Technology-mediated Violence against Women in India

How can we strengthen existing legal-institutional response mechanisms?

A discussion paper from IT for Change
January 2017

Table of Contents

1. Introduction: Understanding Technology-mediated Violence against Women.....1
2. How does the law view technology-mediated VAW? – Taking stock of existing legal provisions.....3
2.1 Gaps in existing provisions of the law.....4
2.2 How can we overhaul existing legal frameworks?.....5
3. Intermediary liability.....8
4. Enhancing the responsiveness of law enforcement agencies.....11
5. Conclusion and questions for discussion.....12

1. Introduction: Understanding Technology-mediated Violence against Women

The purpose of this issue paper is to lay out the key legal, institutional and ethical issues concerning technology-mediated Violence against Women (VAW), to raise critical questions for further deliberation and action. This paper 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, 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. Ironically, the characteristics that make Information and Communication Technologies (ICTs) a strategic instrument for women's empowerment have also led to their persecution. The cloak of online invisibility encourages patriarchal attitudes of entitlement over women, hounding out those women who are seen as threatening prevailing gender norms[3]. A *toxic dis-inhibition*[4] is evident in the online public sphere, lowering thresholds for sexist and misogynistic speech and behaviour.

Technology-mediated VAW 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.[5]"*

1 We are grateful to Japleen Pasricha - FeminisminIndia; Swarna Rajagopalan - Prajnya; and Shakun Mohini, 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

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

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

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

5 APC (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

Some common forms of technology-mediated VAW include[6]:
1. Harassment on web and mobile platforms, whether sexual or not. This may escalate to cyber-bullying and trolling.
2. Stalking/monitoring an individual's movements through tracking her online behaviour.
3. Hacking an individual's email and social media accounts to obtain personal information. Oftentimes, this is linked to 'doxing' – the online publication of such information without the consent of the concerned individual.
4. 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.
5. Creating fake profiles of women with the intent to harass – by discrediting, defaming and damaging their reputations.
6. Non-consensual circulation and malicious distribution of private material, including intimate photographs and sexually explicit imagery/text.
7. Publishing or transmitting content that targets women based on their gender and is accompanied with 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 technology-mediated VAW. In 2014-15, according to NCRB, only about 10% of cybercrimes reported for this period pertain to offences against women/ offences of a sexual nature[7]. Similarly, between 2014-15, the National Commission of Women registered a mere 178 complaints of cybercrimes against women[8]. However, considering that the majority of victims of technology-mediated VAW prefer not to seek legal recourse due to prevailing cultures of victim-blaming and shaming, these statistics must be recognized for what they reveal – 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.[9]

Technology-mediated VAW, contrary to popular imagination, 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 technology-mediated VAW across 7 countries[10] 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.[11] 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.[12]

The pervasiveness of technology-mediated VAW and its increasing normalization thus requires urgent action.

---

6 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

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

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

9 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

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

11 http://www.genderit.org/node/4214

12 Report of the meeting on technology-mediated violence against women in India held on 19 January, 2017 at IT for Change.

Technology-mediated VAW has a number of detrimental impacts on women's well-being. It not only causes severe emotional and psychological distress and portends the threat of physical harm, but also 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.

Countering technology-mediated VAW is not possible without a legal-institutional approach that acknowledges online violence to be as material as offline violence[13]. The experience of violence comprises a continuum of offline and online acts of abuse which reinforce one another. A fresh epistemological approach is hence required to understand the phenomenon for further recommendations on the legal-institutional directions.

2. How does the law view technology-mediated VAW? – Taking stock of existing legal provisions

The primary Acts that deal with technology-mediated VAW 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 technology-mediated VAW 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 offence this provision addresses	What forms of online VAW can this provision help in challenging?
IT Act	Section 66E	The capture and electronic transmission of images of private parts of a person, without his/her consent.	- Non-consensual circulation and malicious distribution of sexually explicit photographic and video material about an individual.
	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.
	Section 67A	The publishing or transmission of sexually explicit content 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.
	Section 67B	The electronic publishing or transmission of material in electronic form that depicts children in obscene or indecent or sexuallly explicit manner.	- Circulation of child pornography
IPC	Section 354 A	Sexual harassment, including by showing pornography against the will of a woman	- Graphic sexual abuse on social media and blog platforms, including trolling. - Sending video and pictures with sexually explicit content and images to a woman, against her will.
	Section 354 C	Voyeurism, including watching or capturing the image of a woman engaging in a private 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	- Non-consensual production, circulation and malicious distribution of sexually explicit photographic and video material about a woman.

13 Research the world over shows that strong laws on violence act as a deterrent.

Act	Clause	Details of the offence this provision addresses	What forms of online VAW can this provision help in challenging?
		where she has agreed to the capture of the images but not to their dissemination.	
	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. 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.

2.1 Gaps in existing provisions of the law

1. Online verbal harassment and abuse that does not involve 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. Similarly, acts of doxing that do not involve the circulation of sexually explicit imagery and are unaccompanied by intimidation/ slander are not covered. Though the IT Act does have a provision which criminalizes hacking (Section 66), it does not explicitly mention hacking for the purpose of doxing.

Sections 499 and Section 507 of the IPC and Section 66 of the IT Act construct online verbal harassment, abuse, trolling and hacking of personal information as "*isolated and individualised crimes*[14]*".*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"*[15]. Anecdotal evidence strongly indicates that abuse or violation directly targets women's social identity and location (particularly sexual orientation and caste).

2. Violence against women is not framed as violation of a woman's bodily integrity and personal autonomy by all sections under the IT Act and IPC. The exceptions are Section 66E of the IT Act and Sections 354C, 354D of the Criminal Laws (Amendment) Act 2013, but they focus narrowly on physical privacy, ignoring thereby the breach of informational privacy[16]. Note that though Section 509 mentions the word 'privacy', it equates intrusion of privacy with the violation of womanly modesty. Sexual violence is largely viewed from the standpoint of maintaining public decency through curbing obscenity and protecting the modesty of women. Feminists have also highlighted that the general experience across countries is that 'consent' may not be interpreted as a multi-

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

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

16 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.

layered act, whereby a woman can withdraw at any point, consent that was previously given. 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 social norms and controls over women's sexuality rather than protecting women's bodily integrity and/ or their informational or decisional privacy. 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 offence, and not in social or gendered terms.

3. There is no recognition in the law of gender based psychological violence against women outside the familial setting[17]. 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.

4. Also, 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.

Existing legal frameworks need an overhaul, so that they acknowledge:

- the systemic nature of technology-mediated VAW, which results in abusive cultures of violence impacting women in both sexually explicit and other sexist ways.

- any act, offline or online, that leads to the violation of a woman's bodily integrity and/ or infringement of confidentiality of personal information, and/ or personal autonomy, as a criminal breach of privacy.

- technology-mediated violations of a woman's personhood that are psychological/ emotional, to be as real as physical violations.

2.2 How can we overhaul existing legal frameworks?

Legal frameworks and institutional mechanisms to tackle technology-mediated VAW can involve reform of existing laws (a piecemeal approach) or enactment of a new legislation specifically addressing technology-mediated VAW (a holistic approach).

Option 1. Possibilities for reform of existing legal provisions, especially the IPC (not exhaustive)

This option is based on the understanding that the real problem in the Indian context in dealing with violence against women has been one of enforcement and not the lack of legal frameworks. Introducing new legislation to address particular types of systemic discrimination or marginalization – such as the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities Act) – has not historically proved effective in ensuring justice for the most oppressed. On the contrary, proliferation of legislation can result in a plethora of scattered legal provisions, without improving implementation by law enforcement agencies.

Specific sections of the IPC need to be revised as follows:

(a) 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*

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

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 to two other key markers of a person's identity: gender identity and sexual orientation[18]. 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.

(b) 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.

Currently, the text of Section 509 is as follows:

> 509. **Word, gesture or act intended to insult the modesty of a woman**. Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.

We propose the following wording for this section:

> **509. Word, gesture or act constituting criminal breach of privacy, including violation of bodily integrity and personal autonomy of a woman.** Whoever, intending to violate the bodily integrity and/or personal autonomy of any woman, utters any word, sends any text, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, such text shall be viewed, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman by accessing and/or distributing, publicly exhibiting or in any manner putting into circulation her personal information[19] without her consent, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.

Explanation: This provision shall apply to offline and online interactions.

(c) Existing legal provisions on the circulation of sexually explicit content and the representation of women's bodies, currently being invoked in relation to technology-mediated VAW must be revisited. 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. As commentaries on Indian law have highlighted, *"the sexism in non-sexually explicit representations remains untouched by any penal liability[20]".* What is demeaning to women therefore must not be confused with the issue of maintaining 'decency'. Some scholars have flagged that all controls on representation of women's bodies, including those pertaining to the production and distribution of pornography need to be completely revoked, as a gender-based hate speech law would suffice to address all forms of misogyny and prevent the social policing of women.

---

18 Padte, R.K. (2013), *op.cit.*

19 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." See* http://sflc.in/wp-content/uploads/2012/07/eBook-IT-Rules.pdf

20 Kumari, Ved (1999), Gender analysis of the Indian Penal Code, in Engendering Law: Essays in Honour of Lotika Sakar edited by Amita Dhanda and Archana Parashar. Lucknow: Eastern Book Company

(d) The fact that perpetrators in many instances of techology-mediated violence against women are known to the victim calls for amendments to the Protection of Women from Domestic Violence Act, 2005 to cover instances that occur within marriage.

Option 2. Introducing new legislation that specifically addresses technology-mediated violence

The introduction of new legislation that specifically deals with technology-mediated VAW is guided by the school of thought that online contexts create new structures of communication and social interaction. Therefore, technology-mediated VAW must be understood and interpreted in law and jurisprudence for the specific nature of patriarchal norms and controls arising in and through digital spaces. Interestingly, some scholars have also argued that structures of communication also shift the norms and rules of social behaviour; for instance, digital spaces reduce the threshold for abusive action. Digitally mediated 'speech' and 'action' must therefore be evaluated distinctly and the law has to take a nuanced approach[21]. This option also takes cognizance of the recent indications from the Ministry of Women and Child Development to move forward in the direction of putting in place a new legal framework on VAW, a pragmatic consideration for feminist advocacy. A few months ago, the Ministry made a media announcement that it is deliberating a new code on online trolling. 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[22]".

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 technology-mediated violence against women and explicitly addresses its emerging forms, can be introduced. Some countries such as the Philippines have adopted the route of enacting new laws that specifically focus on certain forms of technology-mediated violence, such as photo and video voyeurism. Others such as New Zealand have approached the issue from the standpoint of "deterring, preventing and mitigating harm caused to individuals by digital communications", by laying down a set of first principles defining acceptable standards for any digital communication[23], which has been critiqued for undermining free speech[24]. It should also be noted that they are gender neutral.

The ten communication principles laid down by New Zealand's Harmful Digital Communications Act 2015, are listed below:

> Principle 1 - A digital communication should not disclose sensitive personal facts about an individual.
>
> Principle 2 - A digital communication should not be threatening, intimidating, or menacing.
>
> Principle 3 - A digital communication should not be grossly offensive to a reasonable person.
>
> Principle 4 - A digital communication should not be indecent or obscene.
>
> Principle 5 - A digital communication should not be used to harass an individual.

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

22 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

23 Government of New Zealand. Harmful Digital Communications Act 2015. Reprint as at 21 November 2016.

24 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

Principle 6 - A digital communication should not make a false allegation.

Principle 7 - A digital communication should not contain a matter that is published in breach of confidence.

Principle 8 - A digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.

Principle 9 - A digital communication should not incite or encourage an individual to commit suicide.

Principle 10 - A digital communication should not denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability."

There are two options, with respect to overhauling the existing legal framework to render it adequate to meet the challenge of technology-mediated VAW.

Option 1. Reform existing legislation, mainly the IPC, to take cognizance of both offline and online forms of abuses (sexually explicit and other sexist forms), against women. This approach must do away with a focus on 'modesty' or 'indecency' / 'obscenity' and center the idea of 'criminal breach of privacy' to tackle abuses (including psychological and emotional) that are against women's bodily integrity (physical privacy); confidentiality (informational privacy) and personal autonomy (decisional privacy).

Option 2. Introduce new legislation to addresses the harm caused by technology-mediated VAW, responding adequately to the communication context of the digital society and the changing nature of patriarchal control and oppression.

3. 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*[25]*".* 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 harbour 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 harbour 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

25 APC (2014), Frequently asked questions on intermediary liability, https://www.apc.org/en/pubs/frequently-asked-questions-internet-intermediary-l

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-harbour approach to intermediary liability, and the safe-harbour 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
- 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 harbour:

> **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 relatable 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 content[26] from an affected person. They should only act upon judicial or executive orders.

On the one hand, 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.

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 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.[27]

---

26 Unlawful content, according to Rule 3(2) of the Information Technology (Intermediaries Guidelines) Rules 2011is 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, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever; (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."

27 Primary field research carried out by IT for Change

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.[28] To operationalise 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.[29] 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 a third approach, of 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.

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.

Whether this is a good route to expediently address technology-mediated VAW 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 functions. Also, as has been highlighted, merely taking down the offending comment may not be a sufficient deterrent against online VAW. The perpetrator can continue the harassment by posting other comments, including through other alternative profiles. Relief can be assured only through suitable judicial orders.[30]

28 http://www.intgovforum.org/cms/2008-igf-hyderabad/event-reports/74-dynamic-coalitions/1625-dynamic-coalition-on-platform-responsibility-dc-pr

29 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

30 Malhotra, N. (2014), op.cit.

Addressing technology-mediated VAW requires a clear policy on the liability of Internet Intermediaries. There is an inherent balancing act in this; that of guaranteeing freedom from violence without privatizing censorship through unaccountable non-state actors. Invariably, women's concerns and experiences are trivialized and ignored by private intermediaries. The very nature of a 'platform society' that we live in results in a proliferation of contestations around speech and representation. Without a legal and institutional mechanism that can provide timely justice, women 's participation in online structures is bound to get constricted, even leading to self-censorship.

4. Enhancing the responsiveness of law enforcement agencies

Law enforcement agencies fail to recognize that online VAW is as grievous as offline VAW.[31] Women's rights groups highlight that despite trainings on gender sensitization, in their response to complaints about technology-mediated VAW, the police engage in victim blaming and/or trivialization of the offence. The establishment of Cyber Cells does not seem to have improved this state of affairs[32]. Feminists have pointed to how consent is a slippery notion; digital technologies have added much complexity to the idea of consent. Law enforcement officials fail to recognize the legitimacy of women's subjective experience of violation, when consent given earlier is subsequently withdrawn[33]. In the 2016 study cited earlier, *Violence Online 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.[34]

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 Ministry of Women and Child Development is also in the process of setting up a portal titled *'Cyber Crime Prevention against Women and Children'* where women who encounter online harassment can file complaints, which will be taken up by the Cyber Cell of the Home Ministry.

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.[35]
(2) Police and Cyber Cell officers who fail to take cognizance of incidents of technology-mediated VAW brought to their notice, must be penalized[36].

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

31 UN Women (2015), *op.cit.*
32 Primary field research carried out by IT for Change
33 Primary field research carried out by IT for Change
34 Pasricha, Japleen (2016),*op.cit.*
35 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/
36 Such action needs to be treated as an offence that is equivalent to the failure to report offences listed under Section 166 A of the India Penal Code and Section 19 and 20 of the Protection of Children from Sexual Offences Act (2012).

exclusively tackle technology-mediated VAW (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 technology-mediated VAW.

Law enforcement processes in respect of technology-mediated VAW invariably fail women. In addition to a training for responding effectively and sensitively to cases of such violations, procedural amendments to challenge the culture of impunity in these agencies are urgently required.

5. Conclusion and questions for discussion

This paper has attempted to draw up the background context and consolidate the debates on technology mediated VAW and the law. Challenging hegemonic cultures of masculinity that endorse men's sense of entitlement over women and the active perpetuation of misogynstic behaviour is a task that certainly goes 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 digitalised society we inhabit. For instance, jurisdictional limits may have to be redefined to account for remote violence that has become commonplace in the seamless fluidity of communication networks. Similarly, culpability needs to be re-imagined in instances of new forms of violence – such as online recirculation of sexually explicit videos and images without consent. We need to ensure that existing legal provisions penalising 'lasciviousness' – which are based on a narrow framework of public morality – do not end up curbing sexual expression. To explain with an example: individuals producing sex tapes for their private consumption and pleasure have found themselves slapped with cases of violating obscenity laws, when they try to challenge the 'leakage' and non-consensual circulation of such videos. Finally, the nitti-gritty of court procedure may need to be re-visited. For example, the production of secondary electronic evidence in courts of law should not be prohibitively difficult for victims of technology-mediated VAW.[37]

Most importantly, the following questions need to be addressed in order to effectively overhaul existing legal frameworks, determine liability of internet intermediaries, and strengthen institutional response mechanisms, including law enforcement.

Area 1. Overhauling existing legal frameworks:-

37 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 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 vs P.K.Basheer* 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 https://indiankanoon.org/doc/187283766/. On an aside, one must remember that just because digital evidence can be produced, it does not mean justice will be served. Digital evidence can be manipulated by the accused to buttress his case(the defense in the landmark Farooqui decision used the time stamp of a call placed and a cab being booked by an App to allege that oral rape could not have taken place in the duration between the two events.- https://kafila.online/2016/08/14/the-mahmood-farooqui-rape-conviction-a-landmark-verdict-j-devika-nivedita-menon/).

1.1. How do we ensure that psychological violence resulting from privacy violations is effectively addressed?

1.2. How can we move from a protectionist framework to one that foregrounds women's right to privacy, comprising of bodily integrity, personal autonomy and informational confidentiality?

Area 2. Intermediary liability

2.1. What responsibilities should we place on Internet intermediaries in terms of responding to instances of technology-mediated VAW?

2.2. What kind of intermediary liability regime will ensure timely justice for women without ushering in a privatized censorship regime?

Area 3. Institutional machinery, including law enforcement

3.1. What kind of procedural changes can improve law enforcement with regard to technology mediated violence?

3.2. Do we need a separate adjudicatory body to deal with technology-mediated VAW? If yes, what would be this body's powers and functions?

Going forward with this task needs an inclusive national dialogue on technology mediated violence, that triggers a series of conversations between women's rights groups, digital rights activists, independent new media organizations, and free speech advocates. In specific, a series of stakeholder consultations needs to be held in different regions of the country, to produce greater visibility for the issue. The agendas/issues identified through such consultations can be taken forward through policy advocacy. In the area of strengthening support services, one major area to explore is the creation of new digital spaces that help individuals affected by technology-mediated VAW to seek and forge support groups, and find information on institutional remedies. More details of these directions are available at the report of the pre-consultation convened by IT for Change, accessible at http://www.itforchange.net/technology-mediated-VAW-India