Born digital, Born free? A socio-legal study on young women's experiences of online violence in South India

Anita Gurumurthy
Amrita Vasudevan
Nandini Chami

IT for Change | 2019

Table of Contents

Acknowledgements

We want to place on record our gratitude to the young women and young men who participated in the survey and the focus group discussions where they shared their experiences and responses to gender-based cyber violence. We would also like to thank the college management and teachers for facilitating this discussion with the students.

The police officials, counsellors and family court lawyers generously gave of their time to provide their critical insights on the issue of gender-based cyberviolence.

We have been humbled by the openness with which women's rights and dalit rights activists, transgender persons and women survivors, shared their perspectives, all of which were woven into the data that helped build the story of the struggles faced due to gender-based cyber violence.

Knowledge building is always a collaborative endeavour. This South India based research would not have been possible without the help of our partners in the two teams: the Kerala team – J. Devika, Chithira Vijayakumar, Darshana Sreedhar Mini, Resmi P.S and Elizabeth Alexander; and the Tamil Nadu team - Geeta Ramaseshan, Sudaroli Ramasamy, M.R.Sangeetha, S.Prabha, Nandita Krishna and Shreeja Kumar.

1. Background to the research

1.1 Introduction

As we enter the twenty-first century, the emancipatory promise of internet-mediated embodiment and the *"cyborgian"*[i] freedom from repressive gender identity that Haraway imagined, remains unfulfilled. Digital reality has no doubt transformed material, corporeal lives in a number of complex ways. Gender regimes are being destabilized through new struggles and movements embracing the fluidity of digitally refigured space. However, hierarchies of gender and identities of race, caste and other locations are far from erased.

It is from this starting point that IT for Change conceptualized and led the research study, "*Righting gender wrongs: A feminist socio-legal enquiry into online sexism, misogyny and gender-based violence in India*" between 2018-19.

Informed insights based on systematic research are not easily available on gender-based cyberviolence in India. This study, located in South India, is an attempt to fill this gap. It uses a posthuman[ii] feminist frame, exploring how gender regimes operate in digitally-mediated social interactions, unravelling the nature of cyberviolence, and evaluating the effectiveness of prevailing legal-institutional response mechanisms.

1.2 Methodology

In conceiving of gender-based violence in cyberspace, a posthuman understanding of the digital context is important and useful to frame both survivor experiences as well as the systemic injustices of such violence. The study thus rejects the notion that cyberspace is a virtual world that is distinct from its real counterpart. As Katherine Hayles points out, conceiving of information or digital artefacts such as data or software code as separate from biological materiality *"could lead to a dangerous split between information and meaning and flattening of the space of theoretical inquiry"*.[iii] As the effects of digital networks and datafication on culture, subjectivity and the body unfold, it is increasingly clear that cyberspace is produced in a mutually constitutive exchange between networked data and the body. The fluid spaces of the digital dissolve the boundaries of our bodies, enhancing and extending them in relation to other bodies.

With a primary focus on the experiences of young adult females and a minor focus on perceptions of young adult males, the study was undertaken in the Southern Indian states of Karnataka, Kerala and Tamil Nadu. These states were selected because of higher rates of internet penetration and higher than average female tertiary educational attainments.[iv] 'Digital fluency' – an important consideration for this inquiry – is proven to be linked to these factors.[v]

The study adopted a mixed methods research approach, comprising the following elements:

(a) A self-administered, anonymized survey with 881 college-going women aged 19-23 years in 6 cities and small towns in Karnataka, Kerala and Tamil Nadu. The survey focused on mapping how information and communication technologies are used by young women; the experiences they have online; if they have faced harassment and how it impacts them; and whether, and from whom, they seek help in such situations.

(b) 14 Focus Group Discussions (FGDs) with young women and young men in colleges across the 6 locations, avoiding overlap with the survey cohort in order to limit privacy risks.

(c) 44 key informant interviews with a range of stakeholders across all 3 states. In-depth, qualitative interviews were carried out with law enforcement officials of varying ranks, family court lawyers, legal researchers on the issue of cyber-violence, women's rights and dalit rights activists, transgender activists, feminist researchers, journalists, counsellors associated with GBV helplines and crisis support centres, and women survivors willing to discuss their struggles for access to justice.

(d) A review of existing literature examining legal, institutional, cultural, and technological dimensions of gender-based cyberviolence. An inter-disciplinary approach was adopted in the literature review by bringing in an eclectic mix of scholarship from cyberfeminism, gender and development, posthumanism, critical media studies, feminist legal studies, surveillance capitalism, and technology and society.

1.3 Research context

Across all 3 states, gender-based cyberviolence has ballooned into a public crisis. In Kerala, gendertrolling by mobs is such a common phenomenon that a local language term *"pongala"* has emerged for it.[vi] In Tamil Nadu, sexist and casteist vitriol against women activists from dalit communities and minority religions has become normalized in social media forums.[vii] In Karnataka, over 60% of complaints lodged at the Karnataka State Women's Commission pertain to harassment of women via social media.[viii]

The specific manifestations of everyday misogyny reflect the gender and socio-political histories of each of these states. Kerala's gender and development attainments stemming from its social transformation in the early 20th century is often celebrated, but this narrative often masks the ways in which the transition to modernity has also enabled the rise of a bourgeoisie patriarchy marked by a deep social conservatism. Women are able to access education and some forms of paid work because of the 'limited forms of agency that are allowed to women' within these re-constituted patriarchal frameworks of caste-community formations.[ix] But this situation also produces deep contradictions, where strongly individuated women are forced to compromise and confine their

energies to the sphere of the domestic. The internet becomes an explosive ingredient in this mix, as it simultaneously creates opportunities for women's subversion and resistance of the status quo, and the mob-led castigation of 'defiant' women.[x]

Tamil Nadu, in the early twentieth century, witnessed the rise of the 'Self-Respect Movement' led by Periyar, a social activist who emphasized the demolition of the caste order and superstitious ritualistic practices, including those that are violative of women's rights.[xi] Unfortunately, as this movement entered the political mainstream, its initial transformative impetus dissipated, without catalyzing long-lasting change for dalit communities and women.[xii] The interrelated project of annihilating caste and overcoming gender subordination seems to have been lost sight of in the selective co-option of the Movement's ideas by political parties. Tamil cinema, an important vehicle for questioning hegemonic Brahminical ideologies in the hey-days of the Self Respect Movement, is today a tool for reinforcement of gender conservatism.[xiii] With a resurgence of casteist patriarchy, 'honour'-based violence and killings[xiv] and regressive gender ideology, Tamil Nadu's young women are today part of what feminist commentators have characterized as "medieval, bizarre and absurd"[xv] college cultures that exercise strict controls on women through gender segregation, dress codes and social media bans. In a state where traditionally, female modesty is valued highly, app cultures are widely perceived as eroding gender conservative social norms.[xvi]

Unlike the other two states, Karnataka did not witness any mass socio-political reform movement in the early to mid-twentieth century. However, to a smaller extent, the state did witness the birth of organizations devoted to social reform of regressive practices, such as the Indian Progressive Union and Civic and Social Activities Association in Mysore. Both these organizations worked towards progressive legislation on issues such as widow remarriage, raising the marriageable age for girls, and advocating for the education of women and girls.[xvii] Alongside such reformist trends, Karnataka also witnessed a gradual unfolding of a revivalist politics romanticizing India's Vedic past. Right-wing fundamentalism took hold in coastal Karnataka, where it continues to be a dominant force.[xviii] Despite the relatively liberal public-political space for women, the spread of right-wing politics in the state has penalized young women who refuse to abide by its vision of the ideal social order. The state has seen a rising spate of violence against women, with political right-wing outfits decrying their 'westernization' or threatening and carrying out missions to 'rescue' Hindu women from Muslim men,[xix] or even, as in the case of Gauri Lankesh, eliminating outspoken women critics in the media.[xx]

Digitally-mediated spaces in each of the contexts of study are shaped by the idiosyncrasies of local history, with specific manifestations of patriarchal social norms. Although this synthesis pulls together the trends to generate the big picture, it also attempts to surface these differences, where possible.

2. Gender-based cyberviolence and shifting gender norms

2.1 Profile of respondents and incidence of cyberviolence

Of the 881 young women surveyed across the three states, 54% were in the age group of 20-21 years. 47% of the students belonged to forward castes, 35% to Other Backward Castes, 11% to Scheduled Castes and 3% to Scheduled Tribes. 68% of the respondents were Hindus, 22% Christian and 7% Muslim. There were also a very small number of Buddhists (6), Jains (4) and Parsis (1). Only 3% of the respondents identified themselves as homosexual; the rest identified as heterosexual. 52% of respondents reported that English was their primary language of communication online. In all three states, the preference for English outweighed that of the state/local language.

Almost all respondents own a phone and use the internet for work and play.

92% of respondents own their own mobile phone, and 52% of this cohort had a phone that was more than 10,000 INR. 42% of this group had replaced their mobile more than once. It may be reasonable therefore to infer that handset cost is a good proxy for socio-economic location. Using this proxy, a significant proportion of respondents can be categorized as hailing from middle or upper income socio-economic backgrounds. Of course, economic status is not necessarily an indicator for liberal or cosmopolitan family antecedents. Communicating with family and friends (93%), completing college work and assignments (84%), and entertainment (70%) seem to be the most prevalent purposes for which respondents use the internet. Only 20% use the internet to forge new friendships and relationships and to expand their social networks in new ways. 8% of respondents reported using the internet to explore their sexuality, and 2% reported sharing intimate images with their partners, but this could be an area of significant under-reporting due to the social stigma associated with discussing the issue. Previous research documenting internet use among young women in the city of Mumbai also noted that very few women reported accessing anything on the internet related to sexuality, with some women even reporting that accessing sexual content is immoral.[xxi]

Across all sites, the most commonly used platform is WhatsApp (Karnataka - 93%, Kerala - 93%, and Tamil Nadu - 92%). Facebook use comparatively lagged behind (Karnataka -54%, Kerala - 60%, and Tamil Nadu - 56%). This is possibly because the design features of WhatsApp are perceived by young women (and their parents and guardians) as safer than that of Facebook where befriending strangers and venturing beyond circumscribed boundaries of socialization is thought to come more easily. In Kerala, women reported that parents and guardians repeatedly warn them that being on social media platforms is akin to *“catching a tiger’s tail”,* a high-risk proposition that is bound to end distastefully. Nevertheless, young women continue to use social media sites to catch up with friends and acquaintances, even if, and as was revealed in FGDs in Kerala, this is in clandestine ways.

Cyberspace is home to pervasive sexism

In Karnataka and Tamil Nadu, young women reported various threats and risks of using Facebook: their profile picture being compromised, their account being hacked into and used to send lewd messages to others in their

circle of acquaintances, and strangers repeatedly sending friend requests. 17 respondents in the sample reported using dating apps, a figure reflective of low use by women of dating platforms in India.[xxii] Even here, there seems to be a threat to privacy and risk of abuse. It was observed that men who are turned down on dating platforms like Tinder shadow women on platforms such as Facebook and harass them with repeated 'friend requests'.

Of the 881 young women who participated in the survey, 37% reported having faced harassment, abuse and unwanted behaviour online, and 39% reported that other women in their family or circle of friends/acquaintances had faced such acts of cyberviolence. 26% of the respondents who had faced cyberviolence reported that the identity of their perpetrators was known to them, whereas 51% reported that the perpetrator was unknown. 16% reported that they had experienced harassment from both known and unknown perpetrators. The most common applications where respondents had faced harassment were Facebook (61%) and WhatsApp (47%). Also, 90% of respondents who had faced harassment reported that they had been harassed on multiple occasions, which indeed, is a matter of grave concern.

The development of typologies to analyze gender-based cyberviolence is not an easy task. The seriousness or impact of violations can often be subjective as victim-survivors may experience different acts of violence and abuse simultaneously. For the purposes of this research, we adopt a two-way schema, broadly dividing experiences of cyberviolence into acts of identity-based trolling/cyberbullying and acts of sexual harassment. Identity-based trolling/bullying (involving demeaning statements or comments) concerns itself with harassment on the basis of physical characteristics (such as weight, body shape, skin colour etc.) or social identity markers (such as caste, sexual orientation, religion, gender etc.). Acts of sexual harassment range from explicit forms of sexual violence (such as circulation of a woman's morphed photo online; sending unsolicited, sexually explicit messages and pictures; non-consensual circulation of intimate images; sextortion etc.) as well as acts that have undertones of sexual violence (such as cyberstalking, doxxing and impersonation of social media profiles). Needless to add, these two categories are not watertight and in the real world, gender-based cyberviolence may well encompass both types of violations. For the purposes of a socio-legal analysis, however, this classificatory schema works out reasonably well. Given that prevailing legal frameworks tend to make a distinction between identity-based trolling/bullying and sexualized crimes, designing the inquiry in this direction provides a useful point of departure for a critical stocktaking of the categories themselves.

2.2 Identity-based trolling

Irrespective of social location, women face demeaning commentary about their physical bodily attributes. In social media culture, sexual subjectification is the new objectification.

Of the 326 respondents who reported facing cyberviolence, 76% had faced trolling on the basis of their physical characteristics or social identity (83% in Kerala, 74% in Karnataka and 70% in Tamil Nadu).

Bullying based on physical attributes emerges as a common form of violation experienced by young women. 31% of respondents who have faced cyberviolence reported being bullied about their body shape; 30%, their weight; 27%, their looks; and 22%, their skin colour.

Visual communication cultures ushered in by social media and social networking platforms are birthing a regime of mandatory sexual subjectification through their very architectures. Women are coerced to present the best physical version of themselves moulded on a male gaze.[xxiii] Online dating platforms reinforce these ideals in people by placing the image front and centre, with rejection just a swipe away.[xxiv] Platforms such as Instagram generate a perpetual stream of "evaluative photo commentary"[xxv] that reinforces the feedback loop between affirmation of physical appearance and self-worth, for young women and girls.

Research on body shaming points to how, given the proclivities of these platforms for projecting and comparing one's appearance, women and girls begin to engage in self-surveillance, trying to meet tacit standards of desirability. Perpetrators of cyberbullying are also egged-on by popular following for public displays of violence, taking advantage of platform affordances such as 'likes' and 'shares'.[xxvi]

Under pressure to represent themselves as desirable in emerging image-centred cultures, young women often face a tough dilemma. Posting selfies is a rite of passage, but it is also often followed by backlash in the form of sexist and misogynistic comments that punish women for daring to be visible.

Women from marginal social locations face particularly heinous forms of gendertrolling that denigrate their social identity. Misogynistic vitriol faced by dalit women is also casteist.

Trolling about social location was reported by a smaller percentage of respondents compared to trolling based on physical attributes – with 9% reporting that they were attacked on the basis of their caste; 4%, their community; and 4%, their religion.

Notably, while disparaging comments about bodily characteristics were faced by women from all social identities, caste-based markers were mainly invoked in gendertrolling of dalit women. 14% of respondents from dalit communities reported facing caste-based harassment as against 4% of respondents from 'forward' castes.

Qualitative aspects of our study show how women from dalit communities face malicious attacks about their physical appearance that devalue their bodies. A woman dalit rights activist interviewed in Karnataka recounted her friend's experience:

> Immediately after [my friend] posted comments critical of the #MeToo movement in India, two-three men started piling on, saying things like, "Look at your face; you're so disgusting. Nobody wants you,

> You're a *kalmuhi*" [a caste slur that is colloquially used to mean bad luck], and, "You're so disgusting, nobody would even think of raping you; why are you thinking about #MeToo?"
>
> - Female dalit rights activist, Karnataka

Transpeople online are subjected to invasive de-humanizing questions and comments about their bodies through social media. This can be extremely troubling for LGBTQI activists, especially because many people reach out through social media for help and advice.[xxvii] For transwomen in Kerala, despite all the attacks, social media is still a very valuable space for self-crafting and staying safe:[xxviii]

> You cannot imagine how important WhatsApp groups are for our safety. In a city like Kochi where the police are hostile and we are often attacked even if we aren't doing sex work, WhatsApp group allows us to gather quickly to aid a sister who's being attacked.
>
> Transwoman, key informant, Kerala

Other research also suggests that individuals who identify as non-heteronormative report higher incidents of cyber-bullying, with non-heterosexual women being especially vulnerable.[xxix] Seeking help in cases of homophobic bullying is especially difficult because it could entail sanctions from authority figures.

The sheer volume of sexist and misogynistic content available online suggests that gendertrolling is ignored and trivialized[xxx] just as sexist street harassment is considered 'routine'; women are goaded to 'make some adjustments, accept reality and move on'.[xxxi]

2.3 Sexual harassment

Sexual harassment of women is ubiquitous online. Digital interaction normalizes sexualized assertions of male power over women's bodies.

Of the 326 respondents who had faced cyberviolence, 83% had faced sexual harassment of some form. The most commonly reported forms of sexual harassment were cyberstalking/being contacted repeatedly by the same person demanding a sexual relationship (44%), followed by doxxing/instances of personal information being leaked online or fake profiles being created (39%) and sexually explicit images/photos being shared with an individual without her consent (30%).

Cyberstalking seems to be distressingly ubiquitous. A survey respondent in Karnataka [answering an open question] wrote about how her harasser would relentlessly message her through the night, stalk her profile from

unknown handles and try to initiate sexual conversations with her. Another discussed how despite blocking their numbers, unknown persons continued to repeatedly send her unwanted messages. The internet, by rendering spatial constraints redundant and enabling individuals to cloak themselves in anonymity, has unfortunately opened up a 'favourable environment for stalking'.[xxxii]

A young student activist in Kerala reflected:

> I had a friend who was "practising to be a 'kulasthree" (a good girl). She wore a saree, had flowers in her hair, etc. But one day, some guy took photos of her just going about her day and then sent her a message saying 'You are the ideal Malayalee woman. I will always be behind you to capture your beauty." Finished! She had been a confident person till then. She was traumatized. She couldn't even step out of the house without her parents. The threat is very real. Doesn't have to be nude pics! Imagine feeling like there's someone constantly behind you.
>
> Student activist, key informant, Kerala

Not all acts of stalking are perpetrated by strangers. Oftentimes, stalkers are likely to have been former partners/friends/acquaintances with whom the victim has cut ties. A young woman who was part of the FGD in Tamil Nadu shared how after she turned down her male friend's proposal for a romantic relationship, he started using vulgar language on chats. One of the researchers in the project had shared her phone number with a male college student from the FGD, only to stalked and assaulted with persistent calls and unwanted messages. Male entitlement that underpins stalking was more than evident in the FGDs with young men:

> Not accepting a friend request is arrogance. If at all a woman wants to reject it, she should explain why.
>
> – Participant, FGD with young men, Tamil Nadu

Doxxing usually takes the form of fake profiles of women created by perpetrators who intend to cause distress to their victims by channelling unwanted attention towards them. During the key informant interviews carried out in Kerala, a well-known student activist who has a huge online following recalled how an image of her in a well-fitting shirt was posted by unknown perpetrators on a semi-pornographic site. In Tamil Nadu as well, participants of FGDs reported instances of Facebook profiles being hacked and used by harassers to send unwanted messages. Sometimes, acts of doxxing also involve a threat to release a woman's photo morphed with another pornographic image.

Sending women unsolicited 'dick pics' or cyberflashing has become so widespread that women have started groups on Snapchat, Instagram etc. to share experiences and discuss how they have dealt with the issue. The

impulse to send such pictures has been attributed to coerced reciprocity (women owe men an image in return), arousal from the shock value behind such acts, and the acceleration of intimacy that digital space brings about.[xxxiii] Male power and privilege manifest online through a routinization of such sexualized assertions over women. In Karnataka, a survey respondent wrote:

> During the initial stages when I joined Facebook, I used to receive a lot of messages from people and I didn't know. The language and content of those messages were not appropriate, and they made me feel angry and afraid and uncomfortable. The guy was a stranger online and after i just asked him how do you know me, he sent the picture of his dick trying to be proud of his senseless action.
>
> Survey respondent, Karnataka

In the face of sexualized assertions of male power over their body and autonomy, women believe that digital intimacies need to be managed through self-policing.

Violations of a sexual nature, such as non-consensual circulation of intimate images, sextortion, and other forms that involved admission of their sexual history were reported by a small number of women. A higher proportion of survey respondents reported that such violence had been experienced by other women in their family, their friends and circle of acquaintances. Only 3 respondents noted that a sexually explicit image or video of them from a past relationship was put online without their consent, whereas 38 respondents reported being aware of someone else it had happened to. Similarly, only 7 respondents reported being subject to morphing, but 62 knew of someone else it had happened to. And while only 14 respondents admitted to receiving messages blackmailing them into sex on the threat of leaking their intimate picture online, 49 knew of some other woman it had happened to.

The dissonance between the two sets of responses may be attributed to a reluctance to talk about personal sexual experience. The stigma attached to sexual violations and the shifting of blame onto the survivor, especially if the perpetrator is an intimate partner, is partly at play here. The patriarchal prerogative to 'teach a lesson' to women who violate codes of sexual behaviour was seen as normal or inevitable, even by young women themselves. As part of the survey, when respondents were presented with a hypothetical situation where an ex-boyfriend uploads naked pictures of his ex-girlfriend after their breakup, 38% of respondents said that the woman was to blame. In the voices of female survey respondents in Karnataka:

> She should have never sent nude pictures because they can be used as blackmail her once they break up.

> I can't really say that somebody is at fault, but all girls should know their limits in using technology and should understand all cyber threats.
>
> Female survey respondents, Karnataka

Interestingly, when responding to another hypothetical situation where a female student is running a YouTube channel about gender and caste issues and faces a barrage of threats of violence from detractors, 74% of the respondents who had blamed the woman in the earlier case of the leak of naked pictures responded in defense of the channel owner, upholding her right to free expression .

What this suggests is that even as young women are convinced about a woman's right to be present and participate in the digitally-mediated public sphere and express themselves, they have also internalized the notion that to stay online and claim a space for individuation beyond the confines of the domestic, they must manage their voice and visibility responsibly, *"avoiding uses that may make one socially vulnerable in ways that destroy this prospect".*[xxxiv]

Another striking trend was that the proportion of respondents who blamed the woman for the leak of intimate images in response to the hypothetical situation was much higher in Tamil Nadu (63%) when compared to Kerala (28%) and Karnataka (25%). This may be a reflection of the larger reality of repressive gender conservatism rampant in higher education institutions in Tamil Nadu,[xxxv] with social interactions between young men and young women strictly delimited and monitored, and women students forbidden from even setting up social media profiles by the college administration.[xxxvi] Self-policing tends to be an inevitable consequence of patriarchal standards of female modesty.

Toxic male disinhibition in digital spaces naturalizes male transgressions of women's autonomy and privacy.

The phenomenon of non-consensual circulation of intimate images reveals emerging cultures of digital intimacy where the everyday lives of young women and men are "caught between the poles of the precious disinhibition that women seek online and the toxic disinhibition that men display in virtual spaces".[xxxvii] "*Online disinhibition*", as Suler theorizes, is caused by affordances of digital space, including disassociative anonymity, invisibility and asynchronicity.[xxxviii] In its benign form, disinhibition can lead to greater self-exploration and identity building. But at the same time, the absence of visual social cues in digital communication culture can create a lack of empathy, lowering the already low threshold for gender-based abuse, resulting in toxic disinhibition.

When the same hypothetical situation of the 'leaked pictures' was presented before young men as part of a FGD in Karnataka, one of the young men shared his view that the woman victim had actually got her just deserts:

> If she was committed enough to send her nude pictures, how could she break up with him? By leaving her boyfriend, she was cheating on him, and of course, he leaked the picture.
>
> Male participant, FGD, Karnataka

Similarly, in Kerala, a male participant in a focus group reflected on the reactions of his peers in a male-only WhatsApp group to a popular movie dealing with the subject of non-consensual circulation of intimate images in which the female victim commits suicide. He shared that while some friends were willing to be reflective, most members in the group shrugged it off, saying, "*no woman is going to jump from the top of a building just because of a video of her in a bathroom*".[xxxix]

Women in public life are seen as easy game, to be pushed back and punished with malicious and sexualized attacks.

Although the survey did not probe into respondents' public-political life, insights from qualitative inquiry show how women who are active in the public domain are subject to mass attacks by cybertrolls and often silenced through sexualized attacks. Digital spaces are no doubt opening up opportunities for women's voice and political expression, but women seeking to find a public-political identity through social media find it an uphill climb. A senior lawyer from Kerala supporting survivors criticized the widespread belief that cybertrolls are innocuous,"*just about boys out for some fun*".[xl]

> I can say that this is a form of *adicchiruthal* ['forcing to sit down']. That is, a mass booing, that would force the woman to shut up and back off...I think (going online) has spurred women's ability to argue, to use strong words, and especially to use humour! This is provoking a lot of male insecurity... something like an uncontrollable desire to punish... So you go back again and again, get your friends to join, and keep increasing the intensity of the attack till you are satisfied, till you feel the woman has been effectively silenced! That is perhaps why these men, young and old, are so intensely violent, so unashamed of using all kinds of tactics, below-the-belt blows, when a woman is at the centre.
>
> Senior lawyer, key informant, Kerala

Female journalists often face sexualized defamation campaigns, with their public feminine body conflated narrowly with pornography in contrast to the range of meanings that can append to the public masculine body.[xli] Horrific images of women public figures are shared and defended in the name of 'controversial humour' that is deserving of free speech protections.

The sexualization of women's bodies in public life is also used as a political tactic to shame and intimidate their male partners. In Kerala, one of the survivors interviewed for the research, an upper-caste woman in public life married to a lower-caste political leader, found herself the target of cyber-attacks when WhatsApp messages

calling her a prostitute along with morphed images began to circulate in the political constituency he worked in. She recounted her experience thus:

> My partner is a lower caste, working class man. He rose from there. I, however, come from a very comfortable middle class family... (When my morphed pictures appeared on WhatsApp), he was totally unfazed of course, but I did feel terrible for him – that he should face such hurdles in politics just because he married a woman who has a public face, and therefore can be so easily derided."
>
> Woman in public life, key informant, Kerala

The structures of digital space present a paradox for women; they liberate female and male sexual agency, but they also imbibe and perpetuate the domination of male sexual desire, lowering thresholds of sexualized attacks on women and normalizing them as routine expressions of male power and privilege. Intimacies are caught in this space-and-body configuration, forcing women to come to terms with a 'private' that can easily be breached. Patriarchy in cyberspace is also highly intolerant of women who are articulate and political, punishing them publicly and viciously.

2.4 Impacts of violence and coping mechanisms of respondents

Consequences of cyberviolence are very real – ranging from physical, psychological to social, functional and aspirational impacts.

29% of the 326 respondents who faced cyberviolence reported that they continue to feel scared for their safety; 28% felt anxious or depressed; and 11% reported being besieged by a sense of helplessness. In fact, 6% reported to have attempted some form of self-harm. Victims also experienced disruptions to their everyday functioning and routines. 30% of respondents who faced cyberviolence reported that the incident had affected their academic performance at some point.

In Kerala, a lawyer who was a key informant reported how doxxing had affected the professional lives of two of her women clients. Jealous male colleagues had targeted the two women, creating fake profiles of them on matrimonial sites and linking this to their official email IDs. As a result of this, the women were flooded with unwanted emails. This had severe repercussions on their work.[xlii]

As the Special Rapporteur on Violence Against Women has noted, the harms of gender-based cyberviolence may be psychological, physical, sexual, and economic.[xliii] The humiliation of being publicly shamed can result in depression, anxiety and in extreme cases, self harm.[xliv] Women have also reported being fired from their jobs as a result of image-based sexual harassment.[xlv] Being monitored online can cause a paralyzing fear and panic.[xlvi]

There are also times when women are physically attacked as a consequence of the online violence they have faced.[xlvii]

Most damning of all is the chilling effect that acts of cyberviolence have on women's self-expression and efforts to carve out a public identity in digital spaces. After being attacked, 39% of respondents who had faced cyberviolence reported having reduced use of their mobile phone and laptop, 38% deleted their social media accounts, and 26% reported that they continued to feel scared to post or share content online. When asked if knowing about other women facing harassment online affected them, 57% answered that they have become cautious of posting content on their social media, 20% that they have reduced their use of the internet and 15% reported having deleted their social media accounts. Other studies also testify to the fact that survivors of online violence tend to resign themselves to self-censorship.[xlviii]

One of the coping strategies that women active in public-political life exercise under these circumstances is to tailor their online personas. Key informant interviews with women journalists revealed that consequent to experiences of cyberattacks they have had to carefully manage their private and public identities, sometimes using multiple social media profiles – a closed profile to share details of their personal lives, and a public one that is more impersonal and also updated less regularly.

For young women who are still exploring digital space for a public-political identity, and not yet fully assertive online, the effects of cyberviolence are far more chilling. The response seems to be one of re-alignment of public participation, a state of withdrawal and quiescence, as suggested by the following response from a female participant in an FGD in Karnataka:

> I am not that active on social media anymore; I don't post my personal opinions because I see there's a lot of conflict that comes out of this. I would like to choose a platform where I could speak up from place to place [a physical platform] rather than to post on social media.
>
> Female participant of FGD, Karnataka

Rather than come out and seek support, women may simply adjust to cultures of cyberviolence, in order to preserve their space of agency. The family is an important source of support, even though young women fear parental disapproval and a resultant loss of access to digital spaces.

Quitting the web altogether is not realistic and may entail huge social, economic and personal costs for women. Consequently, women adjust to unrewarding and penalizing aspects of their digital lives, fashioning their presence and participation to preclude the possibility of censure or violence.

The importance of continuing to remain online is testified by the reluctance of victims to seek help from family for fear of their access being cut off. 54% of respondents who had faced cyberviolence reported that they would not seek help from parents or relatives. Nearly half of this number reported that this was because they were worried their mobile phone/laptop/gadget may be confiscated. In the FGD with young women in Tamil Nadu, participants reported that they only confide in their close friends, as family members might stop them from using smartphones in the future.

The lack of understanding and empathy among family members was another barrier reported by survey respondents. As a psychiatric counsellor, who works with adolescents and young adults facing violence in Karnataka, put it:

> Parents are in most cases the last resort, because students are obviously afraid of facing the wrath of their family.
>
> Counsellor, Key informant, Karnataka

Yet, the family may also be an important source of support. 47% of the respondents did report telling their parents, siblings and other relatives about their experience. In the larger scheme of things, this implies that effective support for the victim-survivor may be contingent on how equipped the family is to address her well-being. As was acknowledged by the counsellor herself:

> It is very difficult to get the students to admit the problem on their own and for them to voluntarily approach a psychiatrist to help them get through the problem. Parents need to provide the right kind of support at the right time.
>
> Counsellor, Key informant, Karnataka

The research revealed instances of women using humour and satire, and also building a peer networks of support to take collective actions. In one incident shared by research participants in Kerala, a few women students in a hostel whose pictures were being uploaded online with obscene comments decided to complain jointly to the cyberpolice.

> Because we complained as a group, the police did not try to inform our parents – if they had done that, many of us would have had to back out. And since we were like eight girls, with more saying that they too suffered but didn't want to formally complain, we were taken seriously.

– Participant, FGD with young women, Kerala

Acknowledging such instances of women responding to violence with agency is vital. However, a conversation on revamping institutional systems is also necessary for a systemic response that does not transfer the burden to address a deeply pervasive societal problem on survivors.

2.5 Re-socialization of gender power

Male anxiety about female agency leads to continuous social surveillance and household monitoring of women by their men. In homosocial, male-only spaces online, the born-digital generation of young men cultivate their manhood, trivializing women's sexuality and celebrating masculine virility.

The contemporary digital context is marked by a new point of departure for gendered surveillance. Data-based integration of information has seen interconnected assemblages involving state, corporate, community and familial actors policing women's mobility, sexuality, reproductive health and more. Affordances of user tracking and hyper profiling used for commercial dataveillance also facilitate abusive husbands to surveil wives and the state to persecute LGBTQ groups.[xlix]

Similar to other studies in India[l], this research also found numerous instances of household-level monitoring and surveillance of young women's use of digital technologies. In Tamil Nadu, young women reported in FGDs that they were not allowed to have their own smartphones, and had to use their brother's phone when they went online. In Kerala, the research found instances of young women having to share access to their social media accounts/passwords with male family members. Men – brothers and elders – are anxious about their women exercising agency, especially sexual agency.

A woman's desire to be seen online is interpreted as 'immodest' and deserving of humiliation, as revealed by perspectives shared by young men in the FGDs:

> But girls also should keep their accounts private and within their friends' circle. They should be more careful. If they are concerned, why aren't they more careful? There are a lot of ways to do this now. You can share things with only a group of friends. But girls want likes and fame. That may be a problem.
>
> - Participant, FGD with young men, Karnataka

Such vitriol may be accentuated if women's self-expression through selfies or videos is perceived as 'crossing the line'.[li] Reprisal for sexual agency is likely to be immediate and seen as an inevitable consequence, as revealed in the words of a young male student:

> Girls should dress properly when they post music videos on TikTok. If they don't, they should not complain about any misogynist counter-video posted to tease them.
>
> - Participant, FGD with young men, Tamil Nadu

Some young women were quite accepting of this, and in fact, one participant said:

> This is just like a joint account in a bank, Madam, so that we don't make bad mistakes.
>
> Female participant, FGD, Kerala

In addition to surveillance by male relatives, monitoring by romantic partners is also common. One respondent from Kerala shared:

> My boyfriend saw a pic of mine, where I am sitting with one leg on the other. He told me I should not pose for pics like that. Put both feet on the floor, he said.
>
> Female participant from FGD, Kerala

Such policing by family members, kinship networks and romantic partners is typical of 'honour cultures'.[lii] Brothers especially, often fashion themselves as protectors of their sisters, guarding their mobility for the sake of dignity and family honour.[liii] These self-appointed protectors can, and do abuse their position. A cyberactivist interviewed for the research in Kerala shared a case where a young teenager was blackmailed and forced by her cousin to have sex with strangers. He threatened to expose her secret outing with college friends by releazing photos that could get her into trouble with her family.[liv]

Social surveillance also manifests in grouptrolling. While cybermobs may be uncoordinated attacks by multiple men across places, quite paradoxically, a digitally networked environment also encompasses inscrutable, hyper-local fraternities for the conduct of manhood;[lv] all-male 'bro-clubs' in which *"homosocial space, collective action, and gender identity intersect to reify power hierarchies."*[lvi]

Young male students in Kerala told researchers about local young men's WhatsApp groups named after particular places – Kattancherry boys, Kaverinagar boys etc. (names changed). In these homosocial private male spaces, men build a new-age machismo, getting fluent with expletives, making sexualised memes to assert male entitlement, 'hooking' women or chatting them up using fake profiles, and watching porn. Usually, the smokescreen of humour is employed to trivialize these acts. As performative spaces for cultivating masculinity,

such groups collaboratively keep their members in check by maintaining a standard of masculinity that involves collectively celebrating male virility.

Male-only WhatsApp groups of colleagues, neighbours and friends are a common phenomenon across the 3 states. Young men in the FGD in Tamil Nadu remarked that if a sexist meme is posted on their wall, "S*ome of us just reply with a smiley; a few of us might even leave a comment saying 'fact', as a way of agreeing with the joke or meme"*. Others felt that *"Girls should cover whatever is needed to be covered. If it is open, anybody will encroach upon.* (sic)*".*

Taking a defiantly post-feminist stance on sharing misogynistic jokes, one of the young men from the FGD in Karnataka said:

> Take, for example, if I mock at or make sarcastic jokes about my friend. If it is a boy, then it is okay, but the moment I tell it to a woman, they say you are abusing her, you are dominating her. What is there to dominate in sarcasm? Women's empowerment means equality. Men and women should be equal. If I can make a sexually coloured joke about my male friend, I should be able to do that to a female friend as well. Otherwise it is unfair… hypocritical.
>
> Male participant, FGD, Karnataka

Masculinities determine relationships between men and women as well as between men and men. Those who do not live up to the hegemonic standards are deemed inferior and effeminate. Men who do object to sexist content being shared on their groups are quickly shut up for being killjoys.[lvii]

Born-digital women self-fashion their digital visibility and presence, constantly exploring survival tactics to somehow stay online. Aspiring to self-build and self-explore in the 'free' spaces of the digital, they reconcile themselves to its disempowering gender norms,

Circumventing restrictive social surveillance nets is made possible only by maintaining boundaries between the world of the familial-domestic and the private-individual. This is very difficult on social networking and social media platforms whose very design is focused on enabling public exhibition of private relationships. Facebook for instance, allows other people to tag you in pictures without your approval, and so, alternate profiles can be outed.[lviii]

But, somehow, women navigate the surveillance minefield, calculating when the risk is too high and rewards too low. One FGD participant from Kerala told us how it is vital to steer clear of family in building online networks:

> My advice to all the women freshers who migrate from their home town for their studies is 'Don't add people from your native place on your social media'. They are the worst harassers and many of them threaten to make obscene images of us and show it to our families.

Women may also choose to not be on social media altogether, temporarily suspend their accounts, obscure their real identities, or carry out careful self-censorship to appear modest and 'chaste'. A study on image-based representation on Facebook observes how impression management for young Muslim women in India requires curbing any projection of sexuality. Women in the study, learned to fine tune their identity online through experience. If a picture gets a stray comment calling them sexy, then women know not to post similar pictures in the future.[lix] Selfies in a sleeveless top, reflected a young woman from Kerala, are deemed 'modern and forward' and are sure to elicit unwelcome remarks from strangers. The *"Cinderella approach"*, as another FGD participant from Kerala innovatively termed it, is used to slowly cultivate a 'good girl' image and survive online "*using the language and expectations of patriarchal logic to further ones interests*".[lx]

So, what does this add up to for women's self building, especially the born-digital generation whose identities are technologically mediated,[lxi] and who are inheriting a world that is wired patriarchal?

Misogyny online is perceived as quotidian. *"Laugh it off and move on",* said the young women participants of the FGDs, when probed about how they deal with sexist memes and jokes shared by their male classmates.

Across the focus groups, the research found women cautioning each other about sharing intimate pictures. One FGD participant in Karnataka, in fact, said that if any of her friends came to her with such a problem, she would tell her point blank, '*You should have known better than to do it. What were you thinking? Were you in your right mind to send those pictures?' Especially in this age of technology?*" Such fears were clearly not unfounded, with many of women familiar with cases of friends, sisters and cousins whose pictures had leaked online, only for the victims to be blamed by their parents.

Despite the violence they suffer, young women see the digital as an essential part of their social lives and identity. Beholden to its free spaces, they accommodate rather than resist patriarchy, avoid rather than confront misogyny, and assimilate rather than disrupt gender norms.[lxii] Women also police other women. As Kabeer elaborates, the acceptance of violence may look like agency from afar, but is in actuality *"really the denial of agency".*[lxiii]

Reclaiming agency in digital spaces where the odds are stacked against them is possible only for the young women who have a wider network of support and a peer network that enables them to challenge the normalization of sexism and misogyny. But this may be a tall order. As one survivor, sharing her experience of lack of support from the online community, observed:

> But I did feel that my friends in the xxx movement (real name suppressed) online – most of them I know through FB – were not supportive enough … but then that's probably because one doesn't really know them, they are only Facebook friends.
>
> Survivor, key informant, Kerala

The case for feminist counterpublics cannot be overemphasized if we seek transformative change. However, the potential for communities of affinity and choice, trust and solidarity are as contingent in the digital context as they have been historically. The ease of mobilization may not necessarily make building democracy any smoother. Not all women have equal access to these communities, and many a time, these spaces may also replicate hegemonic homo-social cultures, as has been pointed out by dalit feminists about the feminist movement in general.[lxiv] Not to forget, such communities also gain only limited traction, curtailed by contemporary structures of cultural (re)production.[lxv] In this context, effective institutional redress becomes an important first step in the fight against gender-based cyberviolence.

3. Women's experiences of seeking redress for gender-based cyberviolence

3.1 Internal college committees to address sexual harassment

Although mandated by the law, internal committees on sexual harassment in colleges are mostly non-existent or where present, dysfunctional and ill-prepared. Hostile college authorities intimidate students, preventing them from bringing up complaints, whilst students who do step up may easily be victim-blamed.

Of the 326 respondents who had faced gender-based cyberviolence, very few individuals sought redress from formal institutional mechanisms. Only 13% approached college authorities. The main reasons cited for not approaching the college were: lack of awareness that the college had the authority to intervene in these issues (19%) and anxiety about unsympathetic responses from the management and teachers (14%). Only 26% of the 881 survey respondents were aware of the existence and functioning of an internal committee on sexual harassment in their college. Even in colleges that are considered 'progressive and liberal', students are not provided with information about the issue and how they can seek redress.

FGDs with young women in Karnataka and Tamil Nadu revealed a lack of trust in the ability of college authorities to respond in discreet, sensitive and empathetic ways without engaging in victim-blaming. In Tamil Nadu, one young woman participant in the FGD even shared an instance where her friend who was a victim of cyberviolence had been issued a transfer certificate and asked to leave the institution, when she complained.

In Kerala, it was found that internal committees on sexual harassment, even though mandatory under University Grants Commission (UGC) guidelines, are non-existent or non-functional even in major colleges, and in the few institutions they exist, members do not receive adequate training on cyberviolence. Some colleges have also issued circulars banning their students from using mobile phones. In these environments, women victims cannot complain for fear of ensuing disciplinary action for violating the rule book.

In situations where teachers held staunch feminist stances, internal committees on sexual harassment were able to be effectively activated. A woman lawyer from Kerala interviewed for this research shared one such instance:

> … the ICC found him guilty and the college authorities took prompt action, first suspending him and forbidding him to enter campus, and after the ICC report, recommending his dismissal to higher authorities. He's gone to court, but it is doubtful if he will win. In this case, the strong presence of feminist teachers on campus was an important factor. Most departments there, especially the arts and social science departments, have at least one young feminist teacher educated outside Kerala – with good PhDs – and some male feminist teachers too who are quite vocal. This is a campus that managed to organize a queer parade last year with teachers and students participating. But, of course, this is an exception, and in private management colleges, there are often equally well-trained feminist teachers, male and female (more and more the case, because young people joining there are from politicized universities outside Kerala and young men are often refreshingly free of the blatant misogyny of men trained in Kerala), who cannot take a strong stand."
>
> Female lawyer, key informant, Kerala

3.2 Response of law enforcement agencies

Law enforcement agencies tend to adopt a protectionist approach at best and a victim-blaming judgementalism at worst. Fear of police insensitivity was a significant reason for not seeking their help.

Of the 326 respondents who faced cyberviolence, a mere 10% sought assistance from the police. The most common reasons cited for not approaching the police were as follows: lack of awareness that cyberviolence was a crime (46%), lack of comfort about entering a police station (40%), and anxiety that police would trivialize their complaint (33%) or handle the complaints without sensitivity (41%). This reluctance is understandable considering the cultural stigma associated with getting embroiled in 'police cases'.

The deep-rooted patriarchal cultures within institutions of law enforcement that manifest either as unfriendliness or as patronizing protectionism is, of course, another long-standing challenge. This research also found evidence of these cultures spilling over and shaping law enforcement responses to cyberviolence. In Kerala, the police officers interviewed were keen to express their sympathy with victims but in a patriarchal-protectionist way, that

is, more keen to be sympathetic to women who fit the 'good victim' profile, such as teenagers and young women who look unexposed to the world; more responsive to cases where family reputation seemed at stake; and judgmental about cases of gendertrolling against victims who had an active public-political life.[lxvi] The advisories that the Kerala Police have been sharing on safe online behaviour reflect these attitudes,[lxvii] underscoring as they do:

> "*(a) the reduction of internet use and access to it among students, (b) greater surveillance by parents and others of internet use by students, (c) special restrictions for girls, such as avoidance of selfies with boys and uploading their images on Facebook and WhatsApp, as well as the promotion of greater awareness of sexual touch among them, and (d) the strengthening of family communication."*

In Tamil Nadu, in 2018, the police issued advisories to schools and parents asking them to guard against their wards logging onto Tiktok, after the Chennai police busted a racket that had been morphing photos of women downloaded from the app. This has been followed by extensive moral panic and outrage in public discourse about the use of the app, prompting the police to issue a ban that was subsequently struck down.[lxviii]

In Karnataka, a survivor interviewed for the research reported how when she took complaints of gendertrolling to the police, she was met with a thinly-veiled 'you were asking for it' jibe:

> The police told me, "If you don't provoke them, they won't say things like this." And, this was in spite of threats I was getting of rape, acid attack etc.
>
> Female survivor, key informant, Karnataka

Similarly, a lawyer in Karnataka, interviewed for the research, highlighted how for those who face violence in same-sex relationships, especially on dating sites or applications, reaching out to the police would mean outing oneself and risking stigmatization. This, despite the recent Supreme Court decision decriminalizing homosexuality in India.[lxix]

Increasing incidence and capacity-building efforts have contributed to greater awareness amongst law enforcement agencies about pertinent sections of the law in cases of gender-based cyberviolence. Given limitations of resources and the tedious pursuit of digital evidence, the police however tend to deprioritize such cases, trading off investigations in cyberviolence for 'more serious' cybercrimes, like cyberterrorism.

In all 3 states, the research found a high degree of awareness about cyberviolence among the police personnel interviewed, including a recognition that legal provisions in the IPC and the IT Act covered such offences. In the case of Tamil Nadu, the police reported invoking relevant provisions of the Tamil Nadu Prohibition of Women Harassment Act, 1998,which is a state statute.

In Karnataka, considerable progress is noticeable in the past two years. In 2017, when IT for Change conducted a study of perceptions of gender-based cyberviolence among police officials in Bengaluru,[lxx] some officers claimed that women were being victimized because *"they were not exercising common sense".* There were others who expressed the view that "*since the body is not implicated"* in cases of cyberviolence, the IPC, the provisions of which mostly deal with crimes against the body, cannot be applied. In stark contrast, this time round, most of the police officers interviewed demonstrated a better grasp of gender-based cyberviolence, and acknowledged these acts as crimes, seeing room for using the IPC in charging perpetrators. In Tamil Nadu, the research team noted how the officers of the cyber cell are aware of the widespread prevalence of cyberviolence and the need to respond to the same.[lxxi]

Partly, this shift in police perceptions about cyberviolence may be attributable to increased incidence and media attention. The interviews with key informants from the police did suggest that most officials feel that more women have been coming forward to file cases. Unfortunately, there is no way to do an objective trend analysis, as gender-based cyberviolence is not considered a separate category of crime in the prevailing records and documentation system of the National Crime Records Bureau (NCRB). Currently, cyberviolence cases are not separated from other cybercrimes, with the result that neither the NRCB nor individual police stations are in a position to track cases.

Another reason for increased awareness among law enforcement officials about the application of specific legal provisions in cases of cyberviolence may be recent capacity-building initiatives set up by the government. The Cybercrime Prevention Against Women and Girls Scheme set up in late 2017[lxxii] aims to train 27,500 police officers, public prosecutors and judicial officers in cybercrime awareness and 13,500 officials in cybercrime investigation over the next two years, through National/State/UT police academies/institutes. It also sets minimum targets for the training of women officers and recommends that as many women officers as possible need to be trained. Under this programme, over the next two years Karnataka state has set a target for itself to train 90 women in law enforcement agencies, including 20 women Station House Officers.

In Kerala, the state police have launched an ambitious training programme to equip at least two or three officers in every police station to handle cybercrime, and women officers are being trained to counsel women. In November 2018, the Kerala Police Training College organized a training programme on handling cybercrime for 550 women officers and 500 male officers from across different parts of the state.

Despite the capacity-building efforts, police officials often struggle with prioritizing cybercrime complaints as they are already overburdened. In the larger scheme of things, these cases do not seem *"serious enough"* when compared to the *"big burden that [the police] already carry"*.[lxxiii]

In Kerala, police officials feel that since victims often tend to withdraw complaints, and their families may be reluctant to pursue the case and cooperate in the investigation, law enforcement efforts are frustrated and their energies frittered. In Karnataka, a police official pointed out that because marshalling digital evidence for cybercrime often demands tedious co-ordination through MLATS/ Letters Rogatory, preference in cybercrime investigation is often given to what are *"more serious cases, like terrorism".*[lxxiv].

In Tamil Nadu too, evidence of such deprioritization emerged. As the researchers observed: *"Cyber crimes are treated less seriously than regular offences. Even in the case of offences against journalists, directions had to be obtained from the court for registering a case."*[lxxv] It was also noted that in order to manage their workload, the police have introduced a two-step process when addressing complaints of cyberviolence. Initially, they warn the person who carried out the violent behaviour, deciding to register an FIR only if the complainant wants to pursue action. In most cases, women only want the harassment to stop and are not keen to follow up.

3.3 Gaps in the law and its application

The repeal of Section 66A leaves women with very little recourse to pursue cases of gendertrolling. Misogynistic speech is not recognized as grounds for hate, and the police and lawyers find it difficult within other sections of the IPC to establish a case that stands in court.

Law enforcement officials and lawyers who were interviewed for the research pointed out that the repeal of Section 66 A of the Information Technology Act had resulted in a legal lacuna with respect to addressing gendertrolling, that is, in cases of sexist and misogynistic commentary that did not have an angle of sexually explicit content (see Box 1). As a senior police official in Kerala expressed it:

> Now you have to look; is there a sexual aspect? Is there obscenity? If so, evoke the relevant sections; if not, apologize and tell [the victim], the chances of justice are slim.
>
> Police officer, key informant, Kerala

Box 1. The legal lacuna after the repeal of Section 66A of the Information Technology Act

The erstwhile Section 66A of the Information Technology Act penalized electronic communication of a *"grossly offensive or menacing character"* and information *"causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will"*. But its arbitrary deployment by the power-elite to silence critical and dissenting practices resulted in it being struck down by the Supreme Court in *Shreya Singhal v. Union of India* for being vague, arbitrary and unconstitutional.[lxxvi]

While the repeal of Section 66A was undoubtedly essential to preserve freedom of expression, one of the unfortunate by-products of the Supreme Court judgment has been an absence of legal protection for victims

of sexist and misogynstic trolling. The current legal provision on hate speech – Section 153A of the Indian Penal Code – does not mention gender expressly as one of its protected categories. This is because hate speech laws in India find their constitutional validity in Article 19(2) that permits the government to place reasonable restrictions on freedom of speech and expression in the interest of public order. In this framing, a speech act falls under the category of 'hate speech' only when there is demonstrated evidence of incitement to violence through acts that are prejudicial to the harmony between communities and castes. Since the prevailing legal framework in India privileges a 'public order' framing that does not recognize dehumanizing impacts and structural violence of discriminatory speech, it cannot be applied to gendertrolling. Law needs to take into account the intrinsic violence of speech that stigmatizes women, perpetuating notions of female subjugation.

In the absence of a specific legal provision to address gendertrolling, the only resort for the police is to deploy IPC sections pertaining to criminal defamation or criminal intimidation. But these sections have a high legal threshold (see Box 2) and the police may find it difficult to establish a case that stands in court. As a senior police official in Kerala put it:

> But those provisions [criminal defamation and criminal intimidation] wouldn't stand in court... I mean, you'd have to show that her [the victim's] reputation was irreparably damaged, that is, that her character was damaged socially... and as for 507 [criminal intimidation by anonymous communication], you'd have to prove in court that she could actually not perform her normal work etc.
>
> Police officer, key informant, Kerala

Box 2. Why criminal defamation and criminal intimidation are not suited to address gendertrolling

Criminal defamation

As criminal defamation is a non-cognizable crime, the complainant cannot approach the police directly and has to first file the case before a magistrate. Further, only those who are personally aggrieved can file a case of criminal defamation under Section 499.[lxxvii] Also, the process of filing a case under criminal defamation provisions is much harder when compared to filing cases under the (erstwhile) 66A. Furthermore, the complainant receives no assistance from the police and needs to prove the case herself, an additional burden that most women will not be in a position to take up.

Criminal intimidation

In *Manek Taneja & Anr v. State of Karnataka*, the Supreme Court held that the intent to cause alarm is a necessary component of criminal intimidation which needs to be gleaned from the circumstances of the case

at hand.[lxxviii] Whether the grounds for criminal intimidation also include an evaluation of whether the acts of the perpetrator actually did cause alarm is a disputed point. Some courts have held that it is immaterial,[lxxix] while others have pointed out that it is material.[lxxx] The latter stance could work against women because many victims of gendertrolling may continue to use platforms they were trolled on and may not show any overt signs of psychological trauma or alarm.

To deal with online sexual harassment, the police prefer to deploy anti-obscenity sections rather than provisions rooted in privacy and consent. They are also not updated with the latest judicial decisions. This leaves much to be desired for the feminist pursuit of justice.

In the two main legislations that address online sexual harassment, the Indian Penal Code and the Information Technology Act, conceptualizations of sexual violence as a violation of privacy and autonomy [eg. IPC Section 354C (voyeurism), IPC Section 354D (cyberstalking), and Section 66E of the IT Act (privacy violation)] co-exist uneasily with archaic 'anti-obscenity' provisions [eg. Section 292 of the Indian Penal Code, Section 67 of the IT Act].

This research noted that in cases of online sexual violence, police prefer anti-obscenity provisions. Sometimes, this is because the de facto reading by police officials booking the case is often not exactly in consonance with the de jure law and latest judgments in this regard. For example, in Section 66E of the Information Technology Act which punishes the "capture, publishing 'OR' transmission" of images of the "private areas" of any person without their consent as a privacy violation, the police tend to interpret this as an 'AND' clause. Therefore, in cases where a woman may have consented to the capture of her image, but not to its subsequent dissemination, typically, in cases of (what goes by the misnomer), 'revenge porn', the police do not apply the Section. Interviews with police officials in Karnataka reflect this kind of narrow reading of 66E that accounts for consent only during capture of an image, but ignores the vitiation of privacy resulting from its non-consensual dissemination.[lxxxi]

In *The State (Cyber Cell) v. Yogisha* involving unwelcome sexual advances by email, doxxing, creation of a fake profile, and circulation of solicitous messages attributed to the complainant, the court held that Section 66E would apply to such acts of doxxing, as the emails invaded the complainant's privacy.[lxxxii] However, the police often do not seem to be abreast of the latest judgements.

There is also a disturbing tendency where the police tend to invoke Section 67 of the Information Technology Act rather than Section 354C of the Indian Penal Code in cases of non-consensual circulation of intimate images, citing the reason that obscenity provisions are stricter and there is a higher chance of conviction.[lxxxiii] The problem with invoking obscenity provisions is that this may also lead to situations where the victim herself is charged. For instance, in a case of non-consensual circulation of intimate images, if Section 67 is invoked, a strict reading could lead to the woman herself being punished, even if she had initially sent the intimate images of herself voluntarily.[lxxxiv]

At the same time, the police also report that to cope with mutations in cyberviolence, sometimes there is no option other than to turn to anti-obscenity provisions. A cybercrime case in Kerala,[lxxxv] which involved a wedding photo studio misusing video images of brides to produce porn through morphing is a case in point. Given that anti-obscenity provisions in India are rooted in patriarchal, Victorian morals rather than feminist premises of women's dignity, this route may provide a pragmatic solution, but one that opens up threats that could potentially gag sexual expression.

Producing admissible digital evidence in court is complicated not only by poor compliance to Standard Operating Procedures (SOPs) by investigating officers, but also by varying interpretations in Courts of certification standards. Obtaining the cooperation of foreign internet intermediaries implicated in evidence-gathering poses jurisdictional challenges often impossible to overcome.

In order for digital evidence to be admissible, law enforcement agencies follow an SOP, which among other things requires a chain of custody to be maintained that tells the court who all handled the data once it was taken into police custody. The evidence is hashed (hashing of evidence is like a digital fingerprint of a file taken to match copies with the original) so that any tampering can be detected and a write blocker (a device that allows acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents) is also installed.[lxxxvi] Law enforcement officers from Karnataka interviewed for this research shared that they did have a SOP for the collection of digital evidence, but the research team was not given access to this document. In Kerala, the police officer who played a key role in setting up a SOP for the state police admitted to the research team that though this was in operation, there was much to be desired in compliance. Currently, officers seem to be following the SOP only if they have a *"special interest in pursuing the case"*.[lxxxvii]

There also seems to be a lack of agreement about the certification requirements to be followed under the Indian Evidence Act for the production of digital evidence in courts. In 2018, the Supreme Court ruled that if an electronic device is in adverse possession, then certification under section 65B need not be produced.[lxxxviii] The court held, *"the applicability of requirement of certificate being procedural can be relaxed by Court wherever interest of justice so justifies."*[lxxxix] This permissive reading of the law can aid survivors of gender-based cyberviolence in prosecuting their cases without being held up by requirement of the certification. Despite the Supreme Court judgment, ambiguities persist in the interpretation of the certification requirement among lower courts. As one senior police official from Kerala put it:

> Yes, now if the court deems fit it can take into account electronic evidence that is not certified also … but more often than not, certification is required. The court has to decide, and different judges take different stands. Now for example, I just went to Kollam to participate in the trial of a man who murdered his wife… In court his lawyer insisted that the evidence collected by the police and produced

> was inadmissible, and that I could not be evaluating it since I could not be considered 'a responsible person fit to certify'. The judge however asked me about my training and the responsibilities I had handled in my career and struck down the objections… But this is not always the case … other judges could think otherwise. The reasons different judges present for accepting or rejecting digital evidence can be highly subjective.
>
> Police officer, key informant, Kerala

Marshalling digital evidence is difficult for a number of reasons. First, there are infrastructural challenges in state digital forensic labs as technological upgrades are often delayed due to bureaucratic hurdles.[xc] Second, platform intermediaries often do not cooperate or respond promptly to requests from law enforcement officials for user profiles or data. A court affidavit filed by a senior police officer that was accessed by the Tamil Nadu research team observes: "*During the years 2016 to 2018, the Chennai City Police, Cyber Crime Cell had sent about 1940 [IP log] requests to such online social media companies. Out of which, IP logs details were received for only 484 requisitions. It is necessary to state that remaining 1456 IP requisitions were rejected by social media companies*."[xci]

One of the reasons that platform companies use to deny or turn down these requests is that what the police highlight as an 'offence' is a perfectly legitimate speech act under their community standards. A senior officer in Kerala interviewed for the research highlighted how Facebook's western ethnocentric bias leads to convoluted exchanges between the state police and the representatives of the Facebook team:

> For example, the term "machi", which when translated means "infertile woman", lacks the insulting tone it has in Malayalam, and so Facebook refused to consider this as an offence. They kept asking how 'infertile' can be an offending term!
>
> Police officer, key informant, Kerala

Exerting pressure on platform companies to comply with Indian law is further complicated by jurisdictional challenges as for most platform companies, servers are located out of the country. In these cases, access to relevant data is dictated by the Mutual Legal Assistance Treaties (MLATs) – agreements that the government of India has signed with 39 countries, including the United States, with respect to cooperation in cross-border legal processes – and Letters Rogatory or otherwise informal channels (MoUs). While Letters Rogatory have certain advantages such as their wide scope compared to MLAT, under which only data mentioned in the treaty can be recovered, the advantage of the MLAT is that as per international law, the foreign country cannot refuse to share the data if the procedures established under the treaty are followed.[xcii]

MLATs however, tend to lay down a cumbersome process. Law enforcement officials interviewed, observed that to get a response through the MLAT with the US [where most platform companies house their servers], it takes 2-3 years. As noted by a police official in Karnataka, delays can be huge:

> It takes a long time; police request for evidence, Facebook takes 20 days, then FB asks for more information, police responds and again, Facebook takes 20 days to respond. This negatively impacts the investigation process. There are also lots of technical issues. We end up moving from desk to desk in the FB offices in order to get permissions.
>
> Police official, key informant, Karnataka

Research by the Observer Research Foundation on the India-US MLAT has noted that failures in exchanging data occur because the system is dated and not designed to handle the volume of requests for electronic data. It also points to the capacity deficit of Indian law enforcement (for instance, poorly drafted requests resulting in denial of evidence) as well as lax timelines for processing domestic approvals.[xciii]

Even in instances where servers are located in India, where the police may exercise their powers under Section 91 of the Code of Criminal Procedure (CrPC) to access evidence, matters are complicated by the failure of the government to notify rules for the preservation and retention of data by intermediaries as provided in Section 67C of the IT Act.[xciv]

4. Conclusions

In understanding how technology and society are interlaced, it is crucial that research is able to avoid the pitfalls of deterministic thinking – sociological and technological. Indeed, social values do get carried into the imprint of technology. And, technological affordances bear testimony to social relations. Conversely, the particular affordances of technology carry new codes that can destabilize cultural givens.

Digital technologies have generated unprecedented ways of being and doing, dramatically changing the social and economic order. Recoding human subjectivity and social interactions, they recast power relationships. Gender relations are centrally implicated in this shift.

This study examined how the born-digital generation of young female adults who live their lives in the criss-crossing of the online-offline, grapple with the challenges of navigating digital space in the face of cyberviolence. Through a survivor-centred, feminist approach, it sought to unpack the fluidity between human subjectivity, social ideologies, legal norms, institutional rules and digital networks.

What the study concludes is that even as digital space opens up a thrilling new frontier for young women's self-building, intimacy, public expression and more, the techno-architectures of the platform economy are not necessarily liberating. Norms and practices of digital space do not seem to erase gendered hierarchies. On the contrary, even though they are contested by feminist actors and actions, oppressive gender relations continue to prevail in the contemporary configurations of society.

The conclusions from the study are discussed below, along with recommendations for institutional change.

1. Capitalist digital architectures generate regressive social arrangements that perpetuate retrograde gender norms and practices.

The research shows how patriarchal gender narratives are not only pre-coded into online communicative environments, but equally, how capitalist digital architectures generate regressive social arrangements that reify retrograde gender norms and practices. Emerging sociality reflects a gender conservatism, normalizing hegemonic masculinity and defensive femininity.
The study reflects how male privilege in cultures of patriarchy combine with affordances of digital space, naturalizing and routinizing acts of male violence as activities of 'play'. Such toxic disinhibition is not limited to anonymous trolls, for even when profiles exhibit real identities on platforms, people still post violent and hostile messages.[xcv] Platform architectures exploit toxic disinhibition, locking in individuals for their invaluable data. Sexist content is allowed to be highly visible since it finds high currency among users, but feminist content that may be unpopular is relegated to the back pages.[xcvi]

The matrix of domination that operates against women in cyberspace is intersectional. When women speak up or publish their opinions, they invariably face sexist slurs. Feedback systems such as comments, likes and dislikes – far from reining in sexist and misogynistic incivility – may actually exacerbate it. Women from minority religious groups, dalit women, and non-heteronormative women are at a higher risk of being trolled and harassed in particularly heinous ways, with body shaming and malevolence targeting their social identity. As dalit activist Kiruba Munusamy has highlighted, while all women may be insulted online, dalit women may be labled as "hereditary sluts"[xcvii]. Patriarchy in cyberspace constructs and produces a hierarchy of gendered bodies – valuing and devaluing, valorizing and demonizing women, depending on their particular social locations and their assertions of public-political identity.

Image-based cultures of social media reward and reinforce gender performance based on accepted gender norms and roles. Young women project femininity and respectability (even in women only online communities),[xcviii] and men, masculinity and aggressiveness. Inhabiting visual cultures that afford them the space for self exploration and intimacy, young women face a double bind. Digital space is where they find affirmation and recognition. But at all times, they must balance the self exploration and the quest for intimacy with social approval. They must negotiate a shifting line of "just right sexuality"[xcix]- perform femininity by looking attractive for a capitalistic system that thrives on likes,[ii] but not flout gender norms.

The study reveals that young women are particularly critical of other women whose pictures get leaked online, judging victims of violence for their lack of caution and rectitude, rather than unequivocally condemning the male perpetrator for his acts of violence. Young men expressly suggested that women have had a hand to play in the

violence that is meted out to them online. They betray a deep discomfort with the visibility of women in online spaces. When women post selfies or pictures, they are invariably sexualized and blamed.

Young men, the study found, forge male-only online spaces to share images of women and exchange notes about their desirability and sex appeal, send women unwelcome sexual imagery and even disseminate sexually explicit images of ex-partners vengefully after a break up. This normal is internalized by young women and men as natural; obvious practices in prevailing gender cultures that women must somehow navigate.

The chilling effect of violence on women's participation in online spaces is well documented and also reflected in this research. Cyberviolence negatively impacts the civil-political rights of women, their aspirations to be part of the public sphere and the public sphere itself. Young women withdraw from political conversations in digital spaces when attacked. When women withdraw, public discourse has to contend with a gendered realignment that is inimical to democracy and the equal citizenship of women.. Unfortunately, challenging sexist and misogynistic speech in social media is not an option; counter speech may just make women more vulnerable.

What the lived experiences of young women and men from the born-digital generation suggests is an alarming naturalization of gender-based violence, not consciously acknowledged for the social differentiation and injustices it perpetuates. This is not to imply that women are not appropriating digital space for their self-actualization, emancipation and struggles against patriarchy, capitalist exploitation, homophobia, casteism and religious bigotry. On the contrary, what this study underscores is that feminist political subjectivity and agency is under siege, with a largely impalpable, structural shift in the axes of public and private life denying women a part of what it is to be fully human.

2. Gaps in the law perpetuate the naturalization of gender-based cyberviolence, reinforcing a culture of silence that prevents women from seeking redress.

Feminists have had an uneasy relationship with the institution of law. As an inherent part of the patriarchal social structures that feminists seek to dismantle, the discursive space of law presents only a partial solution to feminist visions of justice. In the 1980s, the women's movement in India anchored its struggle to legal reform, with many feminist lawyers and activists eager to seize the law as a vehicle for ushering in a more gender-equal society.[c] Their efforts led to the enactment of many ground-breaking laws that addressed regressive social practices oppressing women; such as dowry, sex-selective abortion and sexual harassment at the workplace. But as time went by, the failure of such progressive legal frameworks to translate into a meaningful transformation of institutional patriarchies in the court system and the police disillusioned many in the movement.[ci] The generation of feminists who came after those who had fought for legal reform also had misgivings about the reduction of women to 'passive victims without agency' by the very laws that had been initially championed by women.

Nevertheless, the law cannot be completely abandoned as a site for gender-transformative social change.[cii] Law has very high symbolic significance, as a statement of the state's commitment to the constitutional value of anti-discrimination. For members of marginalized communities, the law can thus foster a sense of belonging to a polity they have traditionally been denied full membership in.[ciii]

Legal reform is meaningful if it is cast as a project of addressing the law's inability to perceive difference.[civ] If the androcentrism of the law can be overcome, women will have a new vocabulary to articulate how their claim to justice is different and distinct from that of men, because of the uniqueness of their marginalization under a patriarchal order. By criminalizing acts of cyberviolence against women, the law can legitimate the experiences of women harmed, and change the social meaning of such acts.[cv]Currently, the trivialization of cyberviolence – by harassers, by law enforcement, and many a time, by victims themselves – is because the law is unable to completely perceive the mutations of gender-based violence emerging in digital sociality.

When analyzed from this starting point, it is evident that the current legal response to gender-based cyberviolence in India is not only inadequate, but also regressive.

Existing legislation is an uneasy patchwork of 'anti-obscenity' provisions (Section 292 of the Indian Penal Code, Section 67 of the IT Act), and more recently introduced provisions grounded in privacy and consent (Section 354C of the Indian Penal Code, Section 66E of the IT Act). Although the Acts are often used together by the police, in a recent decision, the Bombay High Court held that prosecution under both laws could amount to double jeopardy, and that the special law (IT Act), should override the general law (IPC).[cvi] Needless to say, not all sections of the IPC have mirrors in the IT Act, and vice-versa, and even when there are sections tackling the same kind of crime, minor but crucial differences exist. Unfortunately, obscenity-based provisions tend to be privileged by law enforcement agencies, even in cases where privacy and consent-based provisions could be used, because of their conviction that obscenity provisions are stricter and there is a higher chance of conviction.[cvii] Partly, this is because law enforcement officials have a very narrow interpretation of Section 66E of the IT Act (privacy violation) and are not aware of judgments that extend its application to offences such as doxxing. But it is also true that there are some new types of sexual violations that existing privacy sections (whether in the IT Act or in the IPC) do not cover, such as sending pornographic images to women (dick pics) without their consent. The juggernaut of market-based digital innovations with new products and affordances is only likely to create newer situations that challenge the semantics of the law.

Further, by their very design, anti-obscenity laws are not designed to provide a structural response to gender-based violence and the exploitation of female bodies. They are instead, meant to aid the state in the creation of a sanitized public sphere. Historically, courts in India have used the male gaze to censor sexual expression through obscenity law[cviii]. Even when the Supreme Court has taken a more progressive stance on obscenity,[cix] it has done so by upholding free speech rather than account for the dignity and harm perspective that feminists underscore as important in abusive content.[cx]

The repeal of Section 66A of the IT Act and the failure of the hate speech provision in the IPC to address sexist and misogynistic hate speech have produced a legal lacuna with respect to addressing gendertrolling. As the Law Commission observed in its 2017 report:[cxi] "*Incitement to violence cannot be the sole test for determining whether a speech amounts to hate speech or not. Even speech that does not incite violence has the potential of marginalising a certain section of the society or individual. Moreover, incitement to discrimination lies at the heart of hate speech principles. In the age of technology, the anonymity of internet allows a miscreant to easily spread false and offensive ideas. These ideas need not always incite violence, but they might perpetuate the discriminatory attitudes prevalent in the society.*"

Criminal defamation and criminal intimidation provisions under the IPC adopt a very individual-centerd notion of harm that does not capture the collective harm stemming from generalized misogynistic trolling, especially instances of harassment where women are targeted not individually, but as members of a group - defined by gender, caste, sexual orientation, etc.[cxii]

Marshalling digital evidence also becomes a major impediment in bringing perpetrators to book. In cases of cyberviolence, unless the provisions of the IT Act are explicitly invoked, the cybercrime police station cannot investigate. There is also lack of clarity about the certification requirements to be followed under the Indian Evidence Act for the production of digital evidence in courts, even though in 2018, the Supreme Court had permitted a permissive reading of Section 65(B) of the Indian Evidence Act, waiving the certification requirements for electronic records in instances where a device was in adverse possession. Not all lower courts seem to be abreast of this development.

By ignoring the harms caused by online violence, the legal system becomes complicit in their trivialization.[cxiii] Lack of legal validation of gender-based violence can lead to a marginalization of women's experience, deeming it harmless teasing that women should tolerate. It perpetuates the semantic silences that tend to erase the lived experiences of women, normalizing abuse and violence as socially acceptable in common sense.

The internet's assimilation into dominant structures of patriarchy produces new faultlines of gendered oppression in both public and private spheres that women must negotiate. These new contours of oppression are, by and large, not recognized fully, either in law or public perception. They are 'misframings' or as Fraser puts it, instances wherein "the meta narrative of what is justice is itself unjustly framed",[cxiv] thus depriving women of the very right to make a claim. The continued use of oppressive, anti-obscenity sections is part of the systemic misframing of gender justice.

It is time juridical frames stop functioning in the binaries of offline/online, real/-virtual and start understanding sociality as a human-technological hybrid.[cxv] Part of the techno-social experience for women is gendered violence, and it is time laws are updated to give meaning to the particular experiences of women.

3. Though platform intermediaries have introduced new features for enhanced safety, their response to gender-based cyberviolence typically hides behind the smokescreen of difficult-to-fashion 'community standards' or a blatant transfer of duty to the state.

The take-down of offending content becomes a priority for women who face cyberviolence, especially if it is of a sexual nature. The platform intermediary, therefore, becomes an important actor to ensure redress for victims. Most dominant social media companies have, over time, introduced new design features for improved user safety and security.[cxvi] However, these measures, though very welcome, cannot be a replacement for the necessary responsiveness and effective resolution by the platform of complaints from women users on incidents of misogyny and harassment.

Platform companies have tended to selectively, arbitrarily, and unaccountably, deploy their community standards, based on business interests, in different markets. Facebook's track record of implementing its own community standards on gender-based hate speech is a case in point. This research also underscores another long-standing problem that feminist activists from the global South have been highlighting about platform companies – their non-responsiveness to complaints of harassment in languages other than English.

The community standards enforcement report that Facebook released in May 2019 reveals that the company still struggles to pro-actively enforce its standards for cyberbullying and harassment, but is able to perform better on hate speech. In Q4 2018 and Q1 2019, across its global community of users, the company only caught 14 % of the 2.6 million instances of harassment reported, but for hate speech, the company internally flagged 65.4 % of the 4.0 million moments of hate speech reported by users.[cxvii] A better strike rate for hate speech does not necessarily mean that the criteria used by the platform are universally acceptable. As discussed, oftentimes hate speech criteria of the platform are not attuned to the diversities of the cultural contexts in the global South. With hugely varying standards on acceptable speech across the world, dominant social media corporations seem to veer towards American jurisprudence, using an approach that requires proof of imminent violence rather than an examination of the indignity of speech.

In 2018-19, Facebook has held global consultations for the establishment of an Oversight Board for Content Decisions. The report of the outcome from these consultations has "raised more questions than answers" with lack of clarity on the values or principles guiding the accountability framework that will inform the Board.[cxviii] Also, the report does not address, how exactly Facebook plans to deal with the issue of contextually interpreting human rights standards in different cultural contexts.

In India, platform companies have taken the view that the business of securing women's rights is the sole responsibility of the state and that their liability extends only to compliance with official rules. Even here, their

stance has been that the government needs to establish the nodal agencies that will monitor the internet for flagging illegal/offensive content, in sharp contrast to their conduct in European jurisdictions.[cxix]

Automated filtering of patently illegal content and the traceability of its origin for law enforcement purposes, does remain a vexatious issue. However, as gatekeepers of social and public interaction, platform companies must step up to reexamine their role towards a healthy public sphere. As things stand today, the remote possibility of any redress for women who approach such platforms gets invariably caught up in the rhetoric of 'community standards' that platform companies use to justify opaque actions that are accountable to no one.

4. Survivors invariably do not step up to seek help given the high moral panic associated with young women's sexuality and deep-rooted institutional patriarchies.

Young women do approach their friends for support in instances of cyberviolence. While this plugs the important aspect of addressing psychological trauma to some extent, it is unlikely to provide respite from ongoing incursions. Also, friends may not always step in to support victims of gendertrolling and cyberbullying in online communities because of 'stigma contagion' – the possibility that allies who support the survivor may also come under attack. This can prevent bystanders from intervening.

The normalization and trivialization of cyberviolence also makes it difficult for women to recognize that they have faced violence. Even if they do perceive a violation, if and whether a woman will seek institutional support for relief from cyberviolence depends on familial support, perceived social disapproval/stigma, level of awareness of the law, and trust in law enforcement agencies and the judicial process.

Young women exploring intimacies online do not want to admit to consensual sexual relationships, given the stigma around casual and pre-marital sex and possible loss of face for approaching the police. Other research also confirms that in cases where the perpetrator is a known person, there is a lower chance that the same will be reported, compared to cases where the perpetrator is a stranger.[cxx] Laws on violence are also designed for heterosexual relationships and preclude use by same sex couples who may not be willing to approach parents and other relatives for support.[cxxi] Lack of knowledge that the harassment faced is a crime punishable by the law and low levels of legal awareness also impedes women from making formal complaints.

Law enforcement officials do sometimes trivialize cyberviolence, creating false dichotomies between online and offline violence, and drawing false connections between body and harm. Functioning under limited resources, the police prioritize cybercrimes using self defined notions of urgency. Crimes in which women are disproportionately the victims, such as trolling, doxxing, etc. are treated as far less important. Even here, sexist attacks may not get the same attention as sexual harassment. The police may even blame women for not being careful enough, for not exercising caution, and shame them when sexual relationships are revealed.

There are also survivors who report receiving effective responses from the police. Officials trying to manage within a system that is under-resourced and entailing challenges with respect to territorial jurisdiction in cybercrimes tend to veer towards pragmatic solutions, de-emphasizing legal options and turning women towards platform intermediaries for quick, low cost options. The biases of law enforcement officials also rest foundationally in, and are compounded by patriarchal frameworks of prevailing laws.

The tediousness of the judicial process and the prospect of facing patriarchal actors in various institutional settings who will sit in judgment of the survivor's character may be too much of a cost for survivors to bear. On the other hand, blocking, flagging or reporting the perpetrator on the platform may work only in some cases, and the possibility that the perpetrator may create alternate profiles to continue the harassment is ever-present.

The lack of social responsiveness to and high moral panic associated with young women's sexuality also reinforces a culture of secrecy about gender-based cyberviolence. The result being that victim-survivors are isolated, without any real options to seek psycho-social support and redress.

5. Recommendations

Gender-based cyberviolence is ubiquitous. As a society, we must identify the particular ways in which this results in divesting women of their social and political citizenship. The fight against normalization of sexism and misogyny on a planetary scale is part of the fight to claim the potential for an interconnected, digitally mediated sociality for substantive gender transformation. A systemic change that calls for a rethink about the digital protocols of the communicative arena as well as the socio-cultural fabric of digitally mediated institutional relations is needed. Lawmakers, educational institutions, workplaces, law enforcement agencies, internet intermediaries and civic organizations need to start understanding gender-based cyberviolence for its far-reaching consequences. Progressive civil society actors must come together to build an informed dialogue on norms and strategies for formal and informal institutional mechanisms for redress.

The effectiveness of strategies to address women's equality depends on highest level political commitment, adequate resource allocation and appropriate coordination mechanisms that can provide support for monitoring and recalibration. The National Policy for Women Empowerment is yet to be adopted, although a revised draft was introduced in mid-2019 by the Ministry of Women and Child Development. This leaves the vision of and strategic pathways to women's rights and empowerment lacking a coherent articulation. Schemes introduced by various governments at national and state levels are mostly stand-alone initiatives coming from imperatives to address different aspects of gender-based discrimination.

Digital rights of women tend to be reduced in policy priorities to 'bridging the access gap', a foundational priority no doubt, but conceptualized as an end in itself. Digital strategies and gender strategies need to be integrated in a multi-layered way to enable women's digital citizenship. This means laying down both the pathways for digital enskillment, fluency and empowerment and the priority actions to ensure women's right to freedom from harm. A

systemic response to gender-based violence, including cyberviolence, must come from a progressive vision of society where women are free and equal. That is, free from the lurking threat of all forms of violence to be able to enjoy and express their full citizenship.

A key initiative in India to address gender-based cyberviolence is the cybercrimes portal – set up by the Ministry of Home Affairs (MHA) with funds from the Nirbhaya scheme of the Ministry of Women and Child Development (MWCD). The portal is a means for victims to file complaints (with the option for anonymous complaints) about – online child pornography/child sexual material and sexually explicit content such as rape and gang rape content[cxxii] – which are then forwarded to state level police.

Situating gender-based cyberviolence in an overall framework of a complaints mechanism tends to whittle down the issue as a crime to be managed through law enforcement processes. While an accessible online space for victims to reach out to authorities is certainly welcome, digital strategies must be guided by a rights-based approach that informs, educates and guides. Any online portal must therefore be designed to address preventive, ameliorative and transformative aspects, providing appropriate material for women of different ages, tool kits for educators, interactive FAQs with automated chat bots, connections to other services for support and thus provide all citizens access to valuable resources as a one-stop-shop for learning and action. The victim-survivor who reaches the portal will then have a set of real options for support and redress. As reported in this research, the Kerala police seem to have embarked on an initiative that integrates some of these elements.

Scholars studying violence against women have pointed how effectiveness of strategies to combat the problem often depends on community-embedded approaches that address cultural norms. Cyberharassment may not be the same as street harassment, but tackling the issue will need strong preventive strategies to address local patriarchal cultures. In this study, not only were perpetrators in large measure known to the victim, but local flavours of patriarchy were widely reported in the nature of harms experienced and inflicted. Therefore, offline and culturally embedded efforts in schools, colleges and communities, led for instance, by the Departments of Education and of Rural Development are integral to the efficacy of change processes.

The underutilization of the Nirbhaya Fund is a sad reflection of the absence of a cohesive vision and coordinated execution towards gender-transformative social change. Outlays for the Fund need to be expanded to enable a well-coordinated programme based on inter-ministerial cooperation and built on district level efforts, that not only uses digital technologies as an ‘innovative solution’, but also recognizes the emerging social context in which digital technologies reshape gender relations.

Additionally, national and state level task forces with representatives from different government departments, law enforcement agencies and civil society actors – women’s grassroots organizations, feminist scholars, educators, technologists, legal experts, mental health professions – need to be set up for strategy development, monitoring and review.

The imperative is primarily two-fold: ensuring access to justice for victims-survivors and transforming deep cultures of sexism. This section outlines below the priority actions that are required at the formal institutional levels: legal reform, survivor-centred institutional responses and platform governance.

5.1. Legal Reform

The law can be a useful instrument in enabling the realization of gender equality. Studies suggest that where anti-cyberbullying laws have been introduced, there is a positive impact in terms of more speech by women.[cxxiii] Also, by ensuring that women's complaints are heard, law has an important role to play, given its ability to shift given categories of meaning and thus challenge the normalization of online subcultures of misogyny. Viewed from this perspective, it is clear that there is an urgent imperative to improve the prevailing legal response to gender-based cyberviolence in India.

➔ A new law on sexual harassment, grounded in ideas of privacy, consent and women's dignity, is necessary to deal with emergent forms of sexual violence that are emerging in digital spaces such as doxxing, voyeurism, cyberstalking, involuntary pornography, and non-consensual circulation of intimate images. This will help overcome the current quandary where women victims have to resort to anti-obscenity provisions to deal with such situations. Legal interventions in this direction are being adopted by various governments the world over (see Box 3).

Box 3. Specific legal interventions directed at cyberviolence

The UK government asked its Law Commission to conduct an assessment of the adequacy of the present laws to combat trolling.[cxxiv] Singapore has taken the step of outlawing 'revenge porn' and 'cyber flashing' (acts such as sending dick pics).[cxxv] In Canada, a court in Ontario created the tort of 'public disclosure of private facts' to address a case of non-consensual circulation of intimate images, and in Saskatchewan, the Privacy Act was amended to address non-consensual circulation of intimate images.[cxxvi] The Act places the burden of proof on the accused to prove that he received the images under consent.[cxxvii] The draft Online Safety Modernization Act of 2017 in the US seeks to address doxxing and sextortion, as part of providing a comprehensive response to cybercrimes against individuals.[cxxviii]/

➔ Gender and sexual orientation should be included as protected categories in Section 153A and Section 505 of the IPC. Further, the law must shift its focus from 'incitement of violence' to 'harms to dignity', in order to effectively address the growing pandemic of gendertrolling. Relying on provisions of defamation individualizes harm, whereas a hate speech law seeks to address the structural discrimination that exists in society.

➔ The procedures for presentation and certification of digital evidence must be simplified. The more permissive reading of Section 65B of the Indian Evidence Act by the Supreme Court that allows for a waiver of the certification requirement of digital evidence in instances where a device is in adverse possession, must be applied in cases of cyberviolence. However, it is important that easing up of

certification requirements does not promote illegal collection of digital evidence through invasive state surveillance.

➔ In order to overcome the challenges in cross-border access to data due to the difficulties of enforcing extra-territorial jurisdiction under MLATs,[cxxix] mandating storage of data within India is one option, as recommended by the data localization provisions of the Srikrishna Committee Report.[cxxx] Of course, indiscriminate state access to citizen data is not the goal, and any mandatory data localization should not be allowed to happen without effective privacy and personal data protection legislation.

➔ Intermediary liability law and policy in India is in a phase of transition. A differentiated intermediary liability regime that takes into account differences in the user base, type and functionalities of platform intermediaries in defining responsibility and accountability for content must be put in place. The 2017 European Commission guidelines on Tackling Illegal Content Online are a useful reference point in this regard. These guidelines, while laying down the liability of intermediaries to adopt automated filtering for patently illegal content, also prescribe safeguards such as counter-notice mechanisms that would reinstate the content if found to be legal through a dispute settlement body.[cxxxi] The notice-to-notice system as suggested by New Zealand's Harmful Digital Communications Act also offers a more balanced approach to this issue (See Box 4).[cxxxii]

Box 4. New Zealand's notice-to-notice system

New Zealand's Harmful Digital Communications 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 a 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 cannot 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 respond to the notice 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.[cxxxiii]

5.2. Survivor-centred institutional responses

There needs to be a shift in the institutional cultures of formal redress mechanisms – the police, court systems and committees on sexual harassment in workplaces and colleges – so that patriarchal protectionism is replaced by survivor-centredness.

Police

- ➔ Targets for training of police personnel under the Cyber Crime Prevention against Women and Children (CCPWC) scheme must be increased by all states. Specifically, more women police personnel must be trained under the scheme.
- ➔ The personnel assigned to cyber cells or cybercrime police stations are very few and the ratio of crimes per investigating officer is highly skewed. Staff strength in cyber cells/cybercrime police stations, therefore, needs to be enhanced. There should be more women police officers posted at cybercrime police stations. Every state should have at least one all-women's cybercrime police station. This could help in increasing reporting of cyberviolence.[cxxxiv] **The success of UP government's 'Women Power Line 1090' also demonstrates survivor-centred approaches that guarantee confidentiality and provide support to victims in remote filing of complaints.**
- ➔ State governments need to create as well as improve websites for the reporting of cybercrimes. It is important that these websites are easily navigable and provide step-by-step instructions on how complaints can be filed both offline and online. Additionally, they can host videos of training modules on basic cybersecurity, as well as information about what survivors can do if they are facing cyberviolence in terms of preserving evidence, blocking/deleting abuse on their own and how to reach out to digital corporations. These websites should also link to the online portal set up by the central government for complaints of cyberviolence against women and children.[cxxxv]
- ➔ Police should periodically carry out outreach programmes in colleges to raise awareness of the available legal and non-legal options in cases of gender-based cyberviolence. **Collaborative projects involving the police and women's rights organizations and counsellors need to be set up to provide psycho-social assistance to survivors, so that they can cope with the trauma of violence and navigate the stress of waging a legal battle.**
- ➔ Dedicated data on cybercrimes against women must be collected and reflected in the publication of crime statistics by the National Crime Records Bureau.

Courts

- ➔ Under the CCPWC scheme, judges and public prosecutors need to be trained for cultivating the knowledge, skills and attitude required to ensure gender equality in the digital context. This will go a long way in survivors' access to justice. Pune city has an informal study circle for lawyers, judges and other

stakeholders on cybercrimes.[cxxxvi] Such efforts for continued exchange of ideas can be useful to promote feminist approaches to the law.

- ➔ Judges must avoid taking a protectionist approach and be open to creative applications of the IT Act and IPC provisions that emphasize women's dignity, privacy and autonomy.
- ➔ Free legal aid services are essential to ensure access to justice for survivors of violence who come from marginal socio-economic locations.

Internal Committees on Sexual Harassment

- ➔ All colleges and higher education institutions must set up the Internal Committee (IC) on Sexual Harassment mandated by the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 and the University Grants Commission.[cxxxvii]
- ➔ ICs must deal with complaints of cyberviolence with sensitivity and avoid trivialization and/or victim-blaming.
- ➔ ICs must also be in charge of organizing awareness programmes in colleges on cyberviolence that can address what it means to interact online with sensitivity and respect.

5.3. Platform governance

- ➔ Platform intermediaries must ensure timely and accountable responses to complaints of gender-based cyberviolence. Global platforms with large user bases must annually publish details of the number of complaints received, subsequent action taken, use of proactive tools to flag illegal content, investment in educating users and so on.[cxxxviii]
- ➔ Platform intermediaries must ensure that their content governance standards are transparent and account for women's human rights principles.
- ➔ State legislation must be introduced in order to ensure that platform intermediaries have a binding duty of care to their customers. As highlighted in UK's White Paper on Online Violence, an independent regulator to ensure that companies meet this standard of care is necessary. To bring companies in line, the regulator must have the powers to penalize the company as well as senior management for violations.
- ➔ Platform intermediaries must ensure that their techno-design choices ensure the safety and security of users of their services, especially the prevention of harassment online.[cxxxix] With popular discontent around misinformation and blatant privacy violations by platform intermediaries, governments have also swung into action, requiring intermediaries to adopt a privacy-by-design approach. This has seen a shift in the public stance of platform companies with regard to user privacy. However, with respect to gender-based violations, the click-bait economy that drives platforms dictates their positions. This must change

for user cultures to shift. The technological and social are tightly intertwined and changes to gender relations hinge on a paradigm shift of the platform economy's business ethics.

➔ The proposed amendments to the intermediary guidelines for platform companies have raised concerns about the potential for excessive censorship and surveillance because of their suggestions for automated filtering and enabling traceability (see Box 5). The reality of intermediary impunity and state incursion into civic liberties does present a Catch 22. However, a well-calibrated content governance regime straddling techno-design measures and legal mechanisms is a non-negotiable to protect and promote women's freedoms.

Intermediary liability guidelines in India

In 2014, the *Shreya Singhal v. Union of India* judgment read down the interpretation of an intermediary's 'prior knowledge' of unlawful material to mean notification from the executive/judiciary. In *Re Prajwala* and *Sabu Mathew v. Union of India,* the Supreme Court broke away from this precedent by hauling up digital corporations such as Facebook, Twitter, Microsoft etc., for failing to take action against the spread of rape videos and for allowing pre-natal sex determination adverts on their platforms.

In both cases, prior filtering of content became a point of contention, with the government demanding that companies do some form of content screening before permitting it to be posted/uploaded on the platforms they own, and the companies arguing that unless explicitly pointed to them by the government, they cannot be expected to take down content.[cxl] At the tail end of 2018, the Ministry of Electronics and Information Technology (MeitY) proposed amendments to the Intermediary Guidelines Rules. This draft has raked up much controversy, particularly in its direction to intermediaries to carry out automated filtering.[cxli] Civil society comments on the draft have raised issues of excessive take-downs, especially when the illegality of the content is not apparent; and on the foreclosure of algorithmic scrutiny because of the use of proprietary algorithms by digital corporations.[cxlii]

These concerns about the risks that automated filtering poses because of facilitating an inscrutable, privatized content governance regime are in sync with cutting-edge thinking in international human rights circles.[cxliii] But at the same time, it is important not to throw the baby out with the bathwater, considering that we live in a context where social media companies such as Facebook and Youtube are already enforcing their privatized AI-supported content governance regimes to identify and remove content that violates their terms of use, without any legal oversight.[cxliv] Also, in digital sociality where "machine intelligence is systematically mobilized to hound women", algorithms could well be used to defend women from the onslaught of violence online.[cxlv]

This is not to detract from the larger issue at stake in relation to state power and the fact that guidelines and rules issued by the executive tend to circumvent parliamentary processes of deliberative norm development. The role of the intermediary needs considerable thinking on the part of feminist actors so that the focus of intermediary liability is expanded to include easy redress for experiences of violence that women face and making platforms responsible for feminist techno-design.

6. Post-script and questions for further research

As a socio-legal analysis to understand the phenomenon of gender-based cyberviolence, this study has generated a body of evidence that can support strategies for change. The imperative to build knowledge about gender and power in the digital context cannot be overemphasized. As law and policies play catch up, informing them with insights that are contextual, theoretical and normative is vital. Feminist research has a unique vantage to make such a contribution.

As was argued in this study, legal-institutional change can be an enabler of gender equality. Feminist insights in this regard can provide an ethical compass for debating the appropriate values and principles, norms and rules for institutional change. While this research has attempted to build a thesis about what the present of digital sociality means for the future of gender equality, it is only a partial analysis. Galvanizing the knowledge for change will need continuous knowledge building and new disciplinary pathways.

In order to further test the thesis of this study and to broaden and deepen the knowledge terrain on the issue in India, multiple pieces on the gender canvas need dedicated inquiry; How do particular locations – age group, sexual preference, linguistic background, religious identity, nature of use – impact the victim-survivor and her responses? How do varying architectures of platforms and their structural antecedents affect gender performance and gender norms? How are regressive gender norms being challenged in and through digital counter cultures? How should feminist agency be understood in relation to the digital? How do men respond to digital socialization? How is the law situated in relation to processes of redress in gender-based cyberviolence? What are implications of current legal regimes for gendered meanings of equality and justice? What new institutional mechanisms – formal and informal – are necessary for speedy justice for victim-survivors? How should the law address platform accountability with respect to gender-based cyberviolence?

Strategies for gender transformative change in current times have to contend with an extremely tricky and shifting ground. The state, emboldened by powers of surveillance, is tightening its authoritarian control; surveillance capitalism is ceaselessly inventing business models for planetary scale exploitation of gendered bodies; and cultural norms caught in the crossfire are revalidating women's subordination by appropriating digital space. A renewed conviction, courage and creativity must inform feminist thought and action.

i Haraway, Donna J. *Simians, Cyborgs and Women: The Reinvention of Nature* (Routledge, 1991)

ii Posthumanism is a branch of technology studies which draws attention to how traditional social science theories, with their human-centric bias, cannot fully explain human action. Post-human scholars posit that social configurations be seen for the material, technological and biological assemblages that they are. See Braidotti, R. (2013). *The Posthuman*. Cambridge: Polity Press.

iii Hayles, N. Katherine. *How We Became Posthuman* (University of Chicago Press, 1999)

iv WRO global study

v This particular age group was of interest as our own previous research on gender-based cyberviolence undertaken in 2017 in Bengaluru, Karnataka, and studies in other parts of the globe suggest that young women are disproportionately prone to cyberviolence.

vi Das, Monalisa. “Online abuse of Kerala women rampant, 'pongala' used for group trolling” The News Minute. 15 July, 2015. https://www.thenewsminute.com/article/online-abuse-kerala-women-rampant-pongala-used-group-trolling-46566

vii Munusamy, Kiraba. “Intersection of identities: online gender and caste based violence” GenderIT.org. 7 June, 2018. https://www.genderit.org/articles/intersection-identities-online-gender-and-caste-based-violence

viii Munusamy, Kiraba. “Intersection of identities: online gender and caste based violence” GenderIT.org. 7 June, 2018. https://www.genderit.org/articles/intersection-identities-online-gender-and-caste-based-violence

ix Devika J., Vijayakumar Chithira, Mini Sreedhar Darshana, PS Resmi, Alexander Elizabeth. “Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala.” IT for Change and Centre for Development Studies (2019)

x J.Devika, wire

xi Vijaya, K."Role of Women in Self Respect Movement” *Proceedings of the Indian History Congress* 54. 1993. , https://www.jstor.org/stable/44143032?read-now=1&seq=2#page_scan_tab_contents

xii Geetha, V. “Periyar, Women and an Ethic of Citizenship” *Review of Women's Studies* 30:17. 1998. https://www.epw.in/system/files/pdf/1998_33/17/periyar_women_and_an_ethic_of_citizenship.pdf

xiii Karupiah, Premalatha. “Hegemonic femininity in Tamil movies: exploring the voices of youths in Chennai, India” *Journal of Media & Cultural Studies* 30:1. 2016. https://www.tandfonline.com/doi/abs/10.1080/10304312.2015.1117574?journalCode=ccon20

xiv The well-chronicled torture, abduction and killing primarily of women, but also men, by families and community governance bodies for transgressing supposed 'codes of honour'. See Baxi, Pratiskha; Rai, Shirin, M and Ali, Shaheen Sardar. “Legacies of Common Law: 'crimes of honour' in India and Pakistan' *Third World Quarterly* 27:7. 2006. https://www.researchgate.net/profile/Pratiksha_Baxi/publication/242511496_Legacies_of_common_law_'Crimes_of_honour'_in_India_and_Pakistan/links/53dfdb740cf27a7b8306c90f.pdf

xv Rajendran, Dhanya. “Regressive engineering colleges of Tamil Nadu will remain so until parents change” The News Minute. 29 September, 2015. https://www.thenewsminute.com/article/regressive-engineering-colleges-tamil-nadu-will-remain-so-until-parents-change-34751

xvi Croxson, Helen; Rowntree, Oliver et al. “Triggering mobile internet use among men and women in South Asia” GSMA. 2017. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/11/GSMA-Triggering-Mobile-Internet-Use_Web.pdf

xvii Social reform movements and emancipation of women in Karnataka: 1840-1947,

xviii Kuthar, Greeshma. “How coastal Karnataka was saffronised: The Story of rise and rise of Hindu nationalism in syncretic South Kanara” Firstpost. 7 April, 2019. https://www.firstpost.com/india/how-coastal-karnataka-was-saffronised-the-story-of-the-rise-and-rise-of-hindu-nationalism-in-syncretic-south-kanara-6363461.html

xix “Karnataka Woman Driven to Suicide, Harassed for Friendship With Man From Different Community” News Minute, 8 January , 2018, https://www.thenewsminute.com/article/karnataka-woman-driven-suicide-harassed-friendship-man-different-community-74390

xx “Karnataka Woman Driven to Suicide, Harassed for Friendship With Man From Different Community” News Minute, 8 January , 2018, https://www.thenewsminute.com/article/karnataka-woman-driven-suicide-harassed-friendship-man-different-community-74390

xxi Bhattacharjya, Manjima et al. “EROTICS: sex rights and the internet” Association for Progressive Communications. 2011.https://www.apc.org/sites/default/files/EROTICS.pdf

xxii Gupta, Kriti, “Women Have More Choice on Dating Apps As Data Shows There Are Three Men Per Women” India Times. 19 January, 2019.

xxiii Rosalind Gill

xxiv “No photos please: dating and hooking up via Grindr and notions of self-worth” GenderIT.org. 18 January, 2019 https://www.genderit.org/feminist-talk/no-photos-please-dating-hooking-grindr-and-notions-self-worth

xxv Butkowski, C. P., Dixon, T. L., & Weeks, K. “Body Surveillance on Instagram: Examining the Role of Selfie Feedback Investment in Young Adult Women’s Body Image Concerns” *Sex Roles*, 2019.

xxvi Berne, S., Frisén, A., & Kling, J. . “Appearance-related cyberbullying: A qualitative investigation of characteristics, content, reasons, and effects” *Body Image* 11:4, 2014. https://www.ncbi.nlm.nih.gov/pubmed/25194309

xxvii Udwadia, Zarah; Grewal, Baldeep and Datta, Bishaka. “Free to be Mobile” Point of View. 2019. https://sgt-57ed.kxcdn.com/wp-content/uploads/2019/03/FTBM_Web_final.pdf

xxviii https://www.natcom.org/communication-currents/managing-transgender-identity-online

xxix Hinduja, Sameer & Patchin, Justin W. “Cyberbullying researc summary” Cyberbullying Research Centre. 2011. http://cyberbullying.org/cyberbullying_sexual_orientation_fact_sheet.pdf

xxx “Internet Governance Forum 2015 Best Practive Forum on Online Abuse and Gender-Based Violence Against Women” IGF. 8 December, 2015. http://www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women/file

xxxi Mason-Bish, Hannah. “'Get yer tits out'” Why Misogynistic Street Harrassment is a Hate Crime” International Network For Hate Studies. 17 July, 2016. http://www.internationalhatestudies.com/get-yer-tits-out-why-misogynistic-street-harassment-is-a-hate-crime/

xxxii Shimizu, Aily. “Recent developments: domestic violence in the digital age: towards the creation of a comprehensive cyberstalking statute” *Berkley Journal of Gender, Law & Justice*. Winter 2013. https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1315&context=bglj

xxxiii Waling, A., & Pym, T. “C”mon, No One Wants a Dick Pic’: exploring the cultural framings of the “Dick Pic” in contemporary online publics. *Journal of Gender Studies* 1–16, 2017.

xxxiv Devika J., Vijayakumar Chithira, Mini Sreedhar Darshana, PS Resmi, Alexander Elizabeth. “Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala.” IT for Change and Centre for Development Studies (2019)

xxxvSuler, John. “The Online Disinhibition Effect” *CyberPsychology & Behaviour* 7:3, July 2004. https://www.researchgate.net/publication/8451443_The_Online_Disinhibition_Effect

xxxviSalter, M. “Privates in the online public: Sex(ting) and reputation on social media” *New Media & Society.* 18:11, 2016.

xxxviiGurumurthy, Anita. “How the online space is in crisis and what needs to be done about it” First Post. 8 March, 2019. https://www.firstpost.com/tech/news-analysis/happy-womens-day-2019-how-the-online-space-for-women-is-in-a-crisis-and-what-needs-to-be-done-about-it-6217001.html

xxxviiiSuler, John. “The Online Disinhibition Effect” *CyberPsychology & Behaviour* 7:3, July 2004. https://www.researchgate.net/publication/8451443_The_Online_Disinhibition_Effect

xxxixDevika J., Vijayakumar Chithira, Mini Sreedhar Darshana, PS Resmi, Alexander Elizabeth. “Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala.” IT for Change and Centre for Development Studies (2019)

xl Devika J., Vijayakumar Chithira, Mini Sreedhar Darshana, PS Resmi, Alexander Elizabeth. “Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala.” IT for Change and Centre for Development Studies (2019)

xli Salter, M. “Privates in the online public: Sex(ting) and reputation on social media” *New Media & Society.* 18:11, 2016.

xlii Devika J., Vijayakumar Chithira, Mini Sreedhar Darshana, PS Resmi, Alexander Elizabeth. “Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala.” IT for Change and Centre for Development Studies (2019)

xliii“Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective”, OHCHR. 14 June, 2018.

xliv Bates, S. “Revenge Porn and Mental Health” *Feminist Criminology.* 12:1, 2016.

xlv Seifullah, Annie. “Revenge Porn Took My Career. The Law Couldn't Get it Back.” Jezebel. 18 July, 2018. https://jezebel.com/revenge-porn-took-my-career-the-law-couldnt-get-it-bac-1827572768

xlvi Worsley, Joanne D. et al. “Victims' Voices: understanding the emotional impact of cyberstalking and individuals' coping responses” Sage Open. June, 2017. https://journals.sagepub.com/doi/pdf/10.1177/2158244017710292

xlviiShort, Emma et al. “The Impact of Cyberstalking: The lived experience – A Thematic Analysis” *Studies in health technologies and informatics.* 2014. https://pdfs.semanticscholar.org/56ee/7928ac1ebbcff1561fa4f3bd9a66a2c49b59.pdf

xlviii Filipovic, Jill. “Blogging While Female: How Internet Misogyny Parallels “Real-World” Harassment” Yale Journal of Law & Feminism 19:1, 2007. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1268&context=yjlf

xlix https://www.apc.org/sites/default/files/BigDataSexualSurveillance_0_0.pdf

l Born to be Digital Compendium

li Rudman, L. A., & Glick, P. “Prescriptive Gender Stereotypes and Backlash Toward Agentic Women” *Journal of Social Issues,* 57:4 2001. https://psycnet.apa.org/record/2001-05792-007

lii Pearce, K. E., & Vitak, J. (2016). Performing honor online: The affordances of social media for surveillance and impression management in an honor culture. New Media & Society, 18(11), 2595–2612. doi:10.1177/1461444815600279

liii https://www.epw.in/system/files/pdf/2002_37/43/Work_Caste_and_Competing_Masculinities.pdf

liv Devika J., Vijayakumar Chithira, Mini Sreedhar Darshana, PS Resmi, Alexander Elizabeth. “Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala.” IT for Change and Centre for Development Studies (2019)

lv https://ro.uow.edu.au/cgi/viewcontent.cgi?referer=http://scholar.google.co.in/&httpsredir=1&article=1187&context=artspapers

lvi #TheFappening: Virtual Manhood Acts in (Homo)Social Media Mairead Eastin Moloney1 and Tony P. Love, Men and Masculinities 1-21

lvii Anandhi S., Jeyaranjan J., Krishnan, Ranjan. “Work, Caste and Competing Masculinities.” Economic and Political Weekly (2002)

lviii Pearce, K. E., & Vitak, J. (2016). Performing honor online: The affordances of social media for surveillance and impression management in an honor culture. New Media & Society, 18(11), 2595–2612.

lix Mishra Smeeta, Basu Surhita. “Family honor, cultural norms and social networking: Strategic choices in the visual self-presentation of young Indian Muslim women.” Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8(2), article 3.

lx Devika J., Vijayakumar Chithira, Mini Sreedhar Darshana, PS Resmi, Alexander Elizabeth. “Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala.” IT for Change and Centre for Development Studies (2019)

lxi Palfrey, J. and Gasser, U. (2008) Born Digital: Understanding the First Generation of Digital Natives, New York, Basic Books.

lxii Gurumurthy, Anita. “How the online space for women is in a crisis and what needs to be done about it.” FirstPost. March 8, 2019.

lxiii Kabeer, Naila (1999), The Conditions and Consequences of Choice: Reflections on the Measurement of Women's Empowerment, UNRISD

lxiv Tella K. Keerthana, “ #MeToo: An International Conversation on Sexual Violence Impacting Feminist Discourse Across Borders”, Economic and Political Weekly, October 2018.

lxv Salter, M. (2013). Justice and revenge in online counter-publics: Emerging responses to sexual violence in the age of social media. Crime, Media, Culture: An International Journal, 9(3), 225–242

lxvi Devika J., Vijayakumar Chithira, Mini Sreedhar Darshana, PS Resmi, Alexander Elizabeth. "Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala." IT for Change and Centre for Development Studies (2019)

lxvii"Boys should not tke elfies with girls: Police warns", Mathrubhumi (2018)

lxviii The Madurai Bench of the Madras High Court is hearing a public interest litigation seeking a prohibition on Tiktok downloads. In fact, as part of its interim orders in the petition, the Court had briefly banned Tiktok for a short period of time.

lxix Navtej Singh Johar and Ors. v. Union of India, Ministry of Law and Justice, (2018), WP(Crl.)No.76/2016 (Supreme Court 2016)

lxx Vasudevan Amrita , Gurumurthy Anita, Chami Nandini, "Law enforcement agencies' perceptions of gender-based cyber violence – An ethnographic exploration of Bengaluru city cyber police". IT for Change (2018)

lxxi Ramaseshan Geeta, Ramasamy Sudaroli, Sangeetha M.R., Prabha S., Krishna Nandita and Kumar Shreeja. "A report on gender-based cyberviolence in Tamil Nadu." (2019)

lxxii Government of India, Ministry of Homa Affairs. " CCPWC scheme-capacity building courses for Police Officers, Prosecutors & Judicial Officers". February 2018, https://mha.gov.in/commoncontent/sites/default/files/5%20capacity_building_advisory-2-2-18_09022018%20(4).pdf

lxxiii Devika J., Vijayakumar Chithira, Mini Sreedhar Darshana, PS Resmi, Alexander Elizabeth. "Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala." IT for Change and Centre for Development Studies (2019)

lxxiv Gurumurthy Anita, Vasudevan Amrita, Chami Nandini and Mahesh Sarada. "A report on gender-based cyberviolence in Karnataka." IT For Change (2019)

lxxv Ramaseshan Geeta, Ramasamy Sudaroli, Sangeetha M.R., Prabha S., Krishna Nandita and Kumar Shreeja. "A report on gender-based cyberviolence in Tamil Nadu." (2019)

lxxvi Shreya Singhal v. Union of India, (2015), (Supreme Court 2015)

lxxvii "Under s. 199, Cr.P.C., no Magistrate can take cognizance of an offence falling inter alia under Chapter XXI, I.P.C., that is, sections, 499 to 502 except on a complaint made by some persons aggrieved by such offence. The section is mandatory, so 'that, if a Magistrate were to take cognizance of the offence of defamation on a complaint filed by one who is not an aggrieved person the trial and conviction of the accused would be void and illegal." G. Narasimhan & Ors. Etc v.T. V. Chokkappa 1972 AIR 2609

lxxviii Mandhani, Apoorva. "Posting comments about ill treatment by Police on their FB page may not amount to assault (S.335 IPC) or criminal intimidation (S.503 IPC): SC." *Live Law* (2015)

lxxix Amulya Kumar Behera v. Nabaghana Behera (1995), 1995 CriLJ 3559 (Orissa High Court 2015)

lxxx Kanshi Ram v.. State (2000), 2000 IVAD Delhi 495, (Delhi High Court 2015)

lxxxi Gurumurthy Anita, Vasudevan Amrita, Chami Nandini and Mahesh Sarada. "A report on gender-based cyberviolence in Karnataka." IT For Change (2019)

lxxxii Khanna, Akshay. "Case Note on The state Cyber Cell v Yogesh Pandurang Prabhu." Legal Services India.

lxxxiii "Session 4. Taking positions within and vis-a-vis institutions: interpreting the law, negotiating the law". IT for Change. https://itforchange.net/e-vaw/session-4/ (2019)

lxxxivGeeta Ramaseshan, Sudaroli Ramasamy, M.R.Sangeetha, S.Prabha, Nandita Krishna and Shreeja Kumar. "A report on gender-based cyberviolence in Tamil Nadu." (2019)

lxxxv"Kerala: Police arrest man accused of morphing women's photos for pornography". Scroll.in. April 4, 2018

lxxxvi A copy of the Cyber Crime Investigation Manual developed by private body DSCI can be accessed here- https://uppolice.gov.in/writereaddata/uploaded-content/Web_Page/28_5_2014_17_4_36_Cyber_Crime_Investigation_Manual.pdf. The police personnel we interviewed refused to share a copy of the Karnataka Police Standard Operating Procedure with us.

lxxxviiJ. Devika, Chithira Vijayakumar, Darshana Sreedhar Mini, Resmi PS, Elizabeth Alexander. "Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala." IT for Change and Centre for Development Studies (2019)

lxxxviii
Shahfi Mohammad v. The State of Himachal Pradesh (2018), SLP (CRL.) No.2302 of 2017, (Supreme Court 2018)

lxxxix Shahfi Mohammad v. The State of Himachal Pradesh (2018), SLP (CRL.) No.2302 of 2017, (Supreme Court 2018)

xc J. Devika, Chithira Vijayakumar, Darshana Sreedhar Mini, Resmi PS, Elizabeth Alexander. "Walking on Eggshells in Cyberspace: A report on gender-based cyber violence in Kerala." IT for Change and Centre for Development Studies (2019)

xci Geeta Ramaseshan, Sudaroli Ramasamy, M.R.Sangeetha, S.Prabha, Nandita Krishna and Shreeja Kumar. "A report on gender-based cyberviolence in Tamil Nadu." (2019)

xcii Amber Sinha, Elonnai Hickok, Udbhav Tiwari and Arindrajit Basu, "Cross Border Data-Sharing and India: A study in process, content and capacity." Feb 2016

xciii Bedavyasa Mohanty & Madhulika Srikumar, "Making India-US data sharing work." August 2017.

xciv Gurumurthy Anita, Vasudevan Amrita, Chami Nandini and Mahesh Sarada. "A report on gender-based cyberviolence in Karnataka." IT For Change (2019)

xcv Lapidot-Lefler, N., & Barak, A. 2015. The benign online disinhibition effect: Could situational factors induce self-disclosure and prosocial behaviors?. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 9(2), article 3. http://dx.doi.org/10.5817/CP2015-2-3

xcvi Massanari, Adrienne (2015) "#Gamergate and TheFappening: How Reddit's algorithm, governance, and culture support toxictechnocultures", New Media and Society, 19(3)

xcvii https://www.genderit.org/articles/intersection-identities-online-gender-and-caste-based-violence

xcviii Sivenbring, Jennie, Siekkinen, Frida. "R-E-S-P-E-C-T! Feminine respectability and sexuality for young women online." First Monday, 24(1)

xcix Ambjörnsson, 2004. "I en klass för sig. Genus klass och sexualitet bland gymnasietjejer [In a class of their own. Gender, class and sexuality among girls in upper secondary school]," doctoral thesis, Stockholm University, Faculty of Social Sciences, Department of Social Anthropology, at https://www.adlibris.com/se/bok/i-en-klass-for-sig-genus-klass-och-sexualitet-bland-gymnasietjejer-9789170370274, 2018

c Rayaprol, A., & Ray, S. 2010. "Understanding Gender Justice." Indian Journal of Gender Studies, 17(3), 335–363.

ci Phadke, Shilpa. "Thirty Years On Women's Studies Reflects on the Women's Movement". Economic and Political Weekly, October 2003.

cii Bakshi, Garima. 2017. "The 'Nirbhaya' Movement: An Indian Feminist Revolution." Gnovie journal. 17(2)

ciii Hampton, J. (1998). Punishment, Feminism, and Political Identity: A Case Study in the Expressive Meaning of the Law. The Canadian Journal of Law and Jurisprudence, 11(01), 23–45

civ Robin L West, The Difference in Women's Hedonic Lives: A Phenomenological Critique of Feminist Legal Theory

cv Danielle K. Citron, Law's Expressive Value in Combating Cyber Gender Harassment, 108 Mich.L. Rev.373 (2009)

cvi Gagan Harsh Sharma And Anr v. The State Of Maharashtra And Anr (2018) (Bombay High Court 2018)

cvii "Session 4. Taking positions within and vis-a-vis institutions: interpreting the law, negotiating the law". IT for Change. https://itforchange.net/e-vaw/session-4/ (2019)

cviii

cix Aveek Sarkar & Anr v. State Of West Bengal And Anr (2014), (Supreme Court of India 2014)

cx In the landmark anti-pornography decision *Butler v. Her Majesty the Queen*, the Canadian Supreme Court had observed, "*what is obscene is what harms women, not what offends [a community's] values*", thus underscoring a feminist interpretation of obscenity.

cxi Law Commission of India. "Hate Speech". Report No. 267 (2017)

cxii Henry N., Powell A. "Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence, Violence against women." Violence Against Women 21 (6)

cxiii Danielle K. Citron, Law's Expressive Value in Combating Cyber Gender Harassment, 108 Mich.L. Rev.373 (2009)

cxiv Fraser, Nancy (2008). "Abnormal justice." Yale Law Journal.

cxv Henry N., Powell A. "Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence, Violence against women." Violence Against Women 21 (6)

cxvi Facebook, for instance, has allowed users to lock their display pictures, making their download more difficult. It has also introduced hashing technology that could help women prevent the viral spread of their intimate images, similar to what is already being used to pull down child pornography. Twitter has introduced design features that hide the tweets of key public-political figures/influencers that violate the platform's rules on abuse, harassment and incitement. See https://www.facebook.com/help/community/question/?id=624794050887965 and https://www.bbc.com/news/technology-48791094

cxvii Shieber, Jonathan. 2019. Tech Crunch. "Facebook releases community standards enforcement report." May 23, 2019. https://techcrunch.com/2019/05/23/facebook-releases-community-standards-enforcement-report/

cxviii Shieber, Jonathan. 2019. Tech Crunch. "Facebook releases community standards enforcement report." May 23, 2019. https://techcrunch.com/2019/05/23/facebook-releases-community-standards-enforcement-report/

cxix Network enforcement directive

cxx Sexual Assault and Harassment: A Campus Community Case Study Author(s): Bernice Lott, Mary Ellen Reilly and Dale R. Howard Source: Signs, Vol. 8, No. 2 (Winter, 1982), pp. 296-319

cxxi Brown, C. (2008). *Gender-Role Implications on Same-Sex Intimate Partner Abuse. Journal of Family Violence, 23(6), 457–462.*doi:10.1007/s10896-008-9172-9

cxxii www.cybercrime.gov.in/cybercitizen/home.htm

cxxiii Penney, Jon. 2017. "Can cyber harassment laws encourage online speech?" Medium. (Aug 2017)

cxxiv Government asks Law Commission to look at trolling laws. (Feb 2018). https://www.lawcom.gov.uk/government-asks-law-commission-to-look-at-trolling-laws/

cxxv "Singapore outlaws 'revenge porn', 'cyber-flashing'". 2019. The Jakarta Post. (May 2019)

cxxvi Kilpatrick, Alan. 2018. "Saskatchewan's New Revenge Porn Law". Legal Sourcery (Dec 2018).

cxxvii Stevens, Yuvan. 2017. "'Revenge Porn,' Tort Law, and Changing Socio-Technological Realities: A Commentary on Doe 464533 v ND." Canadian Journal of Law & Technology, Vol. 15, 2017.

cxxviii Robertson, Adi. 2017. "A new internet safety bill would ban swatting, doxxing, and sextortion all at once." The Verge (June 2017)

cxxix India has signed MLATs with 39 countries.

cxxx "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians" Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018)

cxxxi "Communication on Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms". European Union (2017). https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms

cxxxii Gurumurthy, Anita. Vasudevan, Amrita. Chami, Nandini. "Examining technology-mediated violence against women through a feminist framework: Towards appropriate legal-institutional responses in India." IT for Change (Jan 2018)

cxxxiii Vasudevan Amrita , Gurumurthy Anita, Chami Nandini, "Law enforcement agencies' perceptions of gender-based cyber violence – An ethnographic exploration of Bengaluru city cyber police". IT for Change (2018)

cxxxiv Newman, Caroline . "Hiring female police officers helps women report violence, sexual assault, study finds." Phys.org (Sept 2018).

cxxxv Govt of India, Ministry of Home Affairs. "Cyber Crimes Portal." https://cybercrime.gov.in/cybercitizen/home.htm

cxxxvi Personal communication of authors with Vaishali Bhagwat, Advocate and Cyberlaw expert.

cxxxvii University Grants Commission, Regulations. 2016. (Ind) https://www.ugc.ac.in/pdfnews/7203627_UGC_regulations-harassment.pdf

cxxxviii HM Government. 2019. "Online Harms White Paper." (Apr 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

cxxxix These however may not be enforceable but only recommendatory as it involves developing technological devices.

cxl https://indiankanoon.org/doc/147162512/, https://indiankanoon.org/doc/192654466/

cxli Rule 3(9)

cxlii See submission by DEF, IFF, AccessNow, CIS, SFLC, https://meity.gov.in/comments-invited-draft-intermediary-rules; Mixed Messages?
The Limits of Automated Social Media Content Analysis, https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf

cxliii Cite special rapporteur

cxliv https://transparency.facebook.com/community-standards-enforcement, https://www.fastcompany.com/4013603/youtube-is-using-ai-to-police-copyright-to-the-tune-of-2-billion-in-payouts

cxlv https://www.firstpost.com/tech/news-analysis/happy-womens-day-2019-how-the-online-space-for-women-is-in-a-crisis-and-what-needs-to-be-done-about-it-6217001.html