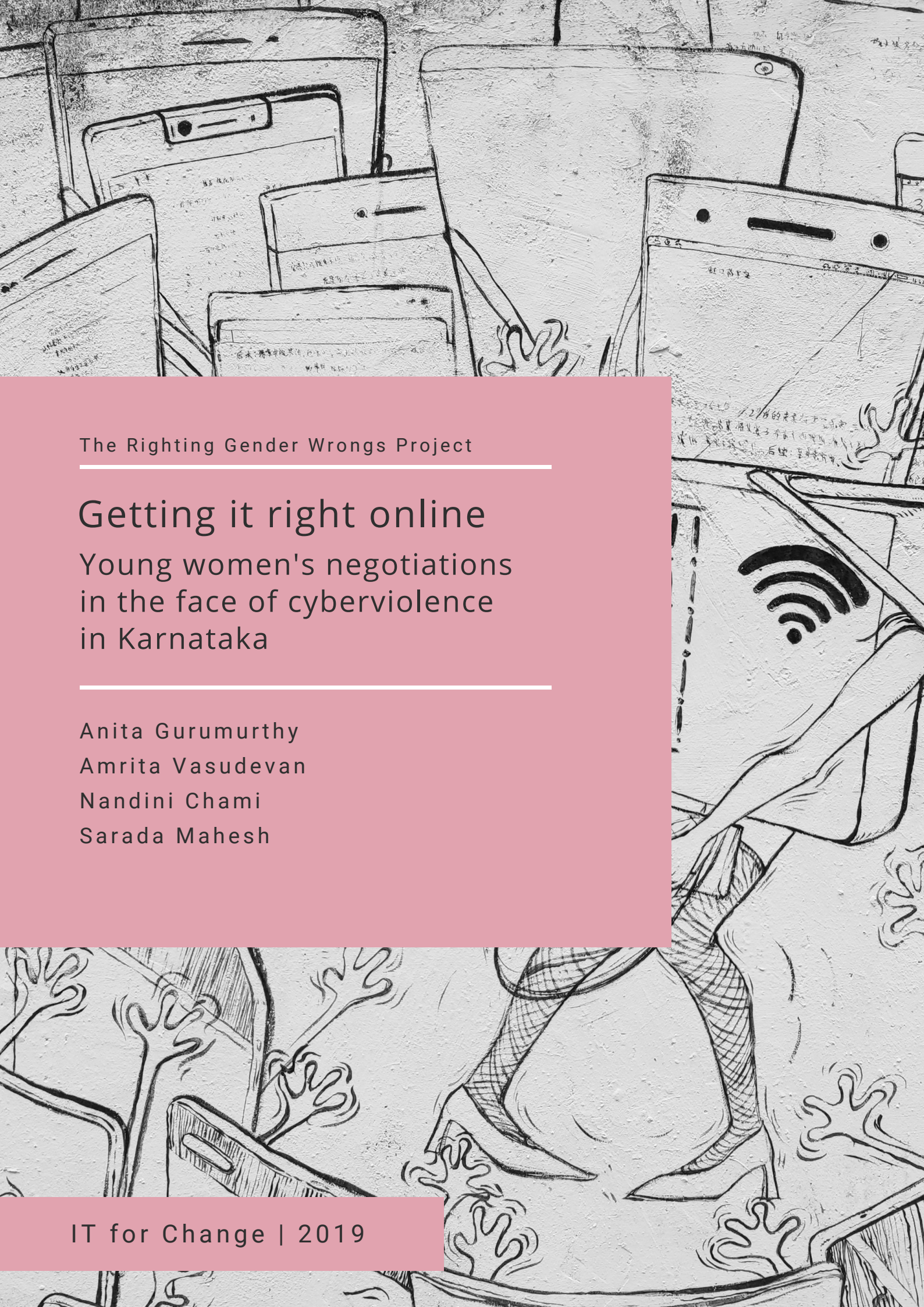

The Righting Gender Wrongs Project

Getting it right online

Young women's negotiations in the face of cyberviolence in Karnataka

Anita Gurumurthy
Amrita Vasudevan
Nandini Chami
Sarada Mahesh

IT for Change | 2019

Authors

Anita Gurumurthy, Amrita Vasudevan, Nandini Chami, Sarada Mahesh

Research coordination team

Principal Investigator: Anita Gurumurthy
Co-investigators: Amrita Vasudevan, Nandini Chami
Research Assistance: Sarada Mahesh
Design: Meenakshi Yadav

Getting it right online

Young women's negotiations in the face of cyberviolence in Karnataka

Page left intentionally blank

Table of Contents

1. Introduction

This is the report of an exploratory field research on the machinations of gender-based cyber violence, carried out in 2 locations in the state of Karnataka between October 2018 to January 2019. The study was undertaken as part of a larger multi-site research, 'Righting gender wrongs: a feminist socio-legal enquiry into online sexism, misogyny and gender-based violence', led by IT for Change and supported by Web Foundation to map emerging typologies of cyberviolence and the effectiveness of prevailing legal-institutional responses to the issue in India.[i]

The point of departure for this research is that for today's young adult, the internet is no longer uncharted territory to be discovered ; it is a natural abode, an integral part of her socialization. The 'born digital' generation does not distinguish between online and offline identities, as their quest for individuation revolves around a simultaneous and seamless navigation of a digital sociality where the boundaries between the 'online' and 'offline' have collapsed. With pervasive digitalization and datafication of everyday life, the resultant traceability of past identities and fluidity between private and public identities present challenges for managing social identity.[ii] It is the experiences of this generation that this research study is primarily concerned with; young adults for whom digital encounters are a 'rite of passage' irrespective of socio-economic location. For these digital natives, there is no binary between cyberspace and real space. But neither is cyberspace a mere extension of real space. Instead, there is a new social space, "the interpenetration of embodied, formerly bounded space by networked space".[iii]

The study of social phenomena today has to account for the inevitable enmeshing of the offline and online. Affordances of virtualization, horizontalization, asynchronicity and anonymity in digitally mediated social spaces not only open up possibilities for subversion of dis-empowering gender norms, but also shape the structures of gender-based violence. Data trails of location and status information have aided surveillance and stalking.[iv] Intimate partner violence is also noted to be enabled by technological affordances.[v]

This report captures the experiences of 335 women in the state of Karnataka and presents an in-depth account of current legal-institutional frameworks, recommending changes needed for access to justice for survivors.

2. Methodology of the study

This study adopted a mixed research methodology, comprising the following specific methods:

(1) A self-administered survey with 335 female college students in the age group of 19 to 23 years from 4 colleges in two cities of Karnataka, Bengaluru and Mysuru. The survey was anonymous and the responses voluntary. It focused on mapping how communication technologies are used by young women; the experiences they have

online; if they have experienced harassment and how it impacts them; and whether, and from whom, they seek help when faced with such a situation. Colleges were selected to include a diverse student cohort, even though the sample was not strictly representative of the demographic of Internet users pursuing higher education in Karnataka. Survey results were used to zero in on the prongs for qualitative research and to corroborate qualitative findings.

(2) Two Focus Group Discussions with female college students and two with male college students, in the age group of 19-23 years, in Bengaluru and Mysuru. There was no overlap between the survey cohort and the participants in the focus group discussion, in order to limit privacy risks. The focus group discussions focused on examining why young men and women use the Internet and what they do once online, what risks are perceived by young women accessing the Internet, and if and how social interactions online potentially normalize gender stereotypes and gender-based violence.

(3) Semi-structured interviews with the following stakeholders:

- Six police officials of varying ranks, including those dealing with cyber crimes. Interviewees were selected through snowballing
- Lawyers – two from an organization in Bengaluru that provides legal services to marginalized groups and undertakes socio-legal research, and one independent lawyer who practices primarily at the family courts in Bengaluru
- A counsellor providing crisis support to women who have faced violence
- A dalit rights activist who is also a teacher at a local college in Bengaluru
- A medical professional who works with an organization for adolescent and child health and runs a project for counselling young adults who face cyber bullying and harassment
- A women's rights activist and a dalit rights activist who campaigned for safer online spaces,
- Two women journalists who have experienced cyberharassment.[vi]

All interviews were face-to-face, except one, which was telephonic. The interviews were on average half an hour to an hour long.

(4) Review of existing literature examining legal, institutional, cultural, and technological dimensions of gender-based cyberviolence.

3. Research context and profile of research participants

Karnataka state has high tele-density[vii] and also records high levels of cyberviolence,[viii] and relatively average level of violence against women.[ix] In February 2019, media reports indicated that over 60% of complaints lodged at the Karnataka State Women's Commission pertain to harassment of women via social media.

Bengaluru, the capital city of Karnataka is a metropolis, often referred to as the Silicon Valley of India for its large concentration of IT companies. The city attracts students from various parts of the country who come for higher education. Reports of cybercrimes from Bengaluru have found their way into the mainstream press for several years. The city also has a fairly well-developed police response to cybercrimes, housing the state level cybercrime police station that has jurisdiction to investigate such offences, across the entire state. Mysuru is a prominent urban centre in Karnataka, which became a metropolis in 2017. The high level of road and rail connectivity and the presence of many reputed higher education have led to the city becoming a popular destination for students from hinterland districts.

Respondents from the survey were from four colleges; one from Bengaluru and three from Mysuru (Appendix 1, Table 1.3). Nearly two-thirds of the respondents were between the ages of 21-23 (Appendix 1, Table 1.1). A majority of the respondents are Hindu (82.08%). 6.56% are Christians, 7.16% are Muslim and there were four Jains and four Buddhists.[x] 60.89% of the respondents belong to General Caste category, 26.26% to Other Backward Castes, 5.07% to Scheduled Castes and 4.77% to Scheduled Tribes (Appendix 1, Table 1.5 and1.6).[xi] 79.70% of survey respondents identified as heterosexual (Appendix 1, Table 1.8). Across colleges, students seemed confused about the question on sexual orientation, and in two colleges (one in Mysuru and one in Bengaluru), a few students seemed uncomfortable when clarification was provided by the survey administrators.

33.22% of the respondents own a mobile phone that costs < 10,000 INR, 32.30% own phones that are in the price range of 10,000-15000 INR, 16.92% in the price range of 15,000-20,000 INR and 17.53% in the price range of > 20,000 INR (Appendix 1, Table 2.2). Also, those who own mobile phones costing more than 10,000 INR reported replacing their phones more often than those who own mobile phones less than 10,000 INR (Appendix 2, CrossTab 2). The cost of mobile phone seems to be a good proxy for the economic class of the respondent, with the majority hailing from upper class groups.

Over 97% of respondents use their own mobile phone, and 2% use someone else's mobile phone (Appendix 1, Table 2.1). 81.19% reported to accessing the Internet from their own phone using a mobile data pack (Appendix 1, Table 2.8). The main purposes for which respondents used the Internet included – communication with friends and family (91.94%), seeking information on matters that cannot be discussed with family or friends (91.61%), and for college work and assignments (91.64%). 23.5 % of the students revealed that they use the Internet to make new friends and relationships and only 10.21% stated that they used the Internet to seek information on sexuality and 3.28% said they have shared intimate pictures online with their partners. (See Appendix 1, Table 2.10).

The sensitivity of disclosure of sexual behaviour may have prevented more students from revealing such aspects of use. Previous research documenting Internet use among young women in the city of Mumbai has also

commented on the fact that very few women reported accessing anything on the internet related to sexuality, with some women even reporting that accessing sexual content is immoral.[xii]

Communication online predominantly takes place in English and Kannada (Appendix 1, Table 1.2). Platforms that are frequently used include WhatsApp (92.53%), YouTube (70.14%), Instagram (68.95%), and Facebook (53.73%).[xiii] 62.38% of the respondents use SMS and only six respondents reported to using dating apps (Appendix 1, Table 2.12), a figure that again seems to reflect underreporting owing to social disapproval.

The use of messaging and social media platforms such as WhatsApp and Instagram is predictably high as most students use the Internet to communicate with family and friends. On the other hand, only 8.65% of respondents use Twitter, a platform that has traditionally been more political and less frequently used for communication among peers. A significant percentage of Twitter users, in a study lead by the Pew Centre, reported that half their feed comprises political posts.[xiv] Facebook and Twitter are more commonly used for information sharing compared to other platforms like Instagram and Snap-chat.[xv] The patterns of use of platforms generally fall/fit into the affordances that their techno-design privileges. Though only 6 respondents said that they use dating apps, this however, does not foreclose the possibility that young women use traditional social media apps such as Facebook, rather than commercial dating apps, to seek out intimate partners and relationships.[xvi]

The subsequent sections of this report summarize the main findings and insights from the research study. Section 4 maps women's experiences of gender-based cyberviolence and its differential impacts on women from across various social locations. Section 5 unpacks the legal response to gender-based cyberviolence, discussing shortcomings/gaps in the law, and also explores how evidence collection and jurisdictional conflicts play out in such instances. Section 6 maps women's perceptions of institutional redress for cyberviolence, and brings in perspectives of survivors, women lawyers and crisis support counselors about the responses of police, courts, and internal committees set up in educational institutions and workplaces to redress sexual harassment. Section 7 discusses how technological architecture – in particular, design choices of digital platforms – molds user behaviour, and in some cases, aggravates misogyny, raising pertinent issues about their accountability and liability. Section 8 concludes the report by summarizing the main findings and proposing critical recommendations on evolving a comprehensive response to tackling gender-based cyberviolence.

4. Experiences of survivors: vulnerability, harm and agency

A little over one-third of the respondents to our survey reported that they had faced some-form of cyberharassment in the past year (Appendix 1, Table 4.1).[xvii] One-third also reported knowledge of another woman (family, friend or acquaintance) experiencing harassment online (Appendix 1, Table 4.9). Half of the 123 respondents who reported facing some form of cyberharassment in the past one year were harassed multiple times (Appendix 1, Table 4.4) and over two-thirds identified their harasser as male (Appendix 1, Table 4.6). One-

third reported that they had been harassed by only one person (in single or multiple instances), another one-third that they had confronted multiple harassers (at the same time or at different times), while most of the remaining were not sure about the identity of the harasser (Appendix 1, Table 4.5).

Gender-based cyberharassment defies easy categorization within the syntax of existing laws. For the purposes of this research, gender-based cyberviolence was classified into three broad sets of violations that women face online. The first is identity-based trolling or bullying, wherein identity markers such as caste, sexual orientation, religion, gender, etc. or physical features – weight, body shape, skin colour, etc. – are attacked. The second pertains to acts of sexual harassment, such as circulation of a woman's morphed photo online, sending unsolicited, sexually explicit messages and pictures, doxxing, non-consensual circulation of intimate images, sextortion and so on. The third includes cyberstalking, which usually involves unwelcome advances, including incessant messaging online. For the purposes of the survey, the second and third kinds of harassment were combined.

4.1. Kinds of gender-based cyberviolence experienced by women

4.1.1 Trolling

75% of the respondents who faced cyberbullying were attacked or bullied for their social identity or physical attributes. They were subjected to body shaming, with negative comments about body shape (38.21%), weight (37.39%), skin colour (19.51%), or looks (39.83%) (Appendix 1, Table 4.11). Six of the 24 respondents who reported being attacked on the basis of skin colour belong to marginalized caste groups.

A dalit rights female activist we spoke to recounted the abuse faced by a friend who posted a video critical of the #MeToo movement in India from the perspective of a dalit woman. The abuse she was subject to specifically attacked her for her skin colour and her looks. As the key informant recounted:

> 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?

15 respondents reported that they had been attacked or bullied on the basis of their sexual orientation and 3 said that they continue to be attacked for the same.

More respondents admitted to knowing of other women who have faced identity-based harassment or trolling when compared to those reporting personal experiences in this regard. Although only 7 respondents answered that they have personally been bullied based on their caste, 36.93% knew of other women who were harassed

online because of caste. Similarly, while only 9 reported to have been attacked online for their religious background, 23.42% reported knowing another woman who had faced such an attack (Appendix 1, Table 4.11).[xviii]

The fact that caste or minority religious identity is reported as the object of trolling and often accompanies sexualized, gender-based trolling is a critical concern. Anecdotal evidence in popular media shows how this tactic is used to intimidate women who are vocal online.[xix] Journalists we interviewed spoke of their experiences of being trolled incessantly and concertedly by multiple handles at once in response to tweets or messages posted on their social media. The harassment of Rana Ayyub, a journalist who has written extensively on the 2002 Gujarat riots was widely reported by national media. Fake tweets defending child rapists and alleging that Muslims in India were no longer safe were falsely attributed to her. Along with the barrage of death threats and sexual violence, her Muslim identity was invoked in order to harass and discredit her.[xx] Late last year, prominent student-leader-turned-politician, Shehla Rashid quit Twitter briefly when she felt she could not deal with the scale of violence online. As a Kashmiri, Muslim woman, she stated that she "ticked all the wrong boxes", making her an easy target of organized cyberviolence.[xxi] Kiruba Munusamy, an advocate in the Supreme Court of India, writing on caste identity and online violence observes that unlike upper caste women, dalit women encounter caste-based violence along with sexual violence online.[xxii] The abuse often takes the shape of criticism of choices (especially consumption of meat) to deride caste based cultures.[xxiii] When being trolled, as with the case of a survivor we interviewed, pictures of the woman eating meat may be pulled up to allege religious betrayal and drum up anti-national claims.

4.1.2 Sexual harassment online

60.97% of the respondents who reported that they have faced cyberharassment have been doxxed, that is, personal details like their phone number and address have been made public without their consent. There have been instances where a fake profile of them was created online using their personal information (Appendix 1, 4.12).

A respondent from the survey reflected:

> An anonymous person put up my picture as his Facebook profile picture. He had no rights to do so. I felt abused and afraid.

Doxxing and identity theft when directed at women usually involved insinuations of sexual solicitation. 42.27% also reported that sexually explicit images or videos were sent to them without their volition (Appendix 1, Table 4.12). The following voices from the survey shed light on the pervasiveness of the problem of unwanted contact/attention online.

> During the initial stages when I joined Facebook, I used to receive a lot of messages from people 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.

> There was a guy online who kept sending nudes to me and asked me to do the same. He even video called me and was completely nude when he did.

A journalist we interviewed noted that while both male and female journalists are harassed, the kind of harassment female journalists face tends to be sexual in nature. This has been corroborated by multiple studies.[xxiv]

These findings assume significance given the lack of adequate and appropriate legal provisions that victims could use to seek redress. (This has been elaborated in Section 5 of the report, dealing with the law). During the FGDs, female college students shared how when sexist content is forwarded to them or how when they come across such content on Facebook, they choose to ignore it for speaking up could make them vulnerable to attack. In fact, some participants thought that a face to face confrontation may be better, although they did not report adopting this route.

11 survey respondents reported receiving blackmail messages that threatened the release of their sexually explicit image or video if they did not extend sexual favours. 5 had been approached by individuals forcibly demanding sexual favours in exchange for not releasing the sexually explicit image/video of the respondent in their possession.

In the words of one respondent from the survey:

> [I] was in a relationship which my parents did not approve, and so I had to break it off. When he finally agreed to the breakup, [he] demanded 42,000 [INR]. He blackmailed me, saying that he would post my nude pics if I did not pay up.

Although, and expectedly, 84.47% of survey respondents answered in the negative when asked if they have experienced non-consensual circulation of their intimate images, 23 reported knowledge of another woman who has faced such harassment. Only one person admitted that a sexually explicit image or video of her from a past relationship was put online without her knowledge or consent. Similarly, while only 3 revealed that a sexually explicit image of them was captured without their knowledge, 17 answered that they knew another woman it had happened to. A respondent from the survey said:

> When my friend and her boyfriend had sex, he took a video of them without her knowledge. After their breakup, he used to blackmail her with the video and call her again and again just for sex.

It is likely that respondents were not comfortable talking about such violations because of the social disapproval attached to casual/pre-marital sexual relationships. Key informants in the police observed that most cases of gender-based cyberviolence pertained to misuse of photos (likely to be morphing), non-consensual circulation of intimate images, and sharing of telephone numbers without the knowledge of the woman, usually by a jilted ex-boyfriend. A police officer we interviewed, noted:

> With respect to gender-based cybercrimes against women, the cases mostly relate to obscene pictures being put up on the internet without their consent. The platforms that these mostly take place on are Facebook and WhatsApp (where their friends can see the pictures). There are also cases of original or morphed pictures being put up on porn websites. Both intimate partner violence and stranger violence occur on platforms like Instagram and Twitter.

4.2. Stranger violence vs. intimate partner violence

33.33% of respondents stated that the perpetrator was someone known to them; mainly, family members (36.20%), friends (46.55%) and neighbours (32.75%) (Appendix 1, Table 4.7 and 4.8). Police officials we interviewed pointed out that in a majority of cases of gender- based cyberviolence that they encounter, the harasser is someone who is known to the woman, usually someone she has been romantically involved with. And in such cases of known abusers, as was observed by a lawyer we interviewed, women are often reluctant to take legal action.

Stranger violence tends to manifest in the form of trolling. Gendertrolling (a sub-set of trolling) tends to be a concerted act by hundreds of trolls who come together to intimidate and overwhelm the victim through insults, particularly gender slurs and threats of violence spanning long periods, and is usually a reaction to women speaking out.[xxv] Group attacks of this nature tend to distribute moral liability and displace accountability.[xxvi] The survivors we spoke to seemed to suggest that trolling which was usually perpetrated by a stranger or anonymously is an organized activity that receives political patronage as well as monetary support. Describing a troll who was nabbed by the police, a survivor told us:

> He doesn't have any smart phone, 2G, 4G all that. He only gets an hour off in the afternoon, goes to the internet cafe and does these things.

Another survivor reflected:

> I know many college kids who are paid about Rs. 10000 per month for commenting and circulating false news.

In stranger violence, the fact that the harasser could be anonymous adds to the hurdles in prosecuting these crimes.

4.3. Impact of and response to gender-based cyberviolence

While calling for online crimes to be taken as seriously as offline crimes, there is a tendency to rely on the possibility of offline impacts. Credibility of the online crime, however, need not and should never be tethered to actual physical harm.

Psychological harm, for instance, can be debilitating and have severe offline consequences on mobility. 41.46% of the respondents who faced harassment, abuse, or unwanted behaviour online reported that they continue to feel scared for their safety and security as well as that of their loved ones as a consequence of the harassment they faced online. 43.08% reported that they felt depressed, 41.46.% felt alone and helpless, 34.95% distanced themselves from friends and family and 30.89% attempted to harm themselves (Appendix 1, Table 5.1).[xxvii] A psychologist who works with young women, interviewed for this research, confirmed this:

> The immediate impact [of gender-based cyberviolence] would be going into depression, dipping of grades, self blame and sometimes even suicidal tendencies. They (women) may also feel a sense of shame, guilt and betrayal.

Research studies on the effects of non-consensual circulation of intimate images – often referred to as 'revenge porn' – usually by an ex-partner, as an act of revenge, have found that survivors feel suicidal tendencies and feelings of depression and anxiety and sometimes, even, post-traumatic stress disorder. Loss of control, lack of confidence, and decreased self-esteem may also result.[xxviii]

In addition to negative psycho-social ramifications, harm from gender-based cyberviolence should also be understood as including the violation of the right to dignity and privacy of women, rather than narrowly focusing on the consequences of the act. Powell uses Fraser's theory of 'misrecognition' to refine current conceptualizations of harms of technology-facilitated sexual violence against women. She argues that if technologically-facilitated sexual violence is understood to be 'misrecognition', that is a form of social subordination that prevents full civic participation of individual group members, it will become possible to move beyond individualized framings of the issue and account for the collective harm stemming from the reproduction of women's subordination in a patriarchal digital cultural order.

4.3.1 Chilling effect of violence

36.58% of survey respondents who have faced online harassment reported that they continue to be scared to post or share messages, images, photos, videos/audios online. 14.63% reported deleting their social media account (Appendix- 1, Table 5.1). Even women who have not directly faced harassment but are acquainted with cases of cyberviolence in their circle of friends/acquaintances reported a change in their online behaviour. 56.75% of such respondents reported exercising greater caution with respect to their own social media participation because of the negative experiences of others.[xxix] Survivors of online violence often tend to resign themselves to self-censorship, as testified to by other studies.[xxx]

One of the coping strategies that women active in public-political life exercise under these circumstances is to tailor online visibility. Key informant interviews with women journalists revealed that consequent to experiences of cyberattacks they have had to carefully manage their private and public identities. One way in which this was

done was through multiple social media profiles: a closed profile to share intimate details of their lives, and a public one that is more impersonal and also less regularly updated.

For young women who are still in the process of leveraging the Internet in their journeys of self-discovery and coming into their own as political actors, the effects of cyberviolence are far more chilling. The response seems to be one of re-alignment to public participation, a state of withdrawal and quiescence, as suggested by the following response from a female participant in the focus group discussion:

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

Amnesty International's study on online violence against women on social media platforms revealed that of the 4000 women polled across eight countries, 32% stated that they stopped posting content on social media.[xxxi] When trolls threaten harm to one's loved ones, the silencing is immediate. One woman journalist interviewed for this research said that after trolls mentioned that they knew the whereabouts of her son, she shut down her Facebook account and stopped commenting on political issues.

While online attacks in isolation may not seem like much, when harassment is continuous, even if minor, the resultant mental trauma can be immense. Such abuse can also feed into other psychological insecurities, leading to a downward spiral. Tantamount to 'death by a thousand cuts', every hurtful attack in a continuous stream of incessant harassment can be, as Zoe Quinn puts it, a "snowflake in an avalanche".[xxxii] A women's rights activist who we interviewed for this research observed:

> Men say things like, "See, I just called a woman ugly. That doesn't make me a criminal." But if a woman who goes online on Twitter gets called "ugly" every day, you have to understand the kind of effect it has on her psychologically and emotionally. It's not just that one comment. It is the fact that she has to suffer every day because of this that it becomes a problem.

The women we spoke to in the FGD, while admitting that they are sent sexist memes by their friends and classmates, told us they laughed it off' because they know "the men don't really mean it when they send those messages". The misattribution of sexism in everyday cultures of social interaction as benign acts also extends to intimate communication on social media. Women may not stand up against what they receive or what is pushed at them non-consensually.

Encouragingly, not all women choose to stay away from active online engagement. Some do not give up. They fight it out, as a survey respondent observed:

> My friend had argued with a guy regarding a feminist issue in her college. Later, the same day he sent her emails threats which said that he would soon sexually abuse her. However, this stopped after she posted his emails on social media, and he received a lot of hate.

It is important that we don't see women only as passive recipients of violence. Women often turn to humour and satire, by appropriating symbols of the internet, like memes, as a strategy to resist and engage with harassers online, as well as raise awareness about gendered harassment with a wider online community.[xxxiii] This however, should not mean that the burden to fight cyberviolence is placed only on women.

4.3.2 Impacts on reputation and livelihood

Reputational harm was brought up in our focus group discussion with women students in Bengaluru in connection with non-consensual circulation of intimate images, especially in relation to job prospects. Not a far-fetched fear, considering employers are increasingly interested in monitoring social media behaviour to judge job applicants.[xxxiv] There have also been cases where women have been asked to leave their jobs when faced with the non-consensual circulation of their images.[xxxv]

Female journalists have expressed fears about their employability in the event that potential employers encounter hate messages or images about them online, which could reduce their chances of being hired.[xxxvi]Women have been forced to quit their jobs and look for other kinds of employment in order to avoid being trolled.[xxxvii] The displacement of blame on women and social sanctions against them in a gender unequal society is not only limited to situations where their private digital lives become public. Misogynistic targetting, active marginalization, termination of their membership in formal spaces, all with serious psychological, reputational, and economic consequences, may arise merely because women were vocal online. The fact that some women opt out of their current employment to escape harassment also implies an erosion of women's right to economic and public participation.

4.4. Image-centred cultures and patriarchal backlash

4.4.1 'Self(ie)-representation and backlash

Self representation on the Internet and its impact on self-image has become a popular line of inquiry in media and psychological scholarship.[xxxviii] Image-based platforms like Instagram which lead to the rise of self documentation through selfies have had a definitive role in these investigations. The selfie has been referred to as "social media driven narcissism" and is thought of as self-promotion to garner attention and admiration.[xxxix] Research has indicated that women post selfies to garner positive affirmation about their physical appearance.[xl] Such image-based communicative practices have had an adverse impact on women's self-esteem and have been

linked to body dysmorphia among young women.[xli] Together with image editing apps, these platforms are driving a regime of mandatory sexual subjectification where women are coerced to look and present the best physical version of themselves moulded on a white male gaze.[xlii] Online dating sites reinforce these ideals in people by placing the image front and centre and rejection just a swipe away.[xliii]

Under pressure to self-represent themselves as desirable in emerging image-centred cultures, women often face a double whammy. Posting selfies is the norm, but it is also often followed by backlash in the form of sexist comments, punishing women for daring to be seen, exercising agency, and thereby not conforming to gender-stereotypes.[xliv]

In a focus group discussion, a male college student reflected:

> But girls also should keep their accounts private and within their friends' circle. There are faults in them as well. Girls 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.

The young male participants in the focus groups largely put the onus on women for their safety, expecting the latter to interact within small, known communities online rather than the open web. Some claimed that when women who post their images are harassed, they are purposely inviting trouble.

A few male participants in the FGD took the route of 'it's just a joke', and 'women should be able to handle online trouble like men do'. One male participant even commented that the balance is always tilted in favour of women when it comes to cases of offensive banter online:

> Society already gives women enough power, and now they are taking unfair advantage of this power. If women make fun of each other, or if a woman makes fun of a man, that's seen as ok. In a group with boys and girls, I know that if I make fun of a boy, he will take it lightly. But if I am to make fun of a girl, I have to think twice, filter things in my mind and then speak it out.

As has been noted earlier, men betray a deep discomfort with the visibility of women in online spaces, especially in cases of image based self-representation. When women post selfies or pictures, they are inevitably sexualized and blamed. This presents, as Salter observes," an incompatible demand that young women "should not be sluts, but should also not be prudes."[xlv] On the one hand, women are forced to perform femininity; by looking cute or sexy for a capitalistic system that thrives on likes and followers.[xlvi] On the other hand, they are chastised for flouting gender norms.[xlvii]

4.4.2 Sexual harassment through the disclosure of intimate images

The male participants in the FGDs seemed to suggest that women were being careless by sending nude images to their partners. They saw women's sexual autonomy as inappropriate and underlined how sharing intimate images went against traditional values. Others claimed – in a discussion of a hypothetical situation where an ex-boyfriend circulates nude pictures of his ex-girlfriend to get back at her – that if the woman had gone as far as sending her nude pictures, how could she think of leaving him? A woman ending a relationship after she had been sexually intimate was seen as an act of cheating for which the release of nude/sexually explicit images by the ex-partner was seen as justified.

This patriarchal prerogative to show women their place through public shaming 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 girlfriend after their breakup, 44.8% of the respondents sympathized with the woman but felt that this was to be expected and that she should have known better. 24.8% felt that the man was at fault for breaking the woman's trust and confidentiality, while 24.5% felt that the woman was solely at fault (Appendix 1, Table 3.1). It is common for male friends and acquaintances to keep their female friends in check about what they post online and how they choose to represent themselves, 'for their own good'.[xlviii]

The majority of survey respondents felt that women had to watch out for themselves in such situations, as revealed by the comments they put down to the open question that followed this hypothetical scenario:

> She should have never sent nude pictures because they can be used as blackmail once they break up.
>
> I can't really say that somebody's at fault, but all girls should know their limits in using technology and should understand all cyber threats.
>
> If the man loved the woman he would not have posted it on the internet. But the woman also has to be in her limits and think of the future.
>
> The woman is not at fault because she trusted the man, but she should have been careful.

In a second hypothetical situation, involving a student who runs a YouTube channel that has progressive discussions on issues of caste and gender (such as inter-caste marriages) getting trolled, 62.68% of the survey respondents said that the student should not pull down her channel. 18.5% said that the girl should be cautious and only 3.88% said that she should have expected such a reaction as it is not right for women to speak like this (Appendix 1, Table 3.2). Some survey respondents also added the following:

> A woman has the freedom to put forth her ideas. She will have to put up a video on the threats she received so that even [the] public supports her.
>
> If she is doing something for society, then she should just stick to it. About the threats, she should report it to the police.

> Women are always considered lower than men in society, which is not right. Men don't want women to achieve more than them. She should continue her work and exercise her freedom. She is doing it in good faith.
>
> YouTube is a platform where people can express themselves, and she has a right to freedom of speech and expression.
>
> It's her right to speak, If people dislike it, then they may unsubscribe.

Survey respondents seem to hold the view that the reputational harm resulting from leaked pictures (in hypothetical situation 1) was too costly and engaging with sexual desires online was, therefore, not worth it. On the other hand, with regard to politically controversial posts, women seem less afraid of the consequences (in hypothetical situation 2).

As new sexual mores in image-based intimacies gain traction in the increasingly visual cultures of the day, stigma and shame may be just round the corner for women if communication intended to be purely private crosses over into public view. The widespread condoning (including by women) of non-consensual sharing by men of women's images and the threat of censure that women face about their online behaviour reflects how digital space folds into mainstream patriarchal socio-cultural space. Digital space in fact becomes an easy route to assert male impunity and privilege in intimate interactions. Women's use of internet-mediated space for private relationships thus leaves them with a Hobson's choice (as was also noted in respect of their public communication). To be in this space implies the inevitability of negotiating its patriarchal norms.

4.5. The role of support systems

Unfortunately, due to the nature of most kinds of gender-based cyberviolence and consequences in the form of perceived loss of reputation and social and economic sanctions, many women are reluctant to seek outside support. As a respondent from the survey put it:

> I did not approach anyone because I did not want to spoil my reputation and my boy friend's reputation. I kept it to myself hoping things would get better.

For many of the survey respondents, online harassment was followed by resigned acceptance of the fact that participation in online spaces comes with risks that must be personally managed. 39.02% of respondents who faced some form of harassment or abuse online have changed phone numbers at some point in time (Appendix 1, Table 5.1).

For most young women as pointed out in our interviews with counsellors, friends seem to be an essential support system. As an informant who runs a counselling helpline observed:

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

This observation was confirmed by quite a few of the survey respondents. Viewed as approachable, non-judgmental, trustworthy and possibly having faced similar situations, friends became the first point of contact for seeking support for gender- based cyberviolence. But peers may not have the resources and the wherewithal to provide a comprehensive response

In the FGDs with women, participants gave varying responses when presented with a hypothetical scenario of non-consensual circulation of intimate images. On being asked what advice they would give if a friend approached them with this problem, one of the participants responded:

> I would have been like, '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, we're obviously cautioning each other about different risks.

Another responded:

> At this point, I don't think any woman, or girl would take it. She would say, 'What the hell is wrong with you?' and confront the boy with her army of girlfriends who will back her up at this point. So, girls won't take such shit from a guy.

There is an acute awareness that young women reveal about what digital life or life in digital times implies in intimate social situations. This extends to a perceived need to negotiate differential norms in digitally mediated interactions. While some women did suggest that a push back to young men's patriarchal actions to shame ex-girl friends was important, it was unclear whether women do challenge men. For women who are already more vocal online such as journalists, strategies like naming and shaming, retweeting the abuse etc. could work. In a study with women scholars in Canada, a large percentage reported resisting violence by speaking out against the harassment, writing about it or sharing their stories with family and friends.[xlix] All these coping strategies may not necessarily be available cross-culturally or for those who, unlike the scholarly community, are not used to navigating digital public spaces. For women who lack a network of support online, the risk of backlash from the harasser may deter them from an open confrontation. In such instances, women tend to rely on technological aides like blocking to prevent abuse or turning on filters to stop seeing abusive content.

5. How the law and law enforcement agencies respond to cyberviolence against women

5.1. Use of IPC and IT Act

The Indian Penal Code (IPC) and the Information Technology Act (IT Act) are the two laws that are predominantly used in cases of gender-based cyberviolence in India. Of the two, the IPC tends to take precedence. Law enforcement officers we interviewed made it clear that when any crime takes place, the IPC is automatically implicated and that the IT Act is applied additionally. Lawyers we spoke to, also confirmed this:

> See, while we [lawyers] have used both the legislations, the IPC and IT Act, [when helping clients file cases of gender-based cyberviolence in police stations], we mostly take recourse to the IPC. The prevailing practice has been to interpret the IPC in a very broad manner and use it to apply it to all kinds of crimes. Over the years, the sections of the IPC have been used by the police and by the state to charge anyone for anything under the sun.

Sometimes, lawyers also strategically and deliberately avoid invoking the Information Technology Act and use only the IPC in order to ensure that the complaints are handled by the local police station which is better equipped rather than the understaffed cyber cell. As one lawyer we spoke to, explained:

> Seeking redress for these cases [where there is non-consensual circulation of intimate images] from the cyber cell hasn't been very useful, as they are overburdened. So, we have to do a trade off and use Section 498A [cruelty by husband or his relatives] and go to the regular police stations where there is more manpower available.

This preference for the IPC may be problematic on multiple counts. Over-reading provisions that were not initially designed to tackle cyberoffences and using them to bring perpetrators to book can backfire, as the chargesheet may not stand judicial scrutiny. Investigation also becomes challenging, as officers of the cybercrime police station can take cognizance and engage in evidence-gathering only when the IT Act is applied. If the IPC alone is invoked, the cybercrime police station cannot investigate such crimes and the general/local police station that does not have the trained personnel or access to equipment that a cybercrime police station does, will have to end up taking the case.

The Cybercrime Division of the CID, which manages one cybercrime police station in Bengaluru and also receives complaints from across the state, conducts training for its officers and also has the necessary technical capacity and infrastructure to handle cybercrimes.[i]

Local police stations have to rely on the cyber cell for assistance, especially in gathering evidence.
The only cyberoffence covered by the IPC is a legal provision for cyberstalking under Section 354D.
Understandably, investigation of complaints of cyberstalking requires digital expertise that only the cyberpolice have. But they cannot take up these cases unless at the time of filing the FIR allied provisions of the IT Act have been invoked along with Section 354D.

In its 2016 Crimes in India report, the National Crime Records Bureau notes that there are 2522 cases of cybercrimes currently under investigation in the state of Karnataka.[li] Where these numbers stand at present is unknown, but, by their own admission, cyber police in the state are reeling under the burden of the backlog, with fresh cases being filed routinely. Filing a case of gender-based cyberviolence under the IPC so that a relatively less burdened local police station can investigate it is a trade-off that survivors may need to make for the expertise of a cyber cell.

In an earlier study we had conducted in 2017-18, we were told by a law enforcement officer that for the IPC to be applied in a case, the physical body should have been implicated.[lii] This is the prevailing practice despite the judiciary having clarified that there is no such requirement in cases involving the non-consensual circulation of intimate images.[liii]

5.2 Gendertrolling and the consequences of striking down Section 66A

The infamous Section 66A of the IT Act was struck down in 2015 by the Supreme Court for being in violation of the Constitution.[liv] There was an almost unanimous condemnation of Section 66A of the IT Act by lawyers and digital rights activists interviewed for the research. Despite reports of the continued usage of Section 66A after it was struck down by the Supreme Court,[lv] the police officers interviewed for this research seemed to agree with the Court's reasoning that the section was being arbitrarily deployed and that "*everyone has freedom of speech and expression.*" There are, however, concerns that there is no alternative provision to cover cases that used to be filed under the section in instances of gendertrolling. In the words of a digital rights researcher interviewed for this study:

> The good thing about the judgment was that it struck down Section 66A of the IT Act, an obstacle to our freedom of speech on the internet. But what section or provision replaced it that would help make culprits liable? Nothing. So merely striking down of historically problematic provisions is not enough. It has to be followed up with something that will protect people.

Sections 499 (criminal defamation), 507 (anonymous criminal intimidation), 509 (insulting the modesty of a woman) and 354A (making sexually coloured remarks) of the IPC have been suggested by lawyers and experts as good substitutes for the erstwhile Section 66A of the IT Act. Scholars have suggested specific ways in which existing sections of the IPC could be deployed to address gendertrolling, such as creative interpretation of Section 354A (sexual harassment), Section 499 (defamation), Section 507 (criminal intimidation by anonymous communication), and Section 509 (insulting the modesty of a woman).[lvi]

With no legal substitute in the IT Act, except the provisions on obscenity, those who are trolled online cannot take recourse to the cyber cell, and will have to rely on the local police station to investigate the case. Except for defamation and criminal intimidation, all other provisions of the IPC that can be invoked by victims of online harassment require the harassment to be sexual/ 'obscene' in nature. Such narrow readings of harassment coming from a warped standard of public morality cannot effectively further women's claims to justice. In the absence of a comprehensive law for gender-based cyberharassment, the IPC does seem to provide some alternative, but one that leaves a lot to be desired. It does not recognize harassment that is sexist but not sexually explicit, and ends up treating sexually explicit attacks on women as amoral deviations from prevailing patriarchal social mores rather than viewing them as an infringement of women's autonomy and dignity.

5.2.1 Applicability of criminal defamation law to cases of gendertrolling

In the case of criminal defamation, since it 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.[lvii]

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 may not be in a position to take up.

5.2.2 Applicability of criminal intimidation law to cases of gendertrolling

Criminal intimidation is a useful provision that the police can ideally apply in cases of online trolling where there is threat of physical or sexual violence, but not necessarily where there is just sexist trolling not accompanied by the threat of physical or sexual violence. The latter is by and large likely to be perceived as 'empty threats', not warranting any alarm. According to the IPC, the essential ingredients to constitute criminal intimidation are:
(1) there should be a threat of injury to [the complainant's] person, reputation or property; or to the person or reputation of any individual in whom the complainant is interested, and
(2) the threat must be with intention to cause alarm to the complainant or force the complainant to undertake an action that she is not otherwise legally bound to perform or abstain from an action that she is legally entitled to undertake.[lviii]

In *Manek Taneja & Anr vs. 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.[lix] Whether the grounds for criminal intimidation also include the evaluation of whether the acts of the perpetrator actually did cause alarm is a disputed point. Some courts have held that it is immaterial,[lx] while others have

pointed out that it is material.[lxi] 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.

5.2.3 Applicability of the hate speech law to gendertrolling

Unfortunately, Section 153A of the IPC that criminalizes hate speech does not mention gender expressly as one of its protected categories and does not lend itself well to misogynistic trolling. Further, 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 or a threat to public tranquillity. Since the prevailing legal framework in India does not place adequate emphasis on the de-humanizing effect of hate-speech,[lxii] it fails to address the kind of hate speech that women face – those speech acts that may not result in violence but which stigmatize women and perpetuate notions of inferiority.[lxiii]

Going by the chequered history of the application of hate speech laws, where they have often been invoked by the power elite to clamp down counter-speech, it is questionable whether amending them to include 'gender identity as a ground' will improve matters. One of the human rights lawyers interviewed for this research opined:

> The [hate speech] provision has historically only seen improper use. Courts pass orders without taking into account any sort of evidence that is brought to the table. They are susceptible to the whims and fancies of the government and a majority of the public, and pass orders that they deem 'safe'. So unless our courts are actually ready to expand their thinking on this, no change in the wording of the law can take us anywhere.

With regard to other laws that protect marginalized social groups such as the Scheduled Caste and Scheduled Tribe (Prevention of Atrocities) Act, 1989, there are inconsistencies in their deployment in case of caste-based trolling The Delhi Court applied the Prevention of Atrocities Act in cases where caste slurs were made against a woman by her co-sister on Facebook. However, the law enforcement officials we spoke to in Bengaluru had never applied the law to gender-based cyber violence.[lxiv]

5.3 Obscenity and consent based provisions in the law and their application to non-consensual circulation of intimate images

5.3.1 Application and Limits of anti-obscenity provisions

Despite availability of other progressive legal provisions criminalizing cybercrimes against women, the archaic anti-obscenity sections, both in the IPC and the IT Act, continue to be used disproportionately by the police.[lxv] Of the sections in the IPC and the IT Act, senior officers tend to recount only the anti-obscenity based provisions, that is, Sections 292 of the IPC and 67 and 67A of the IT Act. These sections, are antiquated and side-step the issue of gender-based violence by focusing on the impact that content deemed obscene may have on the minds of the public.[lxvi] The judiciary in India has taken on a hard, moralistic approach to obscenity, as a result of the Supreme Court adopting the Hicklin test in the *Ranjit D. Udeshi vs. the state of Maharashtra* judgment, a stance that denies individual autonomy by prescribing that moral depravity is harmful to oneself. The Supreme Court did subsequently move on to a more contemporary test of obscenity by using the 'contemporary community standards' test taken from *Roth vs United States* in *Aveek Sarkar & Anr vs. the State of West Bengal.* However, it failed to acknowledge that the Roth decision was discarded by American courts for a more refined test of obscenity in *Miller vs California*.[lxvii] The Miller test is a three-pronged test; for content to be deemed obscene it must "appeal to the prurient interest" of an average person under "contemporary community standards". Second, the work "taken as a whole" must show sexual conduct "in a patently offensive way", defined under state law. Finally, the work must "lack serious literary, artistic, political, or scientific value".

Existing anti-obscenity laws are agnostic to whether expression is consensual or coerced, often resulting in punishing women's agency and autonomy.[lxviii] The law's double-edged approach is evident in cases of non-consensual circulation of intimate images, where a woman may voluntarily share intimate images of herself with her partner, who, without her consent, circulates it online. This situation requires a multilayered reading of consent that Victorian anti-obscenity provisions cannot provide, and in fact, erase. Without such an understanding of consent, the woman is as culpable as her partner under the anti-obscenity provision.

Using the Miller test, non-consensual circulation of intimate images may be seen as obscene, not in terms of retrograde ideas of patriarchal morality, but because such circulation constitutes "involuntary pornography that is socially harmful" and violative of "non-consenting victims' privacy rights".[lxix]

5.3.2 Application and Limits of consent-based provisions

Of all the police officers we spoke to, only one identified Section 66E of the IT Act as a more progressive section of the law that focuses on consent rather than morality, to punish non-consensual capture of intimate images or voyeurism. Section 66E is, however, not without its problems, pertaining as it is to the non-consensual capture, publishing or transmission of images only of a private area of any person without his/her consent. Because of this

exclusive focus on 'private parts' of the body, instances of violation of bodily privacy may not be fully covered – such as where a woman's face may have been morphed with an unknown/non-identifiable naked body. Further, the provision uses a 'reasonable expectation' test to determine what constitutes a circumstance violating privacy:

> Under circumstances violating privacy' means circumstances in which a person can have a reasonable expectation that–
> (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
> (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

The test of reasonable expectation of privacy was rejected by Justice Nariman, in the landmark *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors.* wherein the judge held that privacy was a subjective experience with the individual having sole authority to decide the areas of her life she would like to keep private.[lxx]

Section 66 E also does not adequately cover cases where informational privacy is violated. For instance, when personal information such as the name and phone number of the victim is leaked online, in what is known as an act of doxxing. This is a very common form of harassment. In fact, over 60.97% of respondents who had experienced harassment online reported that their personal data had been leaked online or a fake profile had been created using their personal details (Appendix 1, Table 4.12.) In such cases, a combination of Section 66C, "punishing identity theft", and Section 67 of the IT Act, "punishment for publishing or transmitting obscene material in electronic form", tends to be applied.[lxxi] In many instances, acts of doxxing occur simultaneously with a non-consensual sharing with the victim of pornographic images.[lxxii] In the survey, 42.27% of respondents who had experienced violence online reported that sexually explicit texts, images or videos were sent to them without their consent. (Appendix 1, 4.12.) In recent times, there have been attempts by the judiciary to broaden the ambit of acts of doxxing, though the language of Section 66E was not originally intended to cover them. In *The State (Cyber Cell) vs. 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 67 of the IT Act would not apply to the case at hand, because it was a personal communication between the accused and the complainant.[lxxiii] Instead, Section 66E would apply, as the mails invaded the complainant's privacy.[lxxiv]

Another lacuna in Section 66E is that it does not recognize the multi-layered nature of consent. It covers cases where the victim's images may have been captured without her knowledge, but not those where she may have voluntarily shared intimate pictures in the first place without consenting to their subsequent distribution. This lack of contextual understanding of privacy within the IT Act is surprising, considering that its counterpart in the IPC - Section 354C on voyeurism - explicitly criminalizes the circulation of intimate images even if shared voluntarily in the first instance.

Key informants from the police reported that if the complainant's intimate pictures are being distributed without her consent, the case is booked under Section 66E of the IT Act. In the case of morphing, on the other hand, the anti-obscenity section, i.e., Section 292 of the IPC and/or Sections 67 and/or 67A of the IT Act are applied.

Not everyone shares this strict bifurcation in the application of the IT Act, and more often than not, both Sections 66E and 67 of the IT Act are applied simultaneously. In what is considered India's first conviction for non-consensual circulation of intimate images, the survivor had intimate pictures of herself on her mobile phone which the accused demanded be sent to him. When she refused, he hacked into the complainant's phone and took the pictures, after which he blackmailed her to go out with him. When she refused again, he put up her pictures on a pornographic website. He was charged and found guilty under Sections 354A, 354C, 354D, and 509 of the IPC and Sections 66E, 66C, 67, 67A of the Information Technology Act 2000 (Amendment 2008).[lxxv]

The advantage of the anti-obscenity provisions over Section 66E, seemingly, is that they also cover secondary and tertiary distribution of images beyond the first perpetrator who got hold of the images. There is however, some confusion as to whether such an interpretation of the law is valid. When asked about the difficulties of pinning down culpability in the viral spread of illegal content, a senior level police officer opined that only the person who initiated the crime had the 'mens rea' (criminal intent) to be a perpetrator.

There are laws in other countries criminalizing non-consensual circulation of intimate images that have overcome this shortcoming, by bench marking '*mens rea*' to mean 'where the perpetrator/s have had reason to know that the person shown did not consent to distribution'.[lxxvi] This is a helpful standard considering the viral spread of non consensual intimate images.

On the whole, there seems to be some progress in how the police choose to apply the law to cases of cyberviolence, as evidenced by emerging judicial decisions. Among law enforcement officials, there is a greater awareness of the gendered nature of cyber crimes and the legal provisions that can be applied to such situations. That being said, the police still tend to rely on certain legacy sections, mainly the anti-obscenity provisions of the IT Act and IPC. While partly, this is an outcome of an embedded patriarchal notion of victimhood of women, it is also an outcome of a lacuna in prevailing laws: the absence of strongly worded progressive legal provisions that can be substituted for anti-obscenity. The striking down of Section 66A of the IT Act maybe something that needs to be revisited and re-moulded through a feminist lens.

5.4 Producing digital evidence before the court and the problem with certification

In courts, proof of contents of a document can be furnished either as primary or secondary evidence. Primary evidence is the document itself, and secondary evidence is the certified copy of the primary evidence.[lxxvii] For example, in a case where digital images are being adduced as evidence, if the device on which the image is made

is brought before court, it is primary evidence; but if a copy of the digital image is being produced before the court – say in a CD or printed form, it is secondary evidence. Secondary digital evidence under the Indian Evidence Act is dealt with under Section 65B which lists technical and non-technical conditions for digital evidence to be admissible.[lxxviii]

Section 65 B(2) of the Indian Evidence Act states that a computer output is admissible as evidence only when the following conditions are satisfied:

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

Additionally, Section 65B(4) of the Indian Evidence Act states that:

In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

These special requirements for electronic evidence were being ignored by the judiciary , until 2014, where with *Anvar vs. Basheer*, the Supreme Court mandated the strict application of Section 65B in the production of evidence.[lxxix] In the Court's own words: "The Evidence Act does not contemplate or permit the proof of an

electronic record by oral evidence if requirements under Section 65B of the Evidence Act are not complied with". However, in 2018, the Supreme Court ruled that if the electronic device is in adverse possession, then certification under section 65B need not be produced.[lxxx] The court held, "the applicability of requirement of certificate being procedural can be relaxed by Court wherever interest of justice so justifies."[lxxxi]

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. In any case, there seems to be some dispute over how strictly the requirement of certification was being followed, with police officers giving us widely varying answers.

5.4.1 Maintaining the integrity of digital evidence

Part of the reason why courts have been so particular with admissibility of digital evidence is that electronic records are easy to manipulate and tamper. To avoid the discarding of digital evidence, law enforcement agencies usually follow a Standard Operating Procedure (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 that is done to match copies with the original) so that any tampering can be detected and a write-blocker is also installed.[lxxxii] 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.

Section 45 A of the Indian Evidence Act states that the opinion of an expert examiner of electronic evidence, notified by the central government in accordance with Section 79A of the IT Act, is a relevant fact to the proceedings. However, it was only in 2017 that the central government appointed such examiners. A pilot scheme to appoint state level or central forensic agencies was also initiated in the same year.[lxxxiii] So far, six labs have been notified as examiners of electronic evidence, including the State Forensic Science Laboratory in Bengaluru.[lxxxiv] A senior officer at the forensic lab informed us that when the lab provides assistance to an investigating officer, then a representative of the lab may be called by the court and can be cross-examined as to the validity of the evidence. The appointment of examiners may free up much-needed police personnel for other tasks that would not be possible if they were constantly summoned by the courts.

5.4.2 Working with Internet Intermediaries

The servers of digital platforms/ internet intermediaries are valuable repositories of evidence in cases of gender-based cyberviolence. While formal channels of communication for the requisitioning of evidence have been

established between digital platforms and police functionaries, there is still considerable friction in these exchanges.

An officer at the CID interviewed for the research emphasized how Facebook often refuses to co-operate, causing a delay in investigation. Another officer (from the CID) claimed that Facebook's response is considerably delayed:

> 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.

In instances where servers are located in India, the police may still apply the Criminal Procedure Code (CrPC) to access evidence. Section 91 of the Criminal Procedure Code (CrPC) gives the police wide powers to seek access to documents or data.[lxxxv] But the government is yet to notify rules for the preservation and retention of data by Intermediaries as provided in Section 67C of the IT Act.

When servers are located out of the country, access to relevant data is dictated by the Mutual Legal Assistance Treaties – 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).[lxxxvi] Although the United States, under the Electronic Communication Privacy Act, prohibits companies from sharing content of communications directly with a foreign government, the Act is silent on metadata. Therefore, platform companies headquartered in the United States do share such data with foreign governments on request, subject to company policy.[lxxxvii]

Usually, for India, MLAT requests in criminal matters are handled by the Ministry of Home Affairs (MHA). Summons or warrants with extraterritorial effects are obtained under Section 105 of the CrPC which the registrar of the court forwards with a covering letter to the central government and Ministry of Home Affairs. Then, either through diplomatic missions or directly, MHA communicates the request to the central government of the foreign country. The recipient country coordinates with its investigating agencies to gather the data. The covering letter must set out the facts of the case as well as the evidence sought in light of the legal standards of the country from which data is sought. In the case of the United States, when data is sought, probable cause must be established. Under Letters Rogatory, the investigating agency approaches MHA and then an Indian court issues an LR requesting a foreign court to direct individuals or companies in its territory to produce the evidence.[lxxxviii] 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.[lxxxix]

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, it takes 2-3 years. 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.[xc]

The CLOUD (Clarifying Overseas Use of Data) Act in the US has been touted as a much-needed replacement to the MLAT system through which private companies can directly share data (except that of US citizens) based on an executive agreement with country governments, as long as the latter meets certain privacy and human rights standards,[xci] such as collection and purpose limitation, protection from arbitrary and unlawful interference with privacy, as well as non-discrimination.[xcii] While the Data Protection Bill may qualify India to exchange data with the US, the CLOUD Act is still a one-sided agreement which India had no opportunity to negotiate.[xciii]

India on the other hand is looking to localize data through the Data Protection Bill. The Srikrishna Committee cites access to data for law enforcement as one of the reasons for such provisions.[xciv]

> A requirement to store personal data locally would boost law enforcement efforts to access information required for the detection of crime as well as in gathering evidence for prosecution. This is because it is easier for law enforcement agencies to access information within their jurisdiction as compared to awaiting responses to requests made to foreign entities which store data abroad.

Law enforcement agencies, including a police officer interviewed, supports this stance, by raising the question: if the Reserve Bank of India can demand localization of payment systems data,[xcv] why can't the Indian Computer Emergency Response Team (the nodal agency in charge of cybersecurity in India)?

In the present scenario, when almost all crimes have a cyber angle to them, it is important to put in place a legal framework for data access that meets the necessity and proportionality test with respect to balancing citizen privacy considerations with investigatory mandates of law enforcement agencies.

6. Institutional mechanisms for gender-based cyberviolence

6.1. Perceptions of law enforcement officials about gender-based cyberviolence

There is some degree of dissonance between the perceptions and attitudes of law enforcement officials to gender-based cyberviolence and the experiences of survivors and their lawyers with the police. In 2017, when IT for Change conducted a study of perceptions of gender- based cyberviolence among police officials in Bengaluru,

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”, the IPC, whose provisions most dealt with crimes against the body, could not be applied in cases of cyberviolence. This time around, most of the police officers interviewed demonstrated a better grasp of gender-based cyberviolence, acknowledged the seriousness of these crimes and the room for using the IPC in charging perpetrators. While the reason for such a shift in perception is difficult to ascertain, it may be the case that recent policy developments and capacity building initiatives have played a role in this shift.

The Cybercrime Prevention Against Women and Girls Scheme set up in late 2017[xcvi] aims at training 27500 police officers, public prosecutors & judicial officers in cybercrime awareness and 13500 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. The minimum target set for Karnataka is 90 women in law enforcement agencies, including 20 women Station House Officers. The training curriculum also has special focus on cybercrimes faced by women and children.[xcvii] The scheme intends to not just create officers who are specialized in dealing with cybercrimes, but also attempts to equip as many officers as possible with a general idea of how to deal with cybercrime, especially the first responders.[xcviii] This scheme is indicative of the state’s recognition of the need for systemic changes to combat gender-based cybercrime effectively.[xcix]The state of Karnataka has been granted 3.9 crore rupees under the scheme to set up a ‘Cyber Forensic Lab and Training Centre’ and 40 lakh rupees for capacity building.[c]

6.2. Structure of cybercrime police stations in the state

Karnataka has 37 Cyber, Economic and Narcotics (CEN) Cells as well as 5 city-wide cybercrime police stations, including one each in Mysuru and Bengaluru. The Criminal Investigation Department (CID) based in Bengaluru also houses a cybercrimes division. A senior level police officer interviewed for the study commented that although Mysuru has a cybercrime police station, most cases come to Bengaluru, even though it is understaffed.

There are only 22 personnel assigned to the Bengaluru city cybercrime police station,[ci] and there is a marked absence of senior level female police officers. Research has shown that increasing the number of female police officers at police stations can have a positive impact on reporting of crimes by women.[cii] How the state will fulfil the requirement of training at least 90 women police officers, as per the target set by the newly initiated Cybercrime Prevention Against Women and Girls Scheme, remains to be seen.

The senior police officer in-charge of cybercrimes across the state also told us that police officers at the CEN Cells had recently undergone the 5 day training programme required by the central scheme. Interviews with officers at the cybercrime police station revealed that junior level officers had not received any training, other than the two

days of training they received upon joining the cybercrimes police team. This hopefully will change in the near future, as and when the central scheme is implemented by the state government. Recently, it was announced that with support from Infosys Foundation, more than 5000 personnel from the state would be trained in investigating cybercrimes at the upgraded Centre for Cybercrime Investigation Training and Research at CID headquarters in Bengaluru.[ciii] Hopefully, this would result in more first responders, including women officers, being trained.

6.3. Trends in reporting and statistical documentation of gender-based cybercrimes

Karnataka, according to the NCRB Crimes in India 2016 data, records the highest incidents of cybercrimes after Maharashtra and Uttar Pradesh. Bengaluru in particular, stands second only to Mumbai in the number of cybercrimes registered.[civ]

At the national level, a range of initiatives are being set up for ensuring prompt responses to cyberviolence. However, there is still a long road to be travelled with respect to getting women to come forward and file complaints.

The Ministry for Women and Child Development recently came up with the #IamTrolledHelp Twitter hashtag and a dedicated e-mail id that women could use or write to, as a method to seek police assistance.[cv] However, from July 2016 to January 2018, the number of complaints received by the Ministry over social media platforms was less than 100.[cvi] A cybercrime reporting portal was launched by the Ministry of Home Affairs[cvii] last year to receive complaints of "Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (CP/RGR) content."[cviii] Once a complaint is made on the cybercrimes portal, it is forwarded to the nodal office of that district who has to file an FIR. Within 48 hours of an online complaint being made, the police is mandated to respond to the complainant.[cix] The technical officer at the CID Bengaluru said that only about 90 cases were registered with the portal in the last 6 months, of which there is no clear break-down of the number of cases pertaining to minors and the number pertaining to adults.

Interviews with the police suggest that more women are coming forward to file FIRs for cybercrimes, but there is no way to do a trend analysis, as gender-based cyberviolence is not considered a separate category of crime in the prevailing statistical system. 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 the former.

6.4 Experiences and perception of victims, lawyers, and counselors

Although 36.70% of the women in the survey reported facing harassment online, only seven of them approached the police (Appendix 1, Table 6.1).

In five of these cases, the harasser was known; in three, personal contact details were leaked; and in four, sexually explicit pictures were shown to the respondent without her consent. In one case, sexual relations were forced upon the respondent on the threat of releasing pictures and in four cases, respondents were repeatedly contacted despite indicating that they did not want to communicate with the harasser. Their reasons for approaching the police were varied; to simply stop the harassment, remove sexually explicit and morphed pictures of themselves from the internet, and trace and arrest the harasser. Of the five who answered the question of how the police responded, two said that the police dismissed the complaint (in one case the harasser was known and in the other, unknown) and three said that the police were helpful.

Of the majority of victims of cyberviolence who chose not to approach the police, 45.19% felt that the harassment they experienced was not a crime; 40.38% felt that the police would not take their complaint seriously; 34.61 felt that if they contacted the police, then the latter would contact her parents or college; and 33.65 felt uncomfortable going to a police station (Appendix 1, 6.2).[cx] We were told by two lawyers who represent women from marginalized socio-economic backgrounds that many of the women who approach them are too scared to go to the police and merely wish for the violence to be stopped through a legal notice. In cases of intimate partner violence there is the added apprehension that the violence could escalate. For those who face violence in same-sex relationships, especially on dating sites, reaching out to the police would mean outing oneself and risking stigmatization. This, despite the recent Supreme Court decision decriminalizing homosexuality in India.[cxi] A lawyer who works with queer communities in Bengaluru observed:

> What usually happens is that they would have probably met someone online, like on Tinder or Grindr, and would have invited that person home. When they did meet, the other person would have come with a gang to physically assault the client. Most of our clients haven't even come out to their families, forget coming out to the police. So we have to position the case in such a way that it was a regular case of violence – the person was riding down the street and was hit and his belongings were taken away.

In a study conducted by Digital Rights Foundation in Pakistan based on their 'Cyber Harassment Helpline' data, 45% of the women who reached out to them did not report the act to the police because they felt the police would not take it seriously.[cxii] In England and Wales, 61% of the 1,160 complainants of non-consensual circulation of intimate images reported that the police refused to take adequate action. The perceived futility of, or even possible further victimization involved in, approaching law enforcement authorities in cases of gender-based cyberviolence corresponds to trends in other cases of sexual harassment as well. However, it also needs to be recognized that motivations for not seeking redress may be complex and not confined to one particular reason. Approaching the police also implies making the issue public, something that may just invite more trouble for young women in terms of social disapproval, stigma, and extreme censure by family. The fact some women, even if a small minority, did approach the police suggests that the role of law in redress must be understood better in relation to gender-based cyberviolence. Investigation into cybercrimes necessitates a different process and may

be perceived by victims as highly invasive (requiring disclosure of all digital communication, depositing gadgets in the police station, etc.) and/ or time consuming. In England and Wales for example, among the main reasons cited by police for not taking adequate action include a lack of evidence or the victim withdrawing support for any action.[cxiii]

6.4.1. De-prioritization of gender-based cybercrimes

One of the survivors we interviewed told us that the police do not take cases of online violence seriously because of the belief that there is no physical harm in such cases. A dichotomous approach to online and offline crimes also contributes to the discounting of harms caused by cyber crimes.[cxiv] This, in part, concerns the semantics of the law itself. One senior police official interviewed at the cyberpolice station was of the opinion that his hands are tied since Section 66A of the IT Act was struck down and that he is forced oftentimes to redirect the victim to her local police station, where the case can then be booked under other laws, including the IPC. On the other hand , informants also reported that the police are quick to arrest people, especially from minority communities, if they are perceived as being anti-establishment in online spaces. And in some cases, they continue to invoke the annulled Section 66A.[cxv] PUCL has called attention to the continued arrests under this section before the Supreme Court, which has ruled that officers continuing to use this section will be arrested.[cxvi]

Most survey respondents called for a shift in mindset among law enforcement authorities, calling for prompt action, responsiveness in registering complaints, compassion, and overcoming gender bias and victim blaming. The lack of wider social acknowledgement of the debilitating consequences that women face because of gender-based cyber violence leads to trivialization. One survivor reported that the police refused to file a complaint claiming that since nothing came of her previous complaints, why try again? She said:

> The police asked me “You have already filed a complaint against a person. Why do it again and again?” They are basically saying, you have already filed a complaint before, and yet these people continue to do what they do. So what is the use of this? This is very discouraging for a woman.

Survivors are also advised by the police to stay offline for sometime so that the situation can eventually sort itself out. This, however, is not a real option as more and more women go online and everyday life becomes tied to the digital.[cxvii] One survivor who participated in the research was advised by the police not to post provocative messages, which she perceived as 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, despite me getting threats about rape, acid attack etc.

The family court lawyer interviewed for the research reported that officials at the cybercell may not even register the case:

> These victims already have a lot of burden on their mind. Imagine if they also have to handle the burden of dealing with the police. Our criminal justice system is not in line with the interests of the victims. I also had a friend in the cyber police station who I used to directly go to and he would help in these cases. Some police people are good. It depends on how gender sensitive they are. But some do not bother to even register the cases.

The de-prioritization of gender-based cyber violence stems from the unsubstantiated notion that there is no immediate risk of harm, a view that extends from an assumption that harm is serious only if it concerns the threat of physical violence. An independent researcher and women's rights activist interviewed, shared instances where women journalists who had approached the police to complain about online harassment were told not to worry, as the harasser lived in a different state.

Another women's rights activist who was interviewed, recounted being told by the police in one instance, to just block the trolls, and in another, to approach the intermediary on her own. In the activist's words:

> I had friends at Twitter, so they gave me email ids of persons I could write to. This happened only because I had access. Imagine, for all these years, the cops did not know who to write to. So, I escalated the problem to the Twitter public policy head.

After all this effort had been put in by the activist, the police told her that the evidence she had collected about the abuse was insufficient, as the abusive messages had been deleted and that they needed the log-in and log-out times of the alleged harasser. The social capital of a survivor seems integral to the likelihood of a case of cyberviolence being taken seriously by the police:

> Only because I was a journalist and I had the back up of celebrities they took my complaint seriously, and this was much, much later. Otherwise, they would have not even considered my complaint.

Such second-hand treatment of complaints of gender-based cyberviolence is reported from across the world. Law enforcement agencies have refused to register cases, de-prioritizing gender-based cyberviolence, thereby discounting the victim's experiences.[cxviii] In a multi country study of the experience of online violence in Norway, Denmark, and Iceland, survivors of gender-based cyberviolence recollect being asked by the police to gather evidence themselves. Tellingly, a law enforcement official interviewed for this research pointed out that when the server is located outside the country, co-ordination between the two countries' law enforcement teams is imperative for the case to proceed. In such situations, preference is given to what are "more serious crimes, like terrorism". No surprise then that gender-based cyberviolence gets de-prioritized.

6.4.2 Shifting the burden to produce evidence on the survivor

Producing digital evidence becomes laborious and difficult in cases of cyberviolence. As one survivor explained:

> We have to give the URL [of the content under question] to the police and they will trace the profile and IP address of the person. But sometimes what happens is that these people will

> comment and abuse and then deactivate and delete their profiles, so we cannot find them even with the URL.

A family court lawyer who was a key informant for the research also confirmed this point, noting that oftentimes, the standards of evidence the police demand from the victim cannot be met.

> The police can say 'you may yourself have created these messages and then taken the screenshots' or the perpetrator may say, 'you hacked into my profile and did this'. So the IP address is needed. Only the victims have to get all this information, which is very difficult. If they don't get this, then the police won't accept the evidence.

One of the interviewees spoke to us about a colleague who approached the Bengaluru police to file a complaint of trolling, but was turned back and asked to bring evidence on a CD.

> When we approached them, they asked us to bring the evidence on a CD! A CD, can you imagine?! We told them that see, these abuses are on our Twitter, we can take screenshots and send. But they are like [sic], 'no, we can't'. It's part of the procedure. They even refused to take it on a pen drive. So the entire process was extremely cumbersome- my colleague couldn't travel everyday or leave office. So she got tired and decided not to pursue the case.

The police officer at the cybercrime police station had a different view. He underlined that the burden of finding evidence does not fall on the victim, and that the state has an excellent forensic science lab that aids in the collection of digital evidence. He did add though, that complainants must produce some amount of evidence before a case can be registered, pointing to the need for the victim to share her device/s. In cases where a URL is not present – for instance, on WhatsApp, the police has to trace back the origin of the message starting from the victim's device.[cxix] However, the complainant may be reluctant at times to handover devices, as this could mean sharing complete access to parts of her life that may be immaterial to the case or sensitive information such as but not limited to, intimate images. In the *State of West Bengal vs. Animesh Boxi*, the court noted that the victim initially refused to hand over her phone because of the sensitivity of the material concerned and only after the police convinced her that it was necessary to collect evidence did she hand over her device.[cxx]

The role of the forensic lab is to provide assistance to the cyber police in analyzing digital evidence, and in the gathering of evidence from the device. The field research carried out for this report suggests that the State Forensic Science Lab is overburdened with cases from across Karnataka, and it takes a year to respond to requests.

Survivors are thus stuck between a rock and a hard place. While on the one hand, they need to go through the trouble of recovering evidence, on the other, they may have to give the police complete access to their devices (and by extension, their complete digital history) in an excessive intrusion of their privacy without any guarantee of recovery of evidence in a reasonable time frame.

The accounts of survivors and lawyers suggest that the investigation of gender-based cyberviolence in Karnataka suffers from a systemic disregard of women's realities. Trivialization of cyberviolence is rampant and there is no acknowledgement of the harm that survivors suffer. The few women who overcome the odds to finally file a case are then expected to further jump through hoops just to file a case and get it investigated. Law enforcement agencies in the state need to orient themselves to a survivor centred approach to investigating gender-based cyberviolence. This includes validating the woman's experience and empowering them by restoring to them a sense of control.[cxxi] In case of gender-based cyberviolence, this could be as simple as guiding the complainant to other avenues of redress like the intermediary, if the facts of the case reveal that it is not strictly illegal.

6.4.3 Responses from courts and educational institutions

None of the cases of gender-based cyberviolence handled by the lawyers interviewed for the research escalated to the level where the courts got involved. But two did point out to us that it is not only the judge, but the public prosecutor too, who the women needed to worry about:

> The challenge in the court is not just the judge, it is the public prosecutor as well or any senior advocate who represents you. Public prosecutors really don't have the expertise to deal with these cases. They may just be dismissive or be bought off by the opposite party.

Only two of the respondents to the survey marked that they had approached the courts for redress.
Of the four colleges where the survey was carried out, only two had an Internal Complaints Committee set up to hear complaints of sexual harassment by students, teachers, and non-teaching staff, despite UGC regulations mandating the same in all higher education institutions.[cxxii]

37.01% of the respondents didn't know whether their college had an ICC (Appendix 1, Table 7.2). Eight students had approached their college authorities when they faced harassment online. Two of them were bullied based on their physical appearance, their personal contact details were leaked or a fake profile created; three of them,-were sent sexually explicit content without their consent; and four of them said that they were being talked to and contacted repeatedly for sexual favours despite clearly indicating they were not interested.

In response to the open-ended questions on suggestions to college authorities for improving their response to gender-based cyberviolence, many students asked for awareness programs. They also asked for the setting up of internal committees for sexual harassment sensitive towards, and supportive of, victims of harassment.

7. Technological frameworks: disciplining users

7.1. Impact of platform affordances on risk of violence

It is useful to keep in mind that digital systems do not develop organically. Powerful actors such as social media platforms 'cultivate a landscape' through deliberate design choices.[cxxiii] Platform design choices - both front-end features and back-end algorithms - determine how communications take place and how abuse is perpetrated as well as countered on these spaces. Even the kind of content that gets traded online is nudged by platforms. Take the development of image-based content online. Images on the Internet started with rudimentary emojis constructed from punctuation and alpha-numeric symbols to bring emotional cues to text. From there on, visual cultures on the Internet went on to become more sophisticated and vibrant with uploading of photographs, gifs, memes, image filters and finally videos.[cxxiv] This evolution of image-based communications is partly a testament to users' ingenuity, but more importantly, it is also a result of how platforms seek to structure social communication and interaction. Facebook, for instance, tweaked its ranking algorithms to prioritize Facebook Live. It also invested in partnerships with media companies for the production of content to keep the medium attractive.[cxxv]

Affordances of anonymity and multiple profiles, combined with content governance policies that provide a wide berth for free speech, offered by platforms such as Twitter, have led to abusive mass-coordinated misogynistic attacks.[cxxvi] Even innocuous design features such as 'ease of response' can snowball into en-masse trolling. Just take the case of how enhanced ease of response on Twitter, as compared to Tumblr, has also led to greater harassment on the former.[cxxvii]

The analysis of our survey data reveals that out of Facebook, WhatsApp and Instagram, identity based harassment is correlated significantly only with harassment on Facebook. (Appendix 2, Table 5).[cxxviii] In specific, harassment on Facebook has a strong correlation to harassment on the basis of physical characteristics or social identity. A possible reason for this could be the amount of self-identifying details that one has to reveal on Facebook just to create an account.

There is also a connection between the openness of the platform and the prevalence of anonymous harassment. The analysis of survey data reveals that Facebook and Instagram have a high proportion of unknown perpetrators because they are designed to be open, whereas WhatsApp has more known perpetrators because it is usually used to communicate with people whom one may have had some prior contact offline (Appendix 2, Table 4).

In a focus group discussion with women, one participant remarked that linking the national bio-metric based identity– *Aadhaar* – with social media profiles could enhance security, preventing anonymous attacks. This suggestion may be antithetical to personal privacy, but it may be read as coming from a felt need on the part of young women for safe spaces online.

Quantified appreciation through likes and shares gives individual users feedback on what the 'public' loves and nudges them to produce more such content. Algorithms order content by popularity, reinforcing market considerations in content production.[cxxix] In such a scenario, misogyny also becomes a 'trend' leveraged by the market. Reddit's system of up-voting and down-voting content to earn 'karma' points and the ordering of content as per popularity led to a viral spread on the platform of leaked intimate images of female celebrities.[cxxx]

Platforms are designed for an imagined hetro-normative, invariably white, user. This not only alienates users from marginalized locations,[cxxxi] but also perpetrates violence against them. A study on Facebook's 'public by default' stance - its insistence on linking online identity to offline networks using 'real names' - notes how queer youth of colour are outed by the system only to face family violence. For transnational digital corporations whose design logic is grounded in granular data-based microprofiling for hypertargetted advertising, such default and forced public-ness is the norm. Under a dataveillance culture in platform capitalism, everyone is under the shadow of the data superpanopticon all the time.[cxxxii]

While it is true that individual users may be able to subvert techno-design,[cxxxiii] platforms need to take on the responsibility to make design choices based on social and gender concerns so that women's safety and security of women is prioritized. Tinder, for instance, piloted a feature in India that allows only women to send the first message, a feature they copied from Bumble (dubbed a feminist dating app) in order to enhance the safety of women.

7.2 Non-transparent and culturally agnostic community standards

Despite evidence to the contrary, platforms insist on their neutrality vis-a-vis the communication that takes place over them, claiming they have no role/responsibility in relation to the content that is transacted.

Their terms of use often resemble boiler plate contracts that shrug off any liability for user behaviour. Though social media platforms such as Facebook often lay down community standards pertaining to sharing of content that involves adult nudity and sexual activity, bullying and harassment, violence and graphic content, etc., they are often not enforced strictly. While content guidelines are applied selectively, they perform an important discursive role,[cxxxiv] one that seemingly espouses liberal - constitutional values, like anti-discrimination, without actually enforcing them. Multiple interviewees have experienced situations where intermediaries have been recalcitrant, with the latter often citing their internal regulations as not permitting the take-down of the flagged content. Sometimes, even flagging patently illegal content, if in the local language, can go unanswered. A child rights activist shared:

> I remember 2-3 years ago I had got involved with this Facebook page which used to put pictures of children. Now see, these children were fully clothed in these pictures. There's no pornography in the

> picture itself. These pages would be in Tamil or Malayalam. At the outset, nothing seemed wrong. But when you looked at the captions, they would say, "so tell us in the comments what you would like to do with these children?" Evidently, these were pedophiles. It's all written in Malayalam or Tamil. We used to report this to Facebook but only managed to get one or two of the pages blocked. But then I had friends in Chennai who took it up very strongly with Facebook, demanding that they had to have people who understand these languages.

Additionally, many of the social media companies have not appointed a grievance officer,[cxxxv] even though it is mandated by regulations under the IT Act.[cxxxvi]

Though platforms use a combination of algorithms and human mediation to review content at various levels, there is no transparency as to how 'bad' content is being weeded out and 'good' content retained.[cxxxvii] Although Facebook started publishing data on how community guidelines are enforced,[cxxxviii] the guidelines and their rules of interpretation are unknown. Recently it has come to light that Facebook has developed its own set of "locally illegal markers" for content from India that urges moderators to flag content pertaining to the Tricolour, defamation of deities etc., "without the knowledge of users or any input from local law enforcement agencies." This, even though in a different context, the platform has insisted on maintaining global standards.[cxxxix] While having guidelines that are aware of local contexts is welcome, the kind of content listed that require a double take by reviewers at Facebook are those that could result in the blocking of platforms in the country. Clearly the intentions of censorship are in furthering their own self-interest. With misogynistic or sexist content, it therefore seems unlikely that platforms will do much. Quoting a digital rights researcher we spoke to:

> Content governance online has become a matter for private governance by intermediaries. A consequence of this has been the impinging of our freedom of speech, particularly due to vague 'community guidelines' and 'user policies' drafted by them, which helps them get away with anything.

On the less contentious rules of procedural due process, social media platforms are notorious for functioning in arbitrary ways.[cxl] On substantive regulation, the problem gets compounded. 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.[cxli] Twitter, arguably one of the biggest adherents to free speech, for instance, is one of the few platforms that allows content by Alex Jones (of InfoWars) to remain on its platform despite the fact that such content violates the company's guidelines on hateful content.[cxlii] Facebook defines hateful content in its community guidelines as a "direct attack on people based on …protected characteristics – race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity and serious disease or disability".[cxliii] The platform however, still exhibits discrepancies in implementing its own law; gender based slurs

for instance are often not removed. Even threats of violence are allowed to remain online if the threat does not look credible enough. These only point to the fact that Facebook does not actually understand the concept of misogyny.[cxliv] The most recent iteration of Facebook's community guidelines has made some progress and includes the notion of de-humanising effects of hate speech, defining attack "*as violent or dehumanising speech, statements of inferiority, or calls for exclusion or segregation.*"[cxlv] How well this will be implemented is to be seen.

7.3 Trends in Intermediary liability rules

Part of the reason why intermediaries get away with selective action when it comes to regulating content on their platforms or issues of gender-based violence online is because the law gives them the wide berth to function that way. Platform intermediaries are imagined in the law as passive facilitators of communications, a discourse that they have heavily invested in creating and furthering, with 'safe harbour' provisions from liability. Such 'legal subsidy' was initially given to tech companies in the early 90's to grow their businesses and remain unencumbered by regulatory burden.[cxlvi] The intermediaries of today no longer resemble the intermediary that existed when safe harbours were first introduced. As seen above, they have a major hand in shaping online communication cultures and even manipulate users' online responses.[cxlvii] The legal landscape must, therefore, change.

Through the Supreme Court decision in *Shreya Singhal vs Union of India*, intermediary liability went in 2015 from a strict liability regime to a notice based one,[cxlviii] that is, liability for content take-downs on the basis of a judicial/executive order.[cxlix] The Supreme Court has since faced cases where it has had to re-evaluate its decision from 2015. Two cases of note are, one, the *Sabu Mathew George vs. Union of India,* a public interest litigation challenging the violation by online intermediaries of the prohibition on advertisements relating to pre-natal sex determination tests; and two, in *Re Prajwala,* another public interest litigation taken up by the apex court in response to a letter on the rampant circulation of rape videos on social networks and social media platforms. In both cases, the Supreme Court found it hard to stick by the *Shreya Singhal vs. Union of India* decision, and recommended exceptions that required immediate response by the intermediary, including pre-filtering, without the intervention of the court. Even in the US, there have been concerns that Section 230 of the Communication Decency Act needs to be re-evaluated to account for the kinds of violence that are perpetrated online and the changed nature of intermediaries. 'Good Samaritan' clauses which gave intermediaries the leeway to police their platforms without any liability have been a failure, and there have been calls to change the law.[cl]

The Ministry of Electronics and Information Technology recently released a draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018 as a response to the rise of disinformation through the misuse of social media platforms.[cli] While a detailed discussion of the controversial guidelines is beyond the scope of this report, one important point to be noted is a rule that requires intermediaries to "deploy technology based

automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content."[cliii] Civil society has rightfully been critical of the implications of this vaguely worded provision[cliii] that can have dire consequences for free speech. Apart from the privatization of censorship and the lack of accountability, AI-assisted content filtering has endemic problems such as designer bias, inability to recognize context, and false positives resulting from running on imperfect data sets.[cliv] As a generalized standard for all kinds of content from intimate images circulated without consent of the victim to copyright infringement, the rule may not pass the constitutional muster for 'reasonability' of restrictions on free speech. Due of the costs of implementing these regulations, it has been argued that start-ups should be exempt, lest such regulatory burdens end up cementing the power of big tech such as Google and Facebook.[clv]

A differentiated intermediary regime can be a good alternative to the proposed amendment. Backed by due process and principles of natural justice, including the right to challenge a take-down, such a regime could lead to more equitable results, if the responsibility of the intermediary is made contingent on the kind of content flagged as well as platform design considerations involved. For example, social networking sites with a user base of a particular size could be mandated to use AI to flag or even proactively take-down certain kinds of content such as child pornography or videos of sexual assault, while granting the uploader of such disputed content a chance to appeal this decision. The point is not to reject the use of AI in any situation, but find out ways in which it can augment human driven regulatory processes.[clvi]

8. Conclusions and Recommendations

The digital has entered every aspect of social life. It has spawned unprecedented ways of being and doing that have dramatically changed the social and economic order. For the born-digital generation who were a focus of this study, the Internet is also a critical site for self-building.

The study explored how women across social locations are grappling with the challenges of navigating digital space, managing their relationships and negotiating family and community dynamics in the face of cyberviolence. Through a survivor-centred, feminist, approach, it examined the re-socialization process underlying gender-based cyberviolence, unpacking the law, evaluating state institutions, and taking stock of digital platforms and their processes for redressal.

In the early days of cyberfeminism, there was a prevailing consensus that gender would not be of consequence on the Internet.[clvii] In the landmark 'Cyborg Manifesto', Haraway offers a radical vision of the future of humanity in the digital age, wherein all human beings would become an amalgam of animate and inanimate/ human and machine, 'cybernetic organisms' emancipated from the oppression of embodiment.[clviii] Indeed, even as Haraway's 'cybernetic organisms' have materialized, and part of our minds may be seen as residing on Google's server,[clix] the

idea that life on the Internet "immaterializes gender" does not seem to have borne out. In fact, gender stereotypes of the pre-digital context are not only replicated, but sometimes, even magnified, in the human-machine agglomeration. Reality has come to be a complex mix of the offline and online[clx], as this study bears out, and oppressive gender relations have prevailed even as they are contested.
The following sections discuss the main findings of the study on women's lived experiences of violence in digitally mediated spaces, examining the social norms and structures that legitimize and perpetuate such violence, also making recommendations for how law and policy should provide transformative alternatives.

8.1. The loop between patriarchal norms, techno-architectures and violent gender cultures

The disinhibition that online anonymity and asynchronicity produce in social interactions[clxi] encourages self-disclosure,[clxii] potentially enabling young women to lower their guard and share more about their lives. At the same time, these very affordances also generate 'toxic disinhibition', by lowering thresholds for male assertions of patriarchal gender power.

Psychological studies demonstrate that instances of disinhibition may occur not because people are unable to control themselves, but because they fail to realize that a situation calls for self-control in the first place.[clxiii] 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.[clxiv] Platform design exploits toxic dis-inhibition, keeping individuals glued to their services. Sexist content finds currency among users and is allowed to be highly visible, but feminist content that may be unpopular is relegated to the back pages.[clxv]

When women speak up or publish their opinions, they invariably face sexist slurs. Those from dalit and minority religious communities may have to face disciplining that acquires a distinct brutality, with body shaming and malevolence targeting their social identity. Feedback systems such as comments, likes and dislikes – far from reining in sexist and misogynistic incivility – may actually exacerbate it.

The chilling effect of violence on women's participation in online spaces is well documented, and also reflected in our research. Young women withdraw from political conversations in digital spaces when attacked. Unfortunately, challenging sexist and misogynistic speech in social media is not an option; counter speech may just make women more vulnerable. Quitting the web altogether is also not realistic and may entail huge social, economic and personal costs. Instead, women adjust to unrewarding and penalising aspects of their digital lives, fashioning their presence and participation and tailoring their visibility and voice, to preclude the possibility of censure or violence.

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),[clxvi] 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"[clxvii]- of being attractive, but acceptably so.

The study was undertaken at a time when TikTok, a prominent social media video app, was becoming a rage among young people, so much so that it was even briefly banned in one of the states. The normalization of visual digital cultures accentuates the performative aspects of gender, routinizing sexualized violations. Men forge male-only online spaces to share images of women and exchange notes about their desirability and sexiness, send women unwelcome sexual imagery and even disseminate sexually explicit images of the woman 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 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.

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 reifying retrograde gender norms and practices. Emerging sociality reflects a gender conservatism, normalizing hegemonic masculinity and defensive femininity. 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 they perpetuate. 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 seige, as a largely impalpable, structural shift in the axes of public and private life is denying women a part of what it is to be fully human.

8.2 Misattributions of gender-based cyberviolence

The current legal response to violence 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). Unfortunately, obscenity-based provisions tend to be privileged by law enforcement agencies, even in cases where privacy and consent-based provisions could be used. The rationale offered by officials for this is that obscenity provisions are stricter and there is a higher chance of conviction.[clxviii] The problem with invoking obscenity provisions is that it 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.

Also, 66E itself tends to narrowly conceptualize privacy, limiting it to "the capture and transmission of images of private parts." This prevents women whose privacy is violated when unsolicited pornographic images are sent to them from seeking recourse under this section, again forcing them to turn to anti-obscenity sections for redress.

Because of a tendency to view digitally-mediated sociality in narrow binaries of online and offline, current laws also fail to capture many newly emerging forms of violence that have no pre-digital equivalent, such as gendertrolling and doxxing.

The repeal of Section 66A of the IT Act and the failure of hate speech provisions to address sexist and misogynistic hate speech have produced a legal lacuna with respect to addressing gendertrolling. In this scenario, women victims seeking legal redress are forced to invoke provisions of the IPC not originally intended to deal with cyberviolence, in particular, criminal defamation and criminal intimidation. This does not yield optimal results, as both these provisions set a very high threshold for harm. For example, in relation to the criminal intimidation provision, some courts have ruled that whether the acts of the perpetrator actually caused alarm to the victim is material to establishing the case, thus burdening the victim further in terms of furnishing proof of her charge. Also, these provisions adopt a very individual-centred notion of harm that does not capture the collective harm stemming from generalised 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.[clxix]

Doxxing is a very common form of cyberviolence, with two-thirds of the respondents who had faced violence in our study reporting it. In these cases, personal information is leaked online and becomes an open invitation for harassment, usually sexual. This is a particularly gendered crime that is not adequately covered by any current provision in the IT Act. Here again, the survivor has to fall back on anti-obscenity provisions in addition to Section 66C of the IT Act which punishes identity theft.[clxx]

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. Oftentimes, considering that local police stations tend to use legacy provisions of the Indian Penal Code rather than the IT Act, this proves a major hurdle. 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, although 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.[clxxi] 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",[clxxii] 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 world-virtual world and start understanding sociality as a human-technological hybrid.[clxxiii] 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.

8.3. The Intermediary's accountability in gender-based cyberviolence

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, hence, becomes an important actor to ensure redress for victims. However, so far, platform companies have failed to uphold this responsibility. Instead, they tend 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 longstanding 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.

In India, the legal interpretation of intermediary liability has been evolving over time. In 2014, the *Shreya Singhal vs. Union of India* judgment read down the interpretation of an intermediary's 'prior knowledge' of unlawful material to mean notification from the executive/judiciary. However, in 2018, the Supreme Court reversed this position, based on public interest litigation calling attention to the blatant publication and widespread circulation of illegal content (adverts on sex-determination tests and rape videos) online. The Court hauled up some of the

top global digital platforms such as Google, Microsoft, and Facebook, asking them to institute automated pre-emptive filtering of content.[clxxiv] This line of thinking has subsequently found place in the new set of guidelines on intermediary liability proposed by the government.

While it is true that platform companies already use AI tools for premeptive filtering and blocking for content moderation, the problem with the proposed intermediary liability guidelines tabled by the government is that it does not specify any procedures for challenging such automated decisions to reinstate content that is found to be legal or for audit of such AI tools. This can exacerbate the problem of unaccountable content governance and privatised censorship, as flagged by the critics of the new rules.

8.4 Lack of a survivor centred approach in institutional redressal

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 incursion. 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 women 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.[clxxv] 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.[clxxvi] 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.

If women do manage to make it to the police to report a crime, there are other hurdles to clear. Handing over personal devices such as phones and laptops during the course of the investigation becomes tantamount to giving the police access to all parts of one's life, including those that are irrelevant for the purposes of investigation. When the survivor's device is the only source of evidence, police officials are quick to blame the woman for deleting offensive content.

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. In their view, national security-related cyber

threats figure on top, followed by child pornography. 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 shaming 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 near-unsurmountable challenges with respect to territorial jurisdiction in cybercrimes tend to veer towards pragmatic solutions, deemphasizing legal options and turning women towards platform intermediaries for quick, low cost options. The biases of law enforcement officials also rests foundationally in and are compounded by patriarchal frameworks of prevailing laws. Laws for cyberviolence against women in particular are ineffectual in responding to the nature of harm experienced.

Women who approach the police often seek quick solutions through out-of-court settlements. The tediousness of the judicial process and prospect of facing other patriarchal actors who will sit in judgment of the survivor's character may be too much of a cost for survivors to bear. Blocking, flagging or reporting the perpetrator may work in some cases, but there is always a possibility the perpetrator may create alternate profiles to continue the harassment.

Finally, when it comes to college authorities, despite regulation mandating colleges to set up prevention of internal committees on sexual harassment, implementation leaves a lot to be desired. Colleges may not have set up such a committee or publicized its mandate. The lack of social responsiveness to and high moral panic associated with young people's sexuality also reflects in a culture of secrecy about gender-based cyberviolence. With the result that few seem to take recourse to counselling and professional psychological help.

8.5. Recommendations

For women of the born-digital generation for whom the digital is a 'rite of passage', empowerment and freedom from harm requires changes to deep culture. A society-wide norm shift straddling both formal and informal spaces is necessary to address the systemic inequalities emerging in digital sociality. The depth and breadth of action needs to encompass multiple sites – legal reform, strengthening of institutional capacities to address cyberviolence, gender-responsive platform design and inclusive digital media cultures.

8.5.1 Legal reform

The law can be a useful instrument in enabling the realisation of gender equality. Studies suggest that where anti-cyberbullying laws have been introduced, it has actually encouraged more speech by women[clxxvii]. Also, by ensuring that women's complaints are heard and challenging the normalization of online subcultures of

misogyny, law has an important role to play in its ability to shift given categories of meaning. When 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.

The anti-obscenity provisions in the Indian Penal Code and the Information Technology Act must need to make way for more empowering legal provisions that are consent driven and based on privacy, dignity and gender equality. The nature of injustices and violence meted out to women because they are women is changing. Categories of offences such as doxxing, non-consensual circulation of intimate images, and vitriolic gendertrolling reflect deep sexism and misogyny. The law needs to go beyond online-offline binaries to address this.

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 procedures for presentation and certification of digital evidence must be simplified. The more permissive reading of Section 65B of the Indian Evidence Act that allows for a waiver of the certification requirement of digital evidence in instances where a device is in adverse possession must be widely adopted, for access to justice for victims of cyberviolence.

8.5.2 Survivor-centred institutional responses

Institutional support in the case of cyberviolence needs to be survivor-centred. Systemic changes in policing are needed in order to achieve this. The trivialization and naturalization of women's experiences of hegemonic masculinity and patriarchal power in digitally-mediated spaces is a serious social anomaly. As crime is increasingly a hybrid of online and offline acts,[clxxviii] harm need not necessarily have any immediate and palpable bearing on the physical body. This is something that not only law, but law enforcement agencies, must contend with.

Capacity building programs for law enforcement officials need to go beyond technical skills and also focus on feminist perspectives on society, law and justice, including respect for women's privacy, dignity and autonomy. The overvalorization of financial frauds and terrorist activity and relative neglect of gender-based cybercrimes needs immediate correction. The Cyber Crime Prevention against Women and Children (CCPWC) Scheme launched by the centre is an important intervention. It should aim to equip police officers, judges and public prosecutors across the country with the knowledge, skills and attitude required to ensure gender equality in digital sociality.

Colleges must implement the University Grants Commission's guidelines and mandatorily set up internal committees on sexual harassment to hear cases of gender-based cyberviolence. They must promote spaces

where students can discuss and acquire perspectives and skills to communicate online respectfully as well as raise awareness of legal provisions to tackle cyberharassment and violence among the student community violence.

Counselling and psychological support for victim-survivors is a crucial area where public and private investment is needed. Educational courses to prepare a new generation of professionals to address the psychological and emotional consequences of cyberviolence among young women need to be designed and implemented using feminist frames.

8.5.3 Gender-inclusive technology architectures

Dismantling disempowering design in technological architecture is an urgent step towards gender justice. Social media platforms have been promoting safety features through better design choices – locks that prevent screen-grabs of their display pictures, digital fingerprinting of intimate images that they fear may have leaked, custom filtering, blocking abusers, flagging potential hate speech and so on. Improving structural responsiveness to cyberviolence is also equally vital. Gender-based cyberviolence needs to be treated with as much seriousness as copyright violations in the enforcement of terms of use. Timely response to content take-down requests in cases of cyberviolence and improved transparency and accountability of automated content governance systems are also foundational for women's human rights.

i Online freedom for all = no unfreedom for women, https://itforchange.net/e-vaw/
ii Pg 4, 13 https://pages.uoregon.edu/koopman/courses_readings/phil123-net/identity/palfrey-gasser_born-digital.pdf
iii Pg 4 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=898260
iv Henry, N., & Powell, A. (2014). *Beyond the "sext": Technology-facilitated sexual violence and harassment against adult women. Australian & New Zealand Journal of Criminology, 48(1), 104–118.*doi:10.1177/0004865814524218
v Henry, N., & Powell, A. (2015). Embodied Harms. Violence Against Women, 21(6), 758–779. doi:10.1177/1077801215576581
vi We were particularly interested in speaking to women journalists considering the public nature of their work and their vulnerability to violence both offline and online, https://www.article19.org/resources/unga-resolution-calls-end-attacks-women-journalists/, New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalistshttps://www.osce.org/fom/220411?download=true
vii http://main.trai.gov.in/sites/default/files/PRNo01Eng02012019.pdf
viii http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf pg 417
ix http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf pg 133
x The number of students belonging to minority communities is about the same as the state average gathered from the All India Survey of Higher Education 2017-18, which is around 6%.http://aishe.nic.in/aishe/viewDocument.action?documentId=245
xi Except for Scheduled Tribes, the number of students belong to Other Backward Castes and Scheduled Castes are significantly lower than the state average which around 48.8% and 12.37% respectively as reported by All India Survey of Higher Education 2017-18, http://aishe.nic.in/aishe/viewDocument.action?documentId=245
xii Pg 67,75 https://www.apc.org/sites/default/files/EROTICS.pdf
xiii Respondents were allowed to tick multiple options to the question
xiv http://www.pewresearch.org/fact-tank/2014/11/12/facebook-and-twitter-as-political-forums-two-different-dynamics/
xv https://journals.sagepub.com/doi/full/10.1177/2056305117691544
xvi Pg 11 https://www.academia.edu/29357034/Sexual_expression_in_social_media?auto=download
xvii This figure is consistent with other studies documenting the proliferation of cyber violence, http://www.cjcp.org.za/uploads/2/7/8/4/27845461/issuepaper13-cyberbullying-sa-impact_responses.pdf
xviii Percentage is based on the total number of people who answered Q 4.9 (do you know some other woman who has faced abuse, harassment and unwanted bhaviour online?A), which is 111
xix Internet Governance Forum (IGF) 2015: Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence Against Women describes how location, religion, gender identity, disabilities etc. influence how women get harassed and trolled online. https://www.intgovforum.org/multilingual/filedepot_download/5004/1317
xx https://www.nytimes.com/2018/05/22/opinion/india-journalists-slut-shaming-rape.html
xxi https://scroll.in/article/901889/its-bad-not-just-for-me-its-bad-for-democracy-student-leader-shehla-rashid-on-quitting-twitter
xxii Sanghapali Aruna, a dalit rights activist, speaks of the caste-based violence she faces as a user of social media https://www.firstpost.com/india/my-poster-in-jack-dorseys-hands-wasnt-the-point-real-threat-to-trolls-was-me-seeking-safety-of-oppressed-on-twitter-5590901.html
xxiii Meena Kandasamy, a writer and activist, was trolled for posting about a beef-eating festival organized by dalit groups in India. Considered sacred by Hindu, the meat of cattle is usually not consumed by upper caste Hindus. In the past three years, India has witnessed a spate of violence against minorities on basis of consumption of beef. https://www.npr.org/sections/goatsandsoda/2015/09/11/439252263/women-in-india-speak-out-on-facebook-trolls-threaten-rape-and-murder. Also, see https://www.genderit.org/articles/intersection-identities-online-gender-and-caste-based-violence
xxiv https://journalistsresource.org/studies/society/news-media/female-journalists-harassment-online-research, https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf, https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments
xxv https://philpapers.org/rec/MANGMA-4
xxvi Henry, N., & Powell, A. (2015). Embodied Harms. Violence Against Women, 21(6), 758–779.doi:10.1177/1077801215576581
xxvii Respondents were allowed to tick multiple options in response to the question on impact of abuse, harassment or unwanted behavior online on them.
xxviii https://journals.sagepub.com/doi/10.1177/1557085116654565
xxix Respondents were allowed to tick multiple options in response to the question on impact of abuse, harassment or unwanted behavior online on them.
xxx https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1268&context=yjlf
xxxi https://amnesty.org.in/campaign/online-violence-women/
xxxii https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments
xxxiii Vitis, L., & Gilmour, F. (2016). *Dick pics on blast: A woman's resistance to online sexual harassment using humour, art and Instagram. Crime, Media, Culture: An International Journal, 13(3), 335–355.*
xxxiv In a survey on employers screening candidates using social media found- 40% rejected a candidate for posting provocative or inappropriate photographs, videos or information, https://www.prnewswire.com/news-releases/more-than-half-of-employers-have-found-content-on-social-media-that-caused-them-not-to-hire-a-candidate-according-to-recent-careerbuilder-survey-300694437.html
xxxv https://jezebel.com/revenge-porn-took-my-career-the-law-couldnt-get-it-bac-1827572768
xxxvi Ferrier, M., & Garud-Patkar, N. (2018). *TrollBusters: Fighting Online Harassment of Women Journalists. Mediating Misogyny,*
xxxvii https://unesdoc.unesco.org/ark:/48223/pf0000232358
xxxviii https://www.ncbi.nlm.nih.gov/pubmed/30149282, Mills, J. S., Musto, S., Williams, L., & Tiggemann, M. (2018). "Selfie" harm: Effects on mood and body image in young women. Body Image, 27, 86–92. doi:10.1016/j.bodyim.2018.08.007
xxxix Weiser, E. B. (2015). #Me: Narcissism and its facets as predictors of selfie-posting frequency. Personality and Individual Differences, 86, 477–481. doi:10.1016/j.paid.2015.07.007

xl https://www.researchgate.net/publication/326379672_Selfie_posting_and_self-esteem_among_young_adult_women_A_mediation_model_of_positive_feedback_and_body_satisfaction
xli https://www.sciencedirect.com/science/article/pii/S0747563217306003
xlii https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828637&download=yes
xliii https://www.genderit.org/feminist-talk/no-photos-please-dating-hooking-grindr-and-notions-self-worth
xliv Rudman, L. A., & Glick, P. (2001). Prescriptive Gender Stereotypes and Backlash Toward Agentic Women. Journal of Social Issues, 57(4), 743–762. doi:10.1111/0022-4537.00239
xlv https://journals.sagepub.com/doi/abs/10.1177/1461444815604133
xlvi Pg 18 https://www.jstor.org/stable/pdf/j.ctt15nmj7f.5.pdf?refreqid=excelsior%3Ad01c7657acfed9c95fa45d9673da6da3
xlvii https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2279202&download=yes **(replacing this with https://books.google.co.in/books?id=SFph_SrDZ7gC&pg=PA197&lpg=PA197&dq=On+the+other+hand,+they+are+chastised+for+flouting+gender+norms.&source=bl&ots=qPQGCpwWoX&sig=ACfU3U1pi0u6oFwm8HM8Wr6Ed0vU6VXFXQ&hl=en&sa=X&ved=2ahUKEwiMp-eC_prkAhXKLI8KHUKVAqIQ6AEwCXoECAYQAQ#v=onepage&q=On%20the%20other%20hand%2C%20they%20are%20chastised%20for%20flouting%20gender%20norms.&f=false)**
xlviii https://www.apc.org/sites/default/files/EROTICS.pdf
xlix Veletsianos, G., Houlden, S., Hodson, J., & Gosse, C. (2018). Women scholars' experiences with online harassment and abuse: Self-protection, resistance, acceptance, and self-blame. New Media & Society, 146144481878132. doi:10.1177/1461444818781324
l From interview with a senior officer at the cybercrime police station
li Pg 426 http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf
lii https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Amrita-Anit-and-Nandini-.pdf
liii https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2018/06/State-of-West-Bengal-v.-Animesh-Boxi.pdf
liv https://indiankanoon.org/doc/110813550/
lv https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275893
lvi https://internetdemocracy.in/reports/keeping-women-safe-gender-online-harassment-and-indian-law/
lvii " 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 vs T. V. Chokkappa 1972 AIR 2609
lviii Section 503 of the IPC
lix https://www.scribd.com/doc/253395788/Posting-Comments-About-Ill-Treatment-by-Police-on-Their-FB
lx https://indiankanoon.org/doc/714505/
lxi https://indiankanoon.org/doc/775172/
lxii Gautam Bhatia, Offend Shock or Disturb 155-169
lxiii Kylie Weston-Scheuber, https://lr.law.qut.edu.au/article/view/504.
lxiv https://drive.google.com/file/d/0B1HsQbGlNpEfbVpOSHhoVVBSbXM/view
lxv Pg 16 https://www.apc.org/sites/default/files/Erotics_1_FIND.pdf
lxvi https://itforchange.net/e-vaw/wp-content/uploads/2018/03/ITFC-DISCUSSION-PAPER.pdf
lxvii Gautam Bhatia, Offend Shock or Disturb pg 107-125
lxviii https://www.huffingtonpost.in/2017/07/13/what-can-victims-of-revenge-porn-in-india-do-to-punish-the-perpe_a_23027563/ ; John A. Humbach, *The Constitution and Revenge Porn*, 35 PACE L. REV. 215, 235– 36 (2014).
lxix http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2015/02/67_Stan_L_Rev_447_Barmore.pdf, Pg 463- 464
lxx https://indconlawphil.wordpress.com/2018/09/28/the-aadhaar-judgment-and-the-constitution-i-doctrinal-inconsistencies-and-a-constitutionalism-of-convenience/
lxxi https://indiankanoon.org/doc/164014612/
lxxii https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946&download=yes page 3 **(using this instead: https://pdfs.semanticscholar.org/4dd2/f332c1367e76ca246a3848ec3f1531354edf.pdf)**
lxxiii IT has been referred to in India's first conviction for cyber-stalking although the legal provision for cyber stalking (Section 354D IPC) was not raised, https://www.hindustantimes.com/mumbai/35-yr-old-first-convict-in-a-cyber-stalking-case-in-state/story-sjIiVKJOGxwwUdr4UYyz6O.html
lxxiv https://www.argbyte.com/wp-content/uploads/2015/07/Cyber-Stalking-Yogesh-Prabhu-Court-Judgement.pdf
lxxv In the judgment, the victim argues that she sent the photos on the promise of marriage and hence trust. Although it may well be true she trusted the accused the promise of marriage may well have been highlighted to add legitimacy to the sharing of intimate pictures.
lxxvi http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2015/02/67_Stan_L_Rev_447_Barmore.pdf pg 462; Canadian law - Protecting Victims of Non-consensual Distribution of Intimate Images Act 2017 also criminalizes reckless acts of NCCII
lxxvii Sections 62 and 63 of the evidence Act.
lxxviii Aratrika Chakraborty and Anuradha Parihar, A techno legal analysis of admissibility of digital photographs as evidence & challenges, International Journal of Law pg13-14
lxxix https://cis-india.org/internet-governance/blog/anvar-v-basheer-new-old-law-of-electronic-evidence
lxxx Shafi Mohammad vs. The State of Himachal Pradesh, https://drive.google.com/file/d/1LkdljlxbADz19aS8ObebW3ZKZYxbLtbU/view
lxxxi Shafi Mohammad vs. The State of Himachal Pradesh, https://drive.google.com/file/d/1LkdljlxbADz19aS8ObebW3ZKZYxbLtbU/view
lxxxii 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.
lxxxiii http://meity.gov.in/writereaddata/files/notification-pilot-scheme-for-notifying-examiner-of-electronic-evidence-under-section-79a-of-the-information-technology-act-2000.pdf

lxxxivhttp://meity.gov.in/notification-forensic-labs-%E2%80%98examiner-electronic-evidence%E2%80%99-under-section-79a-information-technology
lxxxv https://cis-india.org/internet-governance/front-page/ip-addresses-and-identity-disclosures
lxxxvi http://www.cbi.gov.in/interpol/mlats.php
lxxxvii https://cis-india.org/internet-governance/files/mlat-report
lxxxviii https://cis-india.org/internet-governance/files/mlat-report
lxxxix https://cis-india.org/internet-governance/files/mlat-report
xc https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf
xci https://epic.org/privacy/cloud-act/
xcii https://cis-india.org/internet-governance/files/analysis-of-cloud-act-and-implications-for-india
xciii https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/
xciv http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, Pg 88
xcv https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0
xcvi https://mha.gov.in/commoncontent/sites/default/files/5%20capacity_building_advisory-2-2-18_09022018%20(4).pdf
xcvii https://mha.gov.in/commoncontent/sites/default/files/5%20capacity_building_advisory-2-2-18_09022018%20(4).pdf
xcviii https://mha.gov.in/commoncontent/sites/default/files/5%20capacity_building_advisory-2-2-18_09022018%20(4).pdf
xcix https://mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-CybercrimePrevention-against-Women-and-Children-Scheme
c https://mha.gov.in/commoncontent/sites/default/files/1.AndhraPradesh_11052018%20(2).pdf
ci Similar numbers have been reported in the media as well - https://timesofindia.indiatimes.com/city/bengaluru/at-cybercrime-station-only-26-staff-to-deal-with-over-6k-cases/articleshow/63991412.cms
cii https://phys.org/news/2018-09-hiring-female-police-officers-women.html, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2335990&download=yes **(using this instead: https://news.virginia.edu/content/study-hiring-female-police-officers-helps-women-report-violence-sexual-assault)**
ciii https://www.thehindu.com/news/cities/bangalore/cyber-crime-lab-upgraded/article26399465.ece
civ file:///home/ubuntu/Desktop/Anita/WRO%20phase%203/literature/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf
cv https://twitter.com/Manekagandhibjp/status/750623172421091328
cvi https://thewire.in/women/online-trolling-of-indian-women-is-only-an-extension-of-the-everyday-harassment-they-face
cvii http://pib.nic.in/newsite/PrintRelease.aspx?relid=183597
cviii https://cybercrime.gov.in/cybercitizen/home.htm
cix Interview with Senor officer at the CID
cx Respondents could tick multiple options
cxi https://indiankanoon.org/doc/119980704/
cxii https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/Helpline-Annual-Report.pdf
cxiii https://www.bbc.com/news/uk-37278264
cxiv European Institute of Gender Equality, Cyber violence against women and girls
cxv https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275893
cxvi https://www.livelaw.in/top-stories/abuse-of-section-66a-unconstitutional-sc-141911
cxvii Henry, N., & Powell, A. (2014). Beyond the “sext”: Technology-facilitated sexual violence and harassment against adult women. Australian & New Zealand Journal of Criminology, 48(1), 104–118. doi:10.1177/0004865814524218
cxviii "Women who do choose to report online harassment are more often than not met with the law enforcement version of a shrug," https://mic.com/articles/114964/this-is-what-happens-when-you-report-online-harassment-to-the-police#.wP4AXi585
cxix Technical officer at the CID cyberpolice station
cxx https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2018/06/State-of-West-Bengal-v.-Animesh-Boxi.pdf
cxxi http://www.gbvims.com/wp/wp-content/uploads/Interagency-GBV-Case-Management-Guidelines_Final_2017.pdf
cxxii https://www.ugc.ac.in/pdfnews/7203627_UGC_regulations-harassment.pdf
cxxiii Ploughing digital landscapes: How Facebook influences the evolution of live video streaming, https://journals.sagepub.com/doi/full/10.1177/1461444817748954
cxxiv On visual cultures - Tim Highfield & Tama Leaver (2016) Instagrammatics and digital methods: studying visual social media, from selfies and GIFs to memes and emoji, Communication Research and Practice, 2:1, 47-62, DOI: 10.1080/22041451.2016.1155332
cxxv Ploughing digital landscapes: How Facebook influences the evolution of live video streaming, https://journals.sagepub.com/doi/full/10.1177/1461444817748954
cxxvi Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms Molly Dragiewicz, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P. Suzor, Delanie Woodlock & Bridget Harris
cxxvii Cho, A. (2017). Default publicness: Queer youth of color, social media, and being outed by the machine. New Media & Society, 146144481774478.doi:10.1177/1461444817744784
cxxviii Pg 20, https://www.jstor.org/stable/pdf/j.ctt15nmj7f.5.pdf?refreqid=excelsior%3Ad01c7657acfed9c95fa45d9673da6da3
cxxix Michel Slater,https://books.google.co.in/books?id=sRsxDQAAQBAJ&printsec=frontcover&dq=inauthor:%22Michael+Salter%22&hl=en&sa=X&ved=0ahUKEwi3htbPjtHfAhUYeH0KHYeDBO4Q6AEIKjAA#v=onepage&q&f=true
cxxx #Gamergate and TheFappening: How Reddit’s algorithm, governance, and culture support toxic technocultures Adrienne Massanari, https://journals.sagepub.com/doi/abs/10.1177/1461444815608807
cxxxi http://ivc.lib.rochester.edu/google-search-hyper-visibility-as-a-means-of-rendering-black-women-and-girls-invisible/
cxxxii Cho, A. (2017). Default publicness: Queer youth of color, social media, and being outed by the machine. New Media & Society, 146144481774478.doi:10.1177/1461444817744784
cxxxiii https://www.hs-heilbronn.de/16580627/2015-baym-nancy-personal-connections-in-a-digital-age-pdf.pdf -Personal Connections in the Digital Age 2nd edition Nancy K. Baym
cxxxiv http://culturedigitally.org/wp-content/uploads/2016/06/Gillespie-Governance-ofby-Platforms-PREPRINT.pdf

cxxxv Interview with police officer in CBI
cxxxvi http://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf
cxxxvii http://culturedigitally.org/wp-content/uploads/2016/06/Gillespie-Governance-ofby-Platforms-PREPRINT.pdf
cxxxviii https://transparency.facebook.com/community-standards-enforcement
cxxxix https://indianexpress.com/article/technology/tech-news-technology/posts-on-kashmir-deities-tricolour-facebook-flags-locally-illegal-content-5536763/
cxl https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2909889&download=yes pg 10 **(using this instead)**
cxli https://newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules
cxlii https://money.cnn.com/2018/08/09/media/twitter-infowars-alex-jones/index.html
cxliii https://www.facebook.com/communitystandards/hate_speech
cxliv https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232325 pg 36
cxlv https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232325 pg 36
cxlvi https://thedailyreview.in/intermediaries-in-india-may-be-on-the-cusp-of-a-brave-new-world/
cxlvii 'In a study with academics from Cornell and the University of California, Facebook filtered users' news feeds – the flow of comments, videos, pictures and web links posted by other people in their social network. One test reduced users' exposure to their friends' "positive emotional content", resulting in fewer positive posts of their own. Another test reduced exposure to "negative emotional content" and the opposite happened. https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds
cxlviii Gupta, Apar (2007): "Liability of Intermediaries in India: From Troubled Waters to Safe Harbours", *Computer and Telecommunications Law Review*, Vol 13, No 2, pp 60
cxlix https://indiankanoon.org/doc/110813550/
cl https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193214
cli https://meity.gov.in/content/comments-suggestions-invited-draft-%E2%80%9C-information-technology-intermediary-guidelines
clii https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf
cliii https://sflc.in/our-comments-meity-draft-intermediaries-guidelines-amendment-rules-2018
cliv https://cis-india.org/internet-governance/resources/Intermediary%20Liability%20Rules%202018.pdf
clv https://thewire.in/government/liability-not-encryption-is-what-indias-new-intermediary-regulations-are-trying-to-fix
clvi https://www.diplomaticourier.com/should-artificial-intelligence-be-used-to-moderate-online-content/
clvii Text as Mask: Gender, Play, and Performance on the Internet Brenda Danet cited in Vitak, J., Chadha, K., Steiner, L., & Ashktorab, Z. (2017). Identifying Women's Experiences With and Strategies for Mitigating Negative Effects of Online Harassment. Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW '17. doi:10.1145/2998181.2998337
clviii https://warwick.ac.uk/fac/arts/english/currentstudents/undergraduate/modules/fictionnownarrativemediaandtheoryinthe21stcentury/manifestly_haraway_----_a_cyborg_manifesto_science_technology_and_socialist-feminism_in_the_....pdf
clix http://www.niemanlab.org/2018/09/google-isnt-just-a-search-engine-its-a-literal-extension-of-our-mind/
clx Griffin, M. (2010). *Webbing Cyberfeminist Practice: Communities, Pedagogies, and Social Action. Kristine Blair, Radhika Gajjalaand, and Christine Tulley (Eds.). Technical Communication Quarterly, 19(4), 455–458*
clxi Green, T., Wilhelmsen, T., Wilmots, E., Dodd, B., & Quinn, S. (2016). Social anxiety, attributes of online communication and self-disclosure across private and public Facebook communication. Computers in Human Behavior, 58, 206-213 in https://digitalcommons.cedarville.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1031&context=channels
clxii https://cyberpsychology.eu/article/view/4335/3402
clxiii https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5768638/
clxiv https://cyberpsychology.eu/article/view/4335/3402
clxv #Gamergate and TheFappening: How Reddit's algorithm, governance, and culture support toxic technocultures Adrienne Massanari, https://journals.sagepub.com/doi/abs/10.1177/1461444815608807
clxvi https://firstmonday.org/ojs/index.php/fm/article/view/9103/7717
clxvii 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, accessed 28 December 2018. cited in https://firstmonday.org/ojs/index.php/fm/article/view/9103/7717
clxviii https://itforchange.net/e-vaw/session-4/
clxix Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence, Violence against women, Henry and Powell
clxx https://indiankanoon.org/doc/164014612/, https://indiankanoon.org/doc/101769261/
clxxi https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1352442
clxxii https://law.yale.edu/system/files/documents/pdf/Intellectual_Life/ltw_fraser.pdf
clxxiii Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence, Violence against women, Henry and Powell
clxxiv https://barandbench.com/wp-content/uploads/2017/10/prajwala-order.pdf
clxxv 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
clxxvi Pg 461, 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
clxxvii https://medium.com/berkman-klein-center/can-cyber-harassment-laws-encourage-online-speech-4e1ae884bfba
clxxviii Marganski, A., & Melander, L. (2015). Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and Its Association With In-Person Dating Violence. Journal of Interpersonal Violence,

33(7), 1071–1095.