and gender power needs to be accounted for, such as in sexual relationships, the theory becomes inappropriate. The co-option and reduction of agency "to the

42 Jain, M (2018), SC rejects victim's plea against acquittal of 'Peepli Live' director Mahmood Farooqui in rape case, <http://www.livelaw.in/sc-rejects-victims-plea-acquittal-peepli-live-director-mahmood-farooqui-rape-case/http://www.livelaw.in/sc-rejects-victims-plea-acquittal-peepli-live-director-mahmood-farooqui-rape-case/>

43 Vikas Garg, Karan Chhabra and Hardik Sikri v. State of Haryana Cr.M.No.23962 of 2017, <https://drive.google.com/file/d/0B1HsQbGINpEfUWtEZE50YWFYd1U/view>

44 As is seen in data protection laws

45 Citron, D.K and Franks M.A (2014) Criminalizing revenge porn, https://law.yale.edu/system/files/area/center/isp/documents/danielle_citron_-_criminalizing_revenge_porn_-_fesc.pdf

46 Schulhofer, S.J(1992), Taking sexual autonomy seriously: Rape law and beyond, https://www.law.upenn.edu/cf/faculty/phrobins/conversations/status/viewFile.cfm?file=schulhofer_11_Law_and_Philosophy_35_461_1.pdf.

47 Little, D (2009), Social agency and rational choice, <https://understandingsociety.blogspot.in/2009/01/social-agency-and-rational-choice.html>

exercise of individual preference...permits little scope for any talk about power, inequities or indeed any structural constraints at all"⁴⁸ means that consent even when seemingly progressive must be continuously unpacked and problematized.

Feminist critiques of the epistemological foundations of law point to the need to interrogate the rational, masculine ideal of a self-sufficient atomized being.⁴⁹ The assumption of innate 'capacity to reason' as a precondition to be recognized as the subject of law fails lived realities of women and their dispensation of consent. The feminist conception of autonomy questions rational theory's assumption of such innateness. Autonomy is engineered by circumstances, is relational, and hence varied and situated. It is not 'all or nothing', but is exercised in degrees.⁵⁰ Socio-economic circumstances constantly ask women to make trade-offs that may not be 'rational'. In a study on dying declaration of women at the hands of dowry violence, it was observed that statements were influenced by various fears of the woman - about the future of her children and her own future if she survived, and the presence of in-laws during the recording of her statement. As a consequence, researchers concluded that although law seems progressive in giving due weight to such declarations, police must conduct further investigations to test the extent to which the woman exercises free agency.⁵¹

In certain kinds of violence, especially custodial sexual violence, there is merit to the presumption of 'no consent'. The feminist movement that mobilized post the *Mathura* judgment rallied for the shift in the burden of proof to the accused in such cases in light of the vulnerability of a woman in custody - (be it a police station, hospital, remand home etc.) and in relation to a man in a position of authority.⁵² However, sex-positive feminists remind us that this baseline of non-consent presumed in cases of rape tends to vest in institutions of the law the power to negate women's sexual agency. Others have argued for the preservation of a normative vision about women's sexual agency, with clear rules that demarcate the line between permissible and impermissible sexual conduct. This would account for the structural context in which autonomy was exercised to trade off sexual agency.⁵³ While the contradiction about agency is at the heart of the feminist question, the quest for feminism is to seek an agency for women that despite structural inequality, subordination and injustice, can be empowering.⁵⁴

Contentions over the sacrosanctity of agency is complicated by the online. The 'free agent' is a familiar trope in techno-libertarian narratives of the Internet⁵⁵, a myth that we must unpack in the face of the dominant, corporate driven model of connectivity. The consent framework may be meaningful in the case of non-consensual circulation of intimate images and can be implemented against the first perpetrator with whom the victim shares an intimate relationship and who we may presume is privy to her intentions (consent or non-consent to circulate etc) vis-a-vis the image. But once uploaded, images on the Internet spread like wildfire, completely unencumbered by non-consent. Stone explains how when images are put up online they can spread from one website to another by scrapping tools.⁵⁶ Social media's propensity for virality further complicates the situation.⁵⁷ In the area of data protection, where consent occupies the status of a fundamental principle, its redundancy in the digital ecosystem has forced a rethink of 'informed consent' in

48 Cornwall, A., Gideon, J. and Wilson, K (2008), Introduction: Reclaiming Feminism: Gender and Neoliberalism, <https://www.ids.ac.uk/files/dmfile/bull39.6intro3.pdf>

49 Završnik, A (2008), The Feminist Critique of Law and the Criminal Justice System, http://www.pf.uni-lj.si/media/s.završnik2008_eng.pdf

50 Feminist perspectives on the self (2015), <https://plato.stanford.edu/entries/feminism-self/>

51 Belur, J et al, (2014) The social construction of 'dowry deaths', http://ac.els-cdn.com/S0277953614004730/1-s2.0-S0277953614004730-main.pdf?_tid=e2204e08-9e24-11e7-a2d0-00000aacb35f&acdnat=1505926871_669a8184195620582cf6ccdd33d77e85

52 Murthy, L., The Bigger Picture: Revisiting Gender Neutrality in Laws Relating to Sexual Assault - Laxmi Murthy <http://www.tarshi.net/index.asp?pid=184>

53 Oberman, M & Baker, K.K. (2016). Women's Sexual Agency and the Law of Rape in the 21st Century, <http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1922&context=facpubs>

54 Lucas, S.D. (2016) The Primacy of Narrative Agency: A Feminist Theory of the Self, https://ses.library.usyd.edu.au/bitstream/2123/15896/2/2016_Sarah_Lucas_Thesis.pdf

55 Referred to as the 'Californian' ideology

56 Stone, Z (2016), Dark net: How revenge porn goes viral, <http://www.vocativ.com/news/271401/revenge-porn-viral/index.html>

technology mediated environments. The techniques of Big Data, and Internet of Things put data into the hands of multiple actors who put data to use in multiple ways, both actions to which the data subject may never have agreed and for which consent may be difficult to take.⁵⁸ A more appropriate framework for this dilemma as Acharya recommends, is a harm framework which places focus on the individual-data subject who may seek redress against harm caused despite giving consent.⁵⁹

The question then is - what principles (rules and limits) should steer the court's analysis, if it is to look beyond consent whilst still recognizing women's agency. The section below articulates a legal framework that builds on the jurisprudence of constitutional morality and the right to privacy, equality and dignity that could guide judicial assessment of harm in cases of TMVAW.

5. Beyond consent: Developing a feminist framework of gender justice

Limiting the law's conception of violence to breach of / adherence to an unequivocal choice ('Yes!' and 'No!') betrays hard fought feminist battles that have forced the law to conduct a microscopic examination of consent/ non-consent as inevitably situated and based on the circumstance that prompt its expression. In a world fundamentally altered by the digital, a framework of choice at face-value would reinforce the *homo economics* as normative standard. Going back to data protection law, scholars suggest a paradigm that adopts a rights-based approach. This grants a data subject an inherent right in the data produced that cannot be divested by consent. The burden of assessing and identifying risks to the individual's right to freedom from harm (due diligence) should then be with data controllers (who collect and use individual-personal data).⁶⁰

Keeping choice at the center, we wish to draw inspiration from legal approaches to data protection, foregrounding harm. Harm, we underline, must be determined on the basis of the rights to privacy, equality and dignity. Further, instead of a patriarchal public morality, which inevitably deems any sexual depiction of a woman 'obscene', thereby disciplining sexual expression, we argue for a feminist framework of constitutional morality.

The right to privacy can be trifurcated into: informational privacy, that is the interest over the control of personal data; physical privacy, that is the right to bodily integrity against unlawful intrusions, and decisional privacy, which protects the personal autonomy of a person from unreasonable external influence.⁶¹ This framework is also discussed by Supreme Court judgment that upheld the fundamental right to privacy.⁶²

The right to privacy is, however, marked by the feminist critique of the obfuscation of violence against women within the household as well as the denial of their privacy in the public sphere. The Law Commission's report on the review of rape laws that came out in 2000 was of the view that criminalizing marital rape would be an 'excessive interference with the marital relationship'. In *Mrs Neera Mathur v. LIC of India and Another*, the court found Life Insurance Corporations subjection of women candidates to a pregnancy test acceptable in order to ensure recently employed women

57 IT for Change (2017), A feminist perspective on gender, media and communication rights in digital times - Key issues for CSW62 and beyond, https://www.iforchange.net/index.php/csw62-position-paper#footnote31_fbg7gl6

58 Acharya, B (2017), Privacy without principles: another look at the Notice and Choice approach, <https://www.medianama.com/2017/09/223-privacy-without-principles-another-look-notice-choice-approach/>

59 Acharya, B (2016), An unprincipled future? The imminent conflict between FIPPs and the Internet of Things, <https://medium.com/@bhairavacharya/an-unprincipled-future-c5d68534333b>

60 Manthan, R. (2017), Beyond consent: A new paradigm for data protection, <http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf>

61 Gilma, M.E (2008), Welfare, privacy, and feminist <https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2255&context=lf>

62 Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCALE

do not go on maternity leave. To questions of the regularity of her menstruation, how painless they were and when was the last time the candidate had her periods, the court deemed that women may be prevented by their 'modesty' from answering them.⁶³

The *Puttaswamy* judgment takes cognizance of the feminist contestations with privacy, proposing an interpretation emanating from gender equality and dignity. The court observes, "The challenge in this area is to enable the state to take the violation of the dignity of women in the domestic sphere seriously while at the same time protecting the privacy entitlements of women grounded in the identity of gender and liberty."⁶⁴ Privacy is not only important in political life to exercise choice without fear, but in personal life to forge intimate relationships. The right then becomes instrumental to equality in democratic society.⁶⁵

There are progressive judgments by the higher judiciary that can aid us in developing a jurisprudence on gender justice that reads privacy, equality, and dignity into each other. In *Anuj Garg*, the Supreme Court struck down the paternalistic provisions of the Punjab Excise Act that prohibited employment of women in establishments where liquor was consumed. The court declared that government actions aimed at 'protecting' women failed to countervail the "bulk of well-settled gender norms such as autonomy, equality of opportunity, right to privacy". Striking down the provision, the court asserted that laws that stereotyped male and female roles were discriminatory and unconstitutional.⁶⁶ Kannabiran similarly argues a radical constitutional interpretation that accounts for constitutional morality of non-discrimination as necessary for a jurisprudence of gender justice to emerge.⁶⁷

In a case involving the restitution of conjugal rights before the Andhra Pradesh High Court, Justice Choudary rightly recognizes the vacating of the woman's agency to that of the state as a violation of her bodily and mental privacy and consequently an affront to her integrity. Although the law is framed in gender neutral terms, the judge also acknowledges the need for substantive rather than "bare equality of treatment regardless of the inequality of realities is neither justice nor homage to constitutional principles".⁶⁸ Sexual violence, the apex court, in another case, observed is not only an intrusion into a woman's right to privacy but also 'offends her self-esteem and dignity'.⁶⁹ Dignity, the court has underlined, is a constitutional value and a goal that must guide interpretation of rights and check the proportionality of statutes.⁷⁰ From earlier case law of *Kharak Singh* and *Gobind* to the most recent ruling on privacy (cited above), the apex court has drawn out the reinforcing connect between privacy and dignity.⁷¹

On the public harm caused by discriminatory depiction of women, the idea of what is derogatory to women must not only include sexually explicit content but also other sexist content that reinforces and reproduces women's social subordination and oppression.⁷² As commentaries on Indian law

63 Mrs. Neera Mathur vs LIC of India and Another, 1992 LAB IC 72, http://www.mcrg.ac.in/development/P_writing/Kalpana1.pdf

64 Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCALE 1

65 Lever, A (2005), Feminism, democracy and the right to privacy, <http://www.minerva.mic.ul.ie/vol9/Feminism.html>

66 Anuj Garg & Ors v. Hotel Association Of India & Ors Appeal (civil) 5657 of 2007; Gautam, B (2014) Grounding a Progressive Jurisprudence of Sex Equality: Anuj Garg v. Hotel Association, <https://indconlawphil.wordpress.com/2014/02/20/grounding-a-progressive-jurisprudence-of-sex-equality-anuj-garg-v-hotel-association/>

67 Kannabiran, K (2009), Judicial meanderings in patriarchal thickets: Litigating sex discrimination in India, http://www.mcrg.ac.in/development/P_writing/Kalpana1.pdf

68 T. Sareetha v. T. Venkata Subbaiah AIR 1983 AP 356

69 The State Of Karnataka v. Krishnappa 2000 CriLJ 1793

70 Jeeja Ghosh & Anr v. Union Of India WP(Civil)NO. 98 OF 2012

71 Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCALE

72 In 1989, the Bombay High Court heard a case challenging the release of a film *Pati Parameshwar*. The film was denied certification for violating the guidelines to the Cinematography Act which prohibited 'visuals, words depicting women in ignoble servility to men, or glorifying such servility as praise worthy...'. The counter challenge mounted was that the denial of certification was a violation of Article 19(1)(a)- freedom of speech and expression. Instead of confining their argument to the merit of free speech, the judges instead sought to praise the attempt of the woman to save her marriage, denying there was anything indecent in such representation. Justice Aggarwal observes, "What is glorified is not servility, but faith, courage and sacrifice". On appeal judge went on to hold - 'The character of Rekha as depicted in the film is one of faith, dedication and endurance and out of sanctity. This is consistent with the traditions of the Hindu society to which she belonged.' Union Of India (Uoi) And Ors. v. Film Federation Of India And Anr. 1989 (3) BomCR 377

have highlighted, “the sexism in non-sexually explicit representations remains untouched by any penal liability”.⁷³ What is demeaning to women therefore must not be confused with the issue of maintaining ‘decency’. The institutionalization of popular morality tied to obscenity is dangerous in that it veers towards paternalism and misogyny. In *Naz Foundation v. Government Of NCT of Delhi*, the High Court argued for the replacement of public morality with constitutional morality in reference to discrimination based on sexual orientation. The court held, “Moral indignation, howsoever strong, is not a valid basis for overriding individuals’ fundamental rights of dignity and privacy”. The state must therefore be the guarantor of constitutional morality.⁷⁴

We now discuss how the framework to examine harm may be operationalized against TMVAW, by re-imagining some problematic legal provisions.

6. Towards new laws on technology-mediated violence against women

For a comprehensive understanding of technology mediated violence that incorporates feminist values of privacy within the larger paradigm of equality and dignity and constitutional morality, we need to look at the possibility of a dedicated law that can define the phenomenon.⁷⁵

For instance in replacing parochial anti-obscenity Sections, alternate legal provision must have a two fold function, firstly, it must redress ‘the woman’ whose representation is being exploited, and ‘women’ who are being discriminated against by such a representation. The starting point of the former should be the violation of personhood of the victim, and the devaluation of her dignity. For the latter, the law must recognize that when sexist images are published, transmitted or circulated, it is not the ‘prurient interest’ that it triggers or its effect ‘to deprave and corrupt persons’ that must be punished but the gendered discrimination that it produces.

6.1 Re-conceptualizing circulation of intimate images

Our contention is that circulation of images, especially intimate sexual images, without the consent of the person represented in those images is more than merely a speech/ representation harm and may need to be construed as an act against the body, thus implicating it.⁷⁶ Booking such offenses under anti-obscenity provisions which target the artifact and its effect on the people who consume it, rather than the impact that such an artifact has on the woman whose representation it carries seems absurd.⁷⁷ The application of anti-obscenity provisions like Section 67A of the IT Act to cases of circulation of videos of rape through WhatsApp, we would like to stress, is grossly inappropriate. In fact legal practitioners have noted how going by the letter of the law in this Section, even a person who voluntarily shares his/her image can be booked under the Section, if such an image is deemed obscene.⁷⁸ To explain with an example: individuals producing sex tapes for their private consumption and pleasure may find themselves slapped with cases of violating obscenity laws, when they try to challenge the ‘leakage’ and non-consensual circulation of such videos.

73 Kumari, V (1999), Gender analysis of the Indian Penal Code, in *Engendering Law: Essays in Honour of Lotika Sakar* edited by Amita Dhanda and Archana Parashar, http://www.cwds.ac.in/wp-content/uploads/2016/12/ca_gender_analysis1.pdf

74 *Naz Foundation v. Government Of NCT of Delhi* WP(C) No.7455/2001

75 Further, as anecdotal evidence suggests, fragmentation of provisions across legislations also complicates enforcement.

76 Extrapolating from Catharine MacKinnon’s theorization regarding pornography “words express, hence are presumed “speech” in the protected sense. Pictures partake of the same level of expressive protection. But social life is full of words that are legally treated as the acts they constitute ... Saying “kill” to a trained attack dog is only words. Yet it is not seen as expressing the viewpoint “I want you dead”- which it usually does, in fact, express. It is seen as performing an act tantamount to someone’s destruction, like saying “ready, aim, fire” to a firing squad.”

MacKinnon, C (1993), Only words, <https://foundationsofgenderstudies.files.wordpress.com/2013/01/catharine-mackinnon-only-words.pdf>

77 MacKinnon, C (1993), Only words, <https://foundationsofgenderstudies.files.wordpress.com/2013/01/catharine-mackinnon-only-words.pdf>

78 Dasgupta, P (2017), What can victims of revenge porn in India do to get the criminals punished? A long and tricky road to justice, http://www.huffingtonpost.in/2017/07/13/what-can-victims-of-revenge-porn-in-india-do-to-punish-the-perpe_a_23027563/

Consent based provisions (Section 66E IT Act and 354C IPC) may seem better than morality based provisions, but as demonstrated in the earlier sections of this paper, the benefit remains in only the letter of the law. Judicial decisions have demonstrated how consent, or the lack of it, is used to negate agency. We thus need to turn to harm based framing of the law, wherein harm is defined as the violation of privacy (personal autonomy (consent), informational privacy and physical privacy), loss of dignity and that which causes gender based discrimination.

Section 66E of the IT Act has a very rudimentary understanding of 'reasonable expectation of privacy' that is not in keeping with contemporary interpretations of the right. Thus, if a woman shares an intimate picture of hers with her partner, she may not be granted the presumption of privacy. On the point of personal autonomy, in *Collector v. Canara Bank*,⁷⁹ the court held that since privacy vests in the person, the disclosure of confidential information to a third party does not diminish the right. This conception is especially useful when intimate pictures may be shared with a third party, as the right to privacy of the person in the representation of herself becomes inherent.

On the other hand, Section 354 C of the IPC considers it an offense if the 'victim consents to the capture of the images or any act, but not to their dissemination to third persons'. Some states in the US have specific 'revenge porn' criminal laws, which as the nomenclature suggests, requires that the act is carried out with a particular intent to harass or cause harm to the victim.⁸⁰ However, holding secondary perpetrators culpable under an American style revenge porn law requires proving intent or *mens rea* that can be difficult to establish.

Knowledge here must thus be construed as actual knowledge (inferred from the conduct of the person), constructive knowledge (also known as knowledge in the second degree where a person deliberately does not make inquiries when he should have) and knowledge in the third degree (the unintentional failure to make inquiries that would be reasonable to the circumstance).⁸¹ The Canadian law - Protecting Victims of Non-consensual Distribution of Intimate Images Act 2017 - creates a tort of distribution of intimate images without consent, if the person who distributes the image *is reckless as to whether or not the person depicted in the image consented to the distribution*. Further, the Act makes it explicit that the right to privacy is not waived, even if the image was shared voluntarily and if the accused *knew or ought reasonably to have known* that there was no consent for it to be published, circulated etc. The Canadian Law on rape too requires the accused to prove that he had taken steps to ensure consent had been given for a particular sexual activity.⁸² Unless judicial interpretation in India goes this far, we will be left with the unfortunate situation where anti-obscenity provisions are invoked.

Aziz too points to alternatives where to cases where the law overlooks intent by focusing instead on the lack of due diligence such as in the case of punishment for reckless indifference in criminal law⁸³ and damages for negligence under civil law. She observes, 'ignorance of the identity of the victim/survivor does not make the violence victimless or the harm unforeseeable.'⁸⁴

79 *Collector v. Canara Bank* (2005) 1SCC 496

80 Kitchen, A.N.(2015) The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment, <https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?referer=https://www.google.co.in/&httpsredir=1&article=4065&context=cklawreview>; US lawmakers back bill to combat 'Revenge Porn' after congressman's nude photo leaks,(2017) <https://www.outlookindia.com/website/story/us-lawmakers-back-bill-to-combat-revenge-porn-after-leak-of-republican-congressman/304940>

81 Gaur, K.D (2011) Textbook on the Indian Penal Code

82 Report of the committee on amendments to criminal law (2012), <http://www.prsindia.org/uploads/media/Justice%20verma%20committee/js%20verma%20committee%20report.pdf>

83 Rash or negligent act leading to death or grievous hurt, endangers human life, or the personal safety of others is punishable under Sections 304A and 338 of the IPC respectively

84 Aziz, Z. A, Due diligence and accountability for online violence against women, <https://www.apc.org/sites/default/files/DueDiligenceAndAccountabilityForOnlineVAW.pdf>

Legal intervention on the distribution of intimate images should therefore account for the victim's right to privacy – through a reading of the right that is adequate to the digital. This would imply recognition of the right of the victim not only in the instance of non-consensual capture of images of herself, but also of non-consensual 'circulation' of the image she may have voluntarily shared. The burden of due diligence to recognize such an idea of right to privacy is on the accused.

6.2 Accounting for gender-based hate speech

In cases of representational violations,⁸⁵ since the legal framework characterizes harm as public rather than private, it is even more important to re-imagine the law to foreground the equality and dignity of women to prevent the much too easy slippage into moralistic semantics.⁸⁶ This will ensure that sexist content that degrades women is targeted. To support a gendered reading of the law, a study by Point of View demonstrates that as it stands, application of anti-obscenity Sections are clearly gendered, but unfortunately not in a gender empowering way.⁸⁷

India does have identity based legislation like the Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989. However, the Act does not adequately address the issue of identity based hate speech. Under the Act, any person who “intentionally insults or intimidates with *intent to humiliate a member* of a Scheduled Caste or a Scheduled Tribe in any place within *public view*”,⁸⁸ is punishable. But if they do not implicate the targeted person directly but only his or her identity, then such acts do not fall afoul of the legislation.⁸⁹ The Delhi High Court has in *Ms. Gayatri Apurna Singh v. State & Anr W.P.* read the Section to cover online abuse ruling, “Offensive statements on the social media like Facebook, whether private or public and intended to humiliate someone belonging to the Scheduled Caste or Scheduled Tribe communities, would be a punishable offense.” The judgment, however, limits the Section's application to when statements are targeted at a specific individual belonging to a SC/ST community. General casteist statements against the community are not punishable.⁹⁰

The existing provision on hate-speech must be amended so that it covers generalized, misogynistic abuse offline and online. Section 153A of the IPC attempts to check speech that incites hatred “on grounds of religion, race, place of birth, residence, language etc.” and “doing acts prejudicial to maintenance of harmony”. In its current form, this provision has two critical drawbacks. Firstly, it fails to acknowledge that different groups, castes, and communities are not on an equal footing, and therefore does not adequately account for misuse by dominant sections of society. Secondly, it does not address hate-speech linked other key markers of a person's identity: sex, gender identity and sexual orientation⁹¹. Section 153A could be re-framed to cover gender-based hate-speech, in a manner that does not enable its invocation/ misuse by self-styled men's rights groups.

The Law Commission's report on 'hate speech' recommended revision to Section 153A of the IPC includes 'sex, gender identity, sexual orientation' within its ambit. It also recommends the insertion of a new Section 505A into the IPC, worded as follows

85 Such as the obscenity provisions -Section 298 of the IPC or Sections 67 and 67A of the IT Act

86 Liang, L. (2015), What Do We Talk About When We Talk About Pornography, <https://thewire.in/7811/what-do-we-talk-about-when-we-talk-about-pornography/>

87 Point of View (2017), Guavas and genitals: A research study https://www.apc.org/sites/default/files/Erotics_1_FIND.pdf

88 Section 3(1)(r) Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989

89 The logic will also apply to a new Section 3(1)(w)(ii) added after the 2015 amendment of the Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Amendment Act, 1989 which penalizes “use of words, acts or gestures of a sexual nature towards a woman belonging to a Scheduled Caste or a Scheduled Tribe, knowing that she belongs to a Scheduled Caste or a Scheduled Tribe.

90 *Ms. Gayatri Apurna Singh v. State & Anr W.P.* (CRL) 3083/2016, <https://drive.google.com/file/d/0Bzj5De7gaTEYTGZsdEF0aGJFN1E/view>

91 Padte, R.K. (2013), Keeping Women Safe, <https://internetdemocracy.in/wp-content/uploads/2013/04/Internet-Democracy-Project-Gender-Online-Harassment-and-Indian-Law.pdf>

505 A. Whoever in public intentionally on grounds of religion, race, caste or community, sex, gender, sexual orientation, place of birth, residence, language, disability or tribe uses words, or displays any writing, sign, or other visible representation which is gravely threatening, or derogatory; (i) within the hearing or sight of a person, causing fear or alarm, or; (ii) with the intent to provoke the use of unlawful violence, against that person or another, shall be punished⁹²

The T.K. Viswanathan committee set up to examine the legal framework on online hate speech also made a similar recommendation to be applied to electronic communications. Scholars have, however, argued that phrases used in the draft Sections are vague and contradict the *Shreya Singhal* judgment.⁹³

6.3 Reformulating ‘outraging the modesty’ of women

Section 509 of the IPC needs to be changed so that it adequately covers all online and offline acts that constitute a criminal breach of privacy. In this attempt, we can take a leaf out of Section 354C of the Criminal Law (Amendment) Act 2013 that moves away from the notion of womanly modesty to a physical privacy framework, in addressing voyeurism. ‘Intended to insult the modesty of a woman’ must be replaced with criminal breach of privacy, which includes violation of bodily integrity and personal autonomy of a woman.

Accessing and/or distributing, publicly exhibiting or in any manner putting into circulation her personal information without her consent should also be expressly included within the Section. Such an interpretation will also cover acts of doxxing. Breach of confidentiality of personal information must be interpreted, building on the observations around the right to confidentiality in the Supreme Court judgment in *R. Rajagopal v. State of T.N.* popularly known as “Auto Shanker case”. The Court held that,

*The ‘right to privacy’, or the right to be let alone is guaranteed by Article 21 of the Constitution. A citizen has a right to safeguard that privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical.*⁹⁴

Decoding the digital is vital in order to argue the need for a fresh epistemological approach to understand TMVAW. The next section elucidates how techno-materiality arranges online and offline conduct.

7. Why the digital is different - the need for a new law

Making incremental changes within an overarching moralistic, protectionist and misogynistic framework that is the IPC and other laws such as the IT Act can take us only so far. An argument in favor of new legislation that specifically deals with TMVAW is guided by the school of thought that online contexts create new structures of communication and social interaction.

⁹² Law Commission, Report no. 267- Hate Speech, <http://lawcommissionofindia.nic.in/reports/Report267.pdf>

⁹³ Sinha, A. (2017), New recommendations to regulate online hate speech could pose more problems than solutions, <https://thewire.in/187381/new-recommendations-regulate-online-hate-speech-problems/>

⁹⁴ *R. Rajagopal v/ State of Tamil Nadu* 1995 AIR 264

To develop a framework of TMVAW, at the outset, we need to establish a certain common understanding. Firstly, the online-offline continuum of violence with one feeding into the other is a necessary starting point. But, we also recognize the ontological and relational axes of the offline are vastly different from the online. The materiality of the online structures violence in ways that the offline never anticipated. For example, the ease of transmission and the ability for violence to spread like wildfire, and the performativity of violence, as in cases of live streaming of gender-based violence, are rooted in the peculiar architectures of a networked online.⁹⁵ Suler, in his works, has noted that disassociative anonymity, invisibility of the reactions of the listener, asynchronicity of expression and reception online can lead to a toxic dis-inhibition that promotes violence.⁹⁶

Secondly, life online is not a simulation of life, but an extension of it;

*The use of Internet-based communication technologies, such as Internet messaging (IM), chat, and social networks, provide an extension of social contexts in which individuals can interact. The various social context and relationships developed using such social technologies, facilitates the development and recognition of an individual's social identification.*⁹⁷

Thus, online violence is not a mere violation of representation, it is a violation of the self, making cyber-touch as harmful as physical touch.⁹⁸

Thirdly, the overwhelmingly neo-liberal logic of the digital frames social interaction online, introducing new actors that the legal framework must account for.⁹⁹ Thus, identity online is not merely a function of individual agency. It is co-constructed by the particular, patriarchal, neo-liberal interventions by actors dominating the Internet.

Digitally mediated 'speech' and 'action' must therefore be evaluated distinctly and the law has to take a nuanced approach.¹⁰⁰ In May 2016, the Ministry of Women and Child Development made a media announcement that it is deliberating a new code on online trolling.¹⁰¹ Similarly, in 2014, one of the recommendations proposed by the National Commission for Women from its consultation on 'Ways and Means to safeguard women from Cyber Crimes in India' was that, "A woman centric information technology law must be drafted defining types of cybercrimes targeting women. IT Act, 2000 (as amended in 2008) is not women sensitive Act (sic). It needs to be reviewed to introduce more innovative approaches in law."¹⁰²

Rather than a piecemeal approach that can be argued to be tactically less plausible or potentially long-drawn, a new legislation that focuses exclusively on the systemic nature of TMVAW and explicitly addresses its emerging forms, can be introduced. Some countries have adopted the route of enacting new laws. Senator Risa Hotiveros from the Philippines has sought the passage of Anti Gender-based Electronic Violence Bill. Taking from the UN Declaration on the Elimination

95 Aziz.Z.A., (2017), Due Diligence and Accountability for online violence against women, <https://www.apc.org/sites/default/files/DueDiligenceAndAccountabilityForOnlineVAW.pdf>

96 Online disinhibition effect (Suler), <https://www.learning-theories.com/online-disinhibition-effect-suler.html>

97 Code.J.R & Zaparyniuk.N.E., (2010), Social Identities, Group Formation, and the Analysis of Online Communities, <http://wiki.stoa.usp.br/images/8/89/Socialidentity.pdf>

98 Broadband commission for digital development working group on broadband and gender,(2015), Cyberviolence against women and girls: a worldwide wakeup call, http://www.unwomen.org/~media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259

99 Pavan, E. (2017). Internet intermediaries and online gender-based violence. In Segrave,M & Vitis,L. Gender, technology and violence. Routledge

100 Christopher-Jones, B. (2016), The online/ offline cognitive divide: Implications for law, <https://script-ed.org/article/the-onlineoffline-cognitive-divide-implications-for-law/>

101 Abraham, B. (2016), Maneka Gandhi wants trolling of Women online be considered as violence, <https://www.indiatimes.com/news/india/maneka-gandhi-wants-trolling-of-women-online-be-considered-as-violence-255267.html>

102 National Commission for Women (2014), Recommendations of the consultation on ways and means to safeguard women from cybercrimes in India, <http://ncw.nic.in/pdfReports/RecommendationsConsultation23072014.pdf>

of Violence against Women, the Bill defines gender-based technological violence by adding to it the flavor of the digital by tethering it to dignity and personhood. The definition states,

Any acts or omissions involving the use or exploitation of ephemeral data or any form of information and communications technology (ICT) which causes or is likely to cause mental, emotional, or psychological distress or suffering to the female victim or Lesbian Gay Bisexual Transgender Queer (LGBTQ) victim, and tending to disparage the dignity and personhood of the same on account of his or her gender

Others such as New Zealand have approached the issue from a gender neutral standpoint. The Harmful Digital Communications Act, 2015 as the name suggests seeks to deter, prevent and mitigate harm caused to individuals by digital communications". Harm, the Act clarifies, is to be understood as 'serious emotional distress'.¹⁰³

7.1. Intermediary liability

There is a new type of private actor implicated in technology mediated violence – the Internet intermediary. Internet intermediaries refer to *"technical providers of Internet access or transmission services, and providers of content hosting services."*¹⁰⁴ The liability that should be fixed on such actors for unlawful or harmful content created by users of their services has been a subject of debate – especially when it comes to discussions on VAW.

Experiences from across the globe reveal that broad liability regimes which impose contributory liability on intermediaries for actions of users (such as that adopted in China and Thailand) lead to over censorship and preemptive content blocking that lead to unjustifiable curbs on citizens' free expression. Safe harbor regimes which provide immunity to intermediaries for the actions of their users, as long as certain conditions laid down in law are met, have proven a better approach to effectively balance the right to free expression with freedom from violence.

Broadly, the conditionalities imposed by safe harbor regimes can be classified into the following categories:

- (a) Regimes that require Internet intermediaries to take down objectionable content, only on the basis of an order by the judiciary and competent executive authority. Eg. Chile, India.
- (b) 'Notice and Take-down' regimes that require Internet intermediaries to take down content that is classified as obscene, harassing or violent or impermissible according to an existing law, once they are notified about such content by a user. Eg. United States.
- (c) 'Notice and Notice' regimes that require Internet intermediaries to notify the author of a piece of content against which a complaint has been received, and then proceed to take down the content subject to certain conditions (such as the author failing to respond to the notice with an explanation of why the particular piece of content should not be taken down). Eg. New Zealand.

India has adopted a safe-harbor approach to intermediary liability, and the safe-harbor has been strengthened by the Supreme Court judgment in *Shreya Singhal vs Union of India*. Section 79 of the IT Act provides immunity from legal liability to intermediaries, with the following exceptions: - conspiracy/abetting in the commission of the unlawful act [Section 79 (3)(a)], and

¹⁰³ The first principles established under the Act have been critiqued for undermining free speech. See O'Brien, D. 2015. New Zealand's Harmful Digital Communications Act: Harmful to everyone except online harassers, retrieved <https://www.eff.org/deeplinks/2015/07/nz-digital-communications-act-considered-very-harmful>

¹⁰⁴ Association for Progressive Communications (2014), Frequently asked questions on intermediary liability, <https://www.apc.org/en/pubs/frequently-asked-questions-internet-intermediary-l>

- failure to expeditiously remove/ disable access to the unlawful material – which may be information, data or communication links, upon receiving actual knowledge about this or being notified by the appropriate government or agency [Section 79 (3) (b)]

In the *Shreya Singhal* judgment which struck down Section 66(A) of the IT Act (an overwhelmingly generic provision that penalized electronic communication of a ‘grossly offensive’ or ‘menacing’ character) for its unreasonable and excessive curbs on the right to free speech, the Supreme Court also read down what constitutes ‘actual knowledge’, as highlighted in Section 79 (3) (b) of the same Act, based on which the intermediary can lose safe harbor:

Para 119.C. *Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relating to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material.*

Para 117. *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.*

Further, the Supreme Court went on to read down the Information Technology (Intermediaries Guidelines) Rules 2011 to re-affirm that intermediaries should not independently take down content, in response to a complaint received about an unlawful piece of content¹⁰⁵ from an affected person. They should only act upon judicial or executive orders. The Supreme Court’s interpretation of intermediary liability may be seen as positive since it leaves no room for delegated enforcement of censorship of unlawful content by intermediary platforms.

In *MySpace vs. Super Cassettes*¹⁰⁶ on the question of knowledge of copyright infringing material on MySpace platform, the High Court held “Knowledge has a definite connotation, that is, a consciousness or awareness and not mere possibility or suspicion of something likely. The nature of the Internet media is such that the interpretation of knowledge cannot be the same as that used for a physical premise.” However, the court, differentiating itself from the *Shreya Singhal* standard of an intervening court/executive order before take down, held that a mere notice is sufficient for take down of copyrighted material. The rationale here being that the *Shreya Singhal* case, unlike the present one, dealt with restrictions on the freedom of speech (Article 19(2) of the Constitution).¹⁰⁷

Evidence from around the world suggests that when enforcement is delegated to intermediaries, and in the case of the ‘Notice and Take-down’ regime of the US, the results are sub-optimal and arbitrary – especially in the domain of online VAW. For example, Facebook has allowed misogynistic pages such as ‘Boobs, breasts and boys who love them’ to flourish, despite repeated complaints, though it continues to censor pictures of breastfeeding mothers. Another problem is that platforms do not take any steps to prevent their user policies from inadvertently facilitating VAW. Recently, in Kerala, trolls used the real name authentication policy of Facebook to get the

¹⁰⁵ Unlawful content, according to Rule 3(2) of the Information Technology (Intermediaries Guidelines) Rules 2011 is content that “(a) belongs to another person and to which the user does not have any right to; (b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libelous, invasive of another’s privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever; (c) harm minors in any way; (d) infringes any patent, trademark, copyright or other proprietary rights; (e) violates any law for the time being in force; (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature; (g) impersonate another person.”

¹⁰⁶ *MySpace vs. Super Cassettes* FAO (OS) 540/2011, C.M. Appl. 20174/2011, 13919 and 17996/2015

¹⁰⁷ Gautam, B. (2017), Online speech and intermediary liability: The Delhi High Court’s MySpace judgment, <https://indconlawphil.wordpress.com/2017/01/16/online-speech-and-intermediary-liability-the-delhi-high-courts-myspace-judgment/>

account of a woman activist suspended. Similarly, when trolling takes place from non-personal pages, despite repeated requests from the affected persons, Facebook has refused to reveal the administrator of such pages.¹⁰⁸

Experiences of users in contexts outside the United States and Europe, including India, reveal that Internet intermediaries are not responsive and do not provide an accessible reporting and redress process, with respect to complaints about online VAW. Research studies indicate that platforms are often unresponsive when the subject-matter involved is not in English. They are also non-transparent about how they resolve/ dispose complaints received. Handing more powers to entities that are already unaccountable to users in the global South seems a bad idea.

The counter-view is that expecting the court to intervene in every instance of online VAW will lead to inordinate delays in resolution, and that a compromise should be reached, by placing upon Internet intermediaries some specific and clearly defined responsibilities, with adequate safeguards to prevent overreach. The proponents of this view hence argue for moving away from an 'intermediary liability' framework to one of 'platform responsibility', wherein online platforms (such as Facebook, Twitter, Youtube etc.) are encouraged to adopt zero tolerance towards human rights violations on the spaces they control, in accordance with the spirit of the UN Guiding Principles on Business and Human Rights.¹⁰⁹ To operationalize this, social networking and social media platforms may have to overhaul their existing Terms of Service (which act as the 'law of the land' in these spaces) so that the commitment to free expression in such agreements is balanced by an effective response to ensuring freedom from violence.¹¹⁰ Skeptics have dismissed this view by citing the poor track record of online platforms in protecting, promoting and respecting the rights of women and gender minorities.

New Zealand has adopted the third approach of Intermediary liability, by putting in place an independent arbitration mechanism that limits the responsibility of Internet intermediaries/ online platforms to that of performing a first level process of arbitration in cases of online VAW, without any powers of censoring content. This has been achieved by the Harmful Digital Communication Act 2015 cited in the earlier section of the paper.

This Act defines harmful digital communication as a piece of communication that can potentially cause harm to an ordinary reasonable person in the position of the victim. An affected person can approach the concerned Internet intermediary/ online platform, who is then required to notify the author of the communication within 48 hours of receiving such complaint. The author has 48 hours to respond with a counter-notice – that either consents to the take-down of such communication or records an objection. The intermediary/ platform can take down the communication only if the author consents. In case of an objection by the author, the intermediary should not take down the content. Their only obligation in such an instance is to notify the complainant, who may then proceed to the process of judicial arbitration prescribed under the Act. Where the author does not reply within 48 hours of being notified by the intermediary/platform or is untraceable because the communication is anonymous, the intermediary/ platform is required to take down the content at the end of this period. This mechanism thus allows the intermediary/ platform to play the role of a mediator between the complainant and the author of a piece of communication reported as 'harmful', to help them arrive at a settlement by following a clearly defined step-by-step process. This urgent need to investigate alternate approaches to or in addition to the mechanisms prescribed by *Shreya Singhal* is promoted by two cases.

108 Primary field research carried out by IT for Change

109 Dynamic coalition on platform responsibility (DC PR), <http://www.intgovforum.org/cms/2008-igf-hyderabad/event-reports/74-dynamic-coalitions/1625-dynamic-coalition-on-platform-responsibility-dc-pr>

110 Nyst, C. (2014), Internet intermediaries and violence against women online: Executive Summary and findings, <http://www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf>

Dr. Sabu Mathew George v. Union of India and Others dealt with intermediary liability of search engines for advertisements on their services regarding pre-natal or pre-conception sex determination banned by the Section 22 of the Pre-natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 (PNDT Act).¹¹¹ Asking for auto-block to be operationalized the court urged for a harmonious reading of the PNDT Act and the freedom of seek information. The court in this case also directed the government (Ministry of Health and Family Welfare) to set up a nodal agency which can receive complaints of advertisements that violate the PNDT Act and then relay it to the search engine for take down. The respondent corporations were directed to set up in-house experts who can, on their own, take down content. In case of doubt, the in-house expert may confer with the government nodal agency. Petitioners have complained that illegal advertisements continue to be seen online and that the court set-up machinery has not been functioning properly. The petitioner also pointed out that although in other cases the Google has conducted pro-active filtering, however, it has refused to do so in this case. As per its December 2017 orders, the Court has directed the nodal agency, the in-house expert and the respondent digital corporation to come together and develop a solution.¹¹² What the solution will be is unknown.

The second case - *In Re Prajwala*¹¹³, dealt with the circulation of videos of rape online. The court set up a committee with representatives of the Ministry of Electronics and Information Technology, Home Affairs, Indian Computer Emergency Response Team, Facebook, Google, Yahoo, Microsoft, WhatsApp and the counsel and *amicus* of the petitioner to develop technological and administrative solutions to the problem. Few of the committees proposals are: expanding key-word searches to take down criminal content¹¹⁴; setting up a cell within the CBI that will deal with these crimes; setting up a Central Reporting Mechanism or a hotline number; creating a hash-bank of criminal content that the Ministry of Home Affairs will maintain. The committee also proposed that Content Hosting Platforms (CHPs), Search Engines and the government together formulate a process for proactively verifying, identifying and initiating take down of criminal content and expeditious initiation of prosecution against users for identified criminal content. The committee has also urged for “greater thrust and emphasis on research & development of Artificial Intelligence (AI)/Deep Learning (DL)/Machine Learning (ML) based techniques for identifying criminal content at the stage of uploading to enable real time filtering.”¹¹⁵ The status report filed by the Government on the implementation of the proposals has however been disappointing.¹¹⁶

Whether these are good routes to comprehensively address TMVAW is a matter for open debate - as the flip side is that we may inadvertently end up consolidating the market power of online platforms by insisting upon their role in arbitration and policing functions.

The penultimate section of the paper will discuss how traditional institutional actors - law enforcement agencies - have dealt with TMVAW.

111 *Dr. Sabu Mathew George v. Union of India* Writ Petition (Civil) No. 341 of 2008, <http://www.advocatekhaj.com/library/judgments/announcement.php?WID=9580>

112 *Dr. Sabu Mathew George v. Union of India* Writ Petition (Civil) No. 341 of 2008, <http://www.advocatekhaj.com/library/judgments/announcement.php?WID=9580>

113 *In Re Prajwala* SMW (Cr.)No(s).3/2015, http://supremecourt.gov.in/supremecourt/2015/6818/6818_2015_Order_23-Oct-2017.pdf

114 Criminal content here refers exclusively to child pornography, rape and gang rape videos

115 *In Re Prajwala* SMW (Cr.)No(s).3/2015, http://supremecourt.gov.in/supremecourt/2015/6818/6818_2015_Order_23-Oct-2017.pdf

116 *In Re Prajwala* SMW (Cr.)No(s).3/2015, http://supremecourt.gov.in/supremecourt/2015/6818/6818_2015_Order_23-Oct-2017.pdf

8. Enhancing the responsiveness of law enforcement agencies

Law enforcement agencies fail to recognize that online VAW is as grievous as offline VAW.¹¹⁷ Women's rights groups highlight that despite trainings on gender sensitization, in their response to complaints about TMVAW, the police engage in victim blaming and/or trivialization of the offense. The establishment of Cyber Cells does not seem to have improved this state of affairs.¹¹⁸ Law enforcement officials fail to recognize the legitimacy of women's subjective experience of violation, when consent given earlier is subsequently withdrawn.¹¹⁹ In the 2016 study, '*Cyber Violence Against Women in India*', out of the 500 respondents interviewed about their experiences of online VAW, 1/3 reported that they had approached the police. Among those who went to the police, 38% expressed the view that "they were not at all helpful" and over half (52 percent) said that officials do not take complaints of online harassment seriously.¹²⁰

To address this lack of responsiveness, the National Commission for Women, in its 2014 consultation on '*Ways and Means to safeguard women from Cyber Crimes in India*' recommended that women officers be deputed to Cyber Cells. The Home Ministry has instituted the Cyber Crime Prevention against Women and Children Scheme financed by the Nirbhaya Fund. The scheme seeks to set up an online reporting platform (as is discussed in the *Prajwala* judgment), forensic labs, forensic training institutes etc.¹²¹ Rs 82.8 Crore has been released under the scheme to set up a 'training lab cum training centre in each state/UT'. While this may be important for fighting cyber crimes in general how they will be applied to mainstream gender-based cyber crimes needs to be laid out. The Ministry has, however released funds for capacity building with respect to prevention of cyber crime against women and girls.¹²²

But this may not be enough – for, the key is to challenge the 'culture of impunity' that law enforcement agencies are mired in. Two potential steps that could be taken in this direction, are detailed below:

- (1) The Police Complaints Authority must function more effectively to be able to address complaints of police inaction. A Police Complaints Authority needs to be set up in every state, an agenda that is long pending, despite the decade-old Supreme Court order mandating this.¹²³
- (2) Police and Cyber Cell officers who fail to take cognizance of incidents of TMVAW brought to their notice, must be penalized¹²⁴.

Further, Investigating officers must be trained in the collection and preservation of digital evidence so that it is produceable in court.¹²⁵ Police must move towards the adoption of standard operating procedure while collecting digital evidence to ensure its admissibility in court.¹²⁶ The production of secondary electronic evidence in courts of law should not be prohibitively difficult for victims of TMVAW.¹²⁷

117 UN Women (2015), Cyber-violence against women and girls: A world-wide wake-up

call, http://www.unwomen.org/~media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf

118 Primary field research carried out by IT for Change

119 Primary field research carried out by IT for Change

120 Pasricha, Japleen (2016), 'Violence' online in India: Cybercrimes against women and minorities on social media,

http://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf

121 Siddiqui, M.Y., Cyber crime prevention against women and children, http://www.swargvibha.in/aalekh/all_aalekh/cybercrime.html

122 Ministry of Home Affairs (2018), Advisory on cyber crime prevention and control,

http://www.mha.nic.in/sites/upload_files/mha/files/CyberCrimePrevention_15012018.PDF

123 Kashyap, Nitish (2016), Bombay HC frowns at state's delay in setting up police complaint authority, <http://www.livelaw.in/bombay-hc-frowns-states-delay-setting-police-complaint-authority/>

124 Such action needs to be treated as an offense that is equivalent to the failure to report offenses listed under Section 166 A of the India Penal Code and Sections 19 and 20 of the Protection of Children from Sexual Offenses Act (2012)

125 Delhi court asks police to improve quality of investigation, impart e-knowledge (2016), <http://indianexpress.com/article/india/india-news-india/delhi-police-court-training-probe-electronic-knowledge-forensic-techniques-police-investigation-2817038/>

126 Income Tax Department (2014), Digital evidence investigation Manual, http://www.itatonline.org/info/?dl_id=1692

127 Courts can set complex standards for determining authenticity of digital evidence which may initially seem necessary, but may in the end prove to be a deterrent to women producing digital evidence. For instance: Section 65B of the Indian Evidence Act lays down the various

In light of the pervasiveness of technology-mediated VAW, coupled with the Supreme Court's decision in the *Shreya Singhal* case, which mandates judicial or executive orders for any content take-downs, it may also be worthwhile for the Ministry of Women and Child Development to consider the establishment of a separate adjudicatory body, with all the powers of a court, to exclusively tackle TMVAW (similar to the National Green Tribunal that specifically addresses cases of environment protection and conservation). This body should also have the power to *suo-moto* take cognizance of cases of TMVAW.

9. Conclusion

This paper has attempted to draw up the background context and consolidate the debates on TMVAW and the law. Invoking the history of feminist thought on the law in the country, we acknowledge that challenging hegemonic cultures of masculinity that endorse men's sense of entitlement over women and the active perpetuation of misogynistic behavior is a task that goes much beyond the domain of legal intervention. However, the need to bring appropriate legislation and institutional changes commensurate with the emerging challenges of digitally mediated social life cannot be over emphasized.

The key issue here is carving out a legal-institutional response that effectively addresses the systemic nature of technology-mediated violence, in its sexually explicit and other sexist ways. This task requires us to re-think some core concepts that we deploy in law, to keep abreast of the changing realities of the digitalized society we inhabit. Culpability needs to be re-imagined in instances of new forms of violence – such as online re-circulation of sexually explicit videos and images without consent where active and constructive knowledge are accounted for. We need to ensure that existing legal provisions penalizing 'lasciviousness' – which are based on a narrow framework of public morality – do not end up curbing sexual expression. Public morality must be replaced by a more democratic, constitutional morality.

Courts must recognize the baggage that comes with consent based provisions using, instead, a feminist jurisprudence. Creating a new law that the digital demands requires the re-imaging of harm in cases of TMVAW as an affront to constitutionally understood notions of equality and dignity borne out of the violation of privacy. This is essential to a feminist understanding of social transformation. Finally, the nitti-gritty of court procedure may need to be re-visited.

Any legal reform on TMVAW should effectively be able to address the following questions, using feminist jurisprudence;

I. In terms of overhauling existing legal frameworks,

- How can we move from a protectionist framework to one that promotes the equality and dignity of women, recognizing the situatedness of TMVAW and foregrounding women's right to privacy, consisting of bodily integrity, personal autonomy and informational confidentiality?

conditions for the admissibility of electronic record, including a certificate identifying the electronic record as authentic that is signed by 'a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities'. The Supreme Court in *Anvar P.V v. P.K.Basheer Civil Appeal No. 4226 of 2012* has categorically held that electronic records cannot be produced as secondary evidence without fulfilling the requirements of Section 65B. This may prove difficult to establish. On an aside, one must remember that just because digital evidence can be produced, it does not mean justice will be served.

- How then do we:
 - How do we frame the culpability of primary and secondary perpetrators in non-consensual circulation of intimate images?
 - How should hate speech laws be amended to include hate speech based on sex, gender and sexual orientation?
 - How do we ensure that psychological violence resulting from privacy violations is effectively addressed?
 - Do we need a new legal provision addressing doxxing, if so how should it account for informational privacy of women?

II. To address Intermediary liability,

- What responsibilities should be placed on Internet intermediaries in terms of responding to instances of TMVAW?
- What kind of intermediary liability regime will ensure timely justice for women without ushering in a privatized censorship regime?

III. Finally, to construct a robust and responsive institutional machinery, including law enforcement,

- What kind of procedural changes can improve law enforcement with regard to technology mediated violence?
- Do we need a separate adjudicatory body to deal with TMVAW? If yes, what would be this body's powers and functions?