Law enforcement agencies' perceptions of gender-based cyber violence

– An ethnographic exploration of Bengaluru city cyber police

Amrita Vasudevan, Anita Gurumurthy, Nandini Chami

IT for Change

Introduction

Gender-based cyber violence, or more commonly online violence, first emerged in the Indian legal landscape a little less than two decades ago through the Information Technology Act, 2000 (IT Act) and its conception of cyber 'crime'. The Act was introduced to legitimize and promote e-commerce and reduce the risk of conducting trade online. In pursuit of the latter, the legislature introduced various sections to penalize criminal use of technology such as hacking, tampering with computer source code, causing damage to computer systems, publication or transmission of obscene content etc. In the second iteration of the Act - brought about by the 2008 amendment, the ambit of offense was increased to include sending offensive messages[1], identity theft, cheating and impersonation using computer resource, non-consensually transmitting private area of a person, etc. It also expanded upon the Section criminalizing publication and transmission of obscene content to include specific references to sexually obscene content and content that depicts children in sexually explicit acts.

The IT Act also caused the Indian Evidence Act to be amended to include electronic evidence. Sections 65A and 65B of the Evidence Act introduced criteria for the submission of digital evidence, extracted from the original instrument, in court. This includes certification 'identifying the electronic record' and details of how the electronic record was produced' signed by the person who occupies an official position with respect to the devise from which the copy of the evidence is taken. The Supreme Court of India's decision in *Anwar v. Basheer* (2012)[2] cemented the inviolability of these conditions precedent to the production of digital evidence in court.[3]

Although the sentiment of the IT Act continues to be the facilitation of e-commerce, the introduction of the new amendments has resulted in a hodge-podge of provisions that deal with anything and everything that is seen to have a causal link with the digital. From digital signatures to data protection, hacking and child pornography - the Act covers it all. In comparison to the IT Act, the Indian Penal Code (IPC) remains a largely pre-digital law, although the 2014 amendment did introduce the concept of cyber stalking.

Through this qualitative study, we would like to make some observations about the perceptions of law enforcement agencies to cases of gender-based cyber violence, specifically, the provisions of the law that they see as applicable.[4] The study was carried out by conducting interviews with

1 This provision has since been held unconstitutional by the Supreme Court's decision in Shreya Singhal v Union of India (2013) 12 S.C.C. 73

2 Anwar v. Basheer Civil Appeal 4226 of 2012

3 Post the judgment, copies of digital data can no longer be adduced, if it does not comply with the conditions set by Section 65B. https://iltb.net/new-rules-to-adduce-digital-evidence-in-courts-4c9e95e61224

4 Technology-mediated gender based violence encompasses acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies

officials of various ranks in the cyber crimes division in the city of Bengaluru and the state forensic science laboratory. Except for interviewee 5. all other interviewees are male.

Bengaluru, according to National Crime Records Bureau data, records the highest number of cyber crimes reported in the country and also happens to have an abysmal conviction rate for these kinds of crime.[5] The city has three cyber cell police stations. This study builds upon our previous work that looked at strengthening the response of the law to acts of gender-based cyber violence.[6]

Interview 1:

Our first interview was with a senior official in the cyber division of Karnataka state police. He first explained to us the law enforcement actors for cyber crime in the city. This includes the three police stations mentioned above as well as a forensic laboratory. He also informed us that the Government of India has given the State of Karnataka 19 crore INR to set up cyber police stations in every district of the state.[7] The cyber crimes police station in the city receives complaints from all parts of Karnataka.[8]

We then asked him about specifically dealing with cyber violence against women. He told us that two Acts apply in these cases - the IPC and the IT Act. The former he holds is to be used in case the violence is clearly “physical”.We pointed to the mental trauma that women and girls subject to gender-based cyber violence experience, especially through acts such as cyber stalking or non-consensual circulation of images of a sexual nature, but the officer sought to differentiate physical harm from mental harm. He also contended that “girls these days, especially urban, are well aware of the nature of the online, and know as much as the boys do about the risks online.”

On the collection of digital evidence, he was of the view that evidence was - “usually in the nature of nude pictures” - and was easy to recover. He mentioned that in cases of incessant online harassment, the girl can always just block the number, or change her own number, noting that most girls would rather block the offensive messages rather than approaching the police. Therefore, “how could the police take action when girls don’t complain?” He also noted that “girls who are educated and located in urban areas are not meek and do approach the police. In rural areas there are no mobiles and no Internet and hence such a problem does not exist.”

Asked about the response by social media platforms to requests of cooperation with law enforcement agencies, if violence is perpetrated through their services, he suggested speaking to personnel at the cyber police station for the specifics (see interview number 3).

-https://www.apc.org/sites/default/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015_0.pdf

5 http://www.indiaspend.com/cover-story/impersonation-identity-theft-most-common-cyber-crimes-reported-in-bengaluru-68907

6 https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Discussion_Paper.pdf; Although our research uses ‘technology-mediated violence against women’, the term is not used in the law, nor is it of common parlance among law enforcement officials in India. The term cyber/ online violence has been used in our interviews instead.

7 Similar grants have been made to other states as well. Home Minister for the State of Karnataka announced on a visit to Mysuru that Cyber Crime Police stations will be set up in very district of the state shortly. 50 crore INR has been set aside for technology upgrade at police stations in the state. https://starofmysore.com/cyber-crime-police-station-district-headquarters-minister/

8 https://blog.ipleaders.in/how-to-register-cyber-crime-complaint-with-cyber-cell-of-police-online-complaint-procedure/

On the low conviction rates, he opined that once technical capabilities in the forensic labs are stepped up, conviction rates will increase, and so, the financial support extended by the Government of India was a positive step in this direction.[9]

Interview 2:

The next interview was also conducted with a high ranking officer in the Bengaluru city police. He oversees the on-ground personnel who register First Information Reports of incidents of cyber crimes. He told us that most gender-based cyber violence cases that they handle deal with the circulation of obscene images. In many of these cases, the material is shared on social media, and once shared, the information is used to threaten and blackmail the women. When asked about provisions of the law that would apply in cases of cyber crime, he stated that both IPC and IT Act apply. Bemoaning "the death of common sense necessary in online behavior", he observed that "women in these cases fail to exercise caution". Additionally, he noted, teenagers are especially susceptible to sharing private information. He also held that such sharing of material is different from cases of credit card fraud or where there is hacking and information is being stolen (economic offenses), where the victim is either caught unawares or is duped. The latter are "genuine crimes".

On the cooperation extended by social media companies in redressing the violence carried out on their platforms, the officer said that it depends on the company. In his experience, Facebook has a policy of sharing user information/data while WhatsApp does not. He also referred to the raid conducted by the Mangaluru police on Facebook's office in Maharashtra last year. The raid took place because of Facebook's refusal to respond to the request for information from the police regarding certain derogatory posts of a religious nature that were shared on the platform.[10]

The interviewee then referred us to two officials who investigate cyber crimes on the ground.

Interviews 3 and 4:

Two officials investigating cyber crimes met with us at the police station. We continued our query on the role of social media companies in the law enforcement process. Interviewee 3 remarked that WhatsApp does not hand over user data, but does provide the IMEI number of the handset in which the application was first installed. They also do store the origin and destination data of a communication, but it was not clear if this information is shared with law enforcement. Further, since WhatsApp uses 'end to end' encryption, interception becomes very difficult because of the large volumes of data that would have to be stored.[11] Facebook on the other hand, we were told, stores data on most activities (posts, likes, shares etc) that take place on its platform and has unique links to each of this information. In cases where this information is shared, the police can, through "reverse engineering", trace the possible origin of the crime. The official was however quick to warn that in case of cyber crimes, technology alone cannot be relied on to provide solutions, and that old fashioned human capacity necessary for appropriate and astute investigation was equally important.

9 The Union budget 2017-18 set aside 18, 636 crore INR for the modernization of police forces, http://indianexpress.com/article/india/rajnath-singh-ccs-pm-modi-government-approves-rs-25000-crore-umbrella-scheme-for-police-reforms-4864331/

10 http://www.coastaldigest.com/news/94070-mangaluru-police-raid-facebooks-mumbai-office-over-non-cooperation

11 The volume can be so large that it can bring down servers.

Interviewee 3 also disclosed to us that although Facebook was willing to share user data, they take 20 to 30 days to respond, during which time the company ensures that all internal rules and standards are complied with. To reach out to Facebook, the police sends an e-mail (with an ID that is registered with the company) requesting the IP address (in order to trace the accused). Because the turn around is delayed, police are often forced to pursue other means to secure evidence. In some cases, Facebook will not share information if they think an offense has not occurred according to their internal rules. For example, whether something is obscene can become a point of dispute between the company and the police. In case Facebook refuses to share information, police have to rely on the complainant's evidence. In any case, sole reliance cannot be placed on evidence given by Facebook. So, for example, in case of the publication of an "obscene" image, "a screenshot of the image is taken, following which it is sent to the forensic lab, which will verify its genuineness".

Interviewee 4 concurred with Interviewee 3 - that circulation of obscene content was the most common case on gender-based cyber violence they received. Most cases were between intimate partners who have parted ways. The officer also pointed out that "privacy and consent in a world run by apps is an obsolete concept, because the user allows companies unrestricted access to their phone galleries, which may contain private images, or monitor location data."

With respect to the circulation of obscene content, the most commonly applied Sections were 67A (which penalizes publication and transmission of sexually explicit content) and 67B (which penalizes publication and transmission of content that depict children in sexually explicit acts) of the IT Act. Because Section 66E of the IT Act (adopts a 'violation of consent' approach to penalizing non consensual circulation of images of private parts) can overlap with Section 67(A) , we wanted to know how the official determines which Section would be applied. Interviewee 3 answered that it would depend on the evidence available. He then proceeded to open and read the statute book at the police station. He pointed to examples listed under Section 66E that dealt with surreptitious video recording – like a CCTV in a changing room. Therefore, he asserted that "in cases where intimate pictures are shared voluntarily at first instance, and are subsequently recirculated, no privacy may be breached and hence Section 66E will not be applicable." This limited reading of privacy we also observe in the language of the law.[12]

When asked about cyber stalking in particular, he disclosed that it was another area in which they received complaints. For these cases, the police applied Section 354 D of the IPC (concerning 'following a woman and attempts to contact her'). Regarding the warning put up on the Bengaluru City Police website of the cyber crime- 'matrimonial fraud'[13], Interviewee 3 explained that women registered on these sites are often duped by men who siphon money from them.[14]

Interviewee 4 informed us that from March 2017, around 200-300 cases of cyber crimes against women, but very few on minors.[15] After a complaint is received, the laptop, mobile phone etc. of the

12 Section 66E- 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

13 http://www.bcp.gov.in/Cyber_Crime_Police_Station.aspx

14 http://indianexpress.com/article/cities/pune/fraud-on-matrimonial-networking-sites-cyber-police-register-62-cases-since-january-2016-4422853/

15 UNICEF reports that very few cases of cyber violence against minors get reported and even fewer reach conviction in India. The report quotes a 2012 study carried out by Microsoft which ranked India third among the 25 countries studied for cyber-bullying of minors. http://unicef.in/PressReleases/418/UNICEF-India-launches-the-first-comprehensive-report-on-Child-Onl

complainant are seized for investigation. Interviewee 3 believes that the complainant is best placed in relation to their device to produce appropriate evidence. However, he does recognize that complainants may be reluctant to give up all devices and information, for it may be compromising, sensitive, and/ or embarrassing. The officer offered an example to illustrate the dilemmas involved in investigating cyber crimes: suppose a husband and wife approach a police officer in a case of the wife being harassed through her mobile. The investigation could throw up evidence of the wife's extra-marital relationship with the accused that later turned into harassment. The investigating officer here is placed in a tough position. His or her consideration cannot be only legal. The official will need to consider privacy, security and dignity, as well as psychological, social and economic factors, as also being important.

Interviewee 3 informed us that through mutual legal assistance treaties (MLAT), which India has signed with 33 countries including the US, the police is able to request and receive data even when stored on foreign servers. These treaties are essential, without which even if the accused and complainant are in resident in India, if the server is located in a foreign jurisdiction, the data cannot be accessed. But under the treaty, data can be retrieved only if the domestic offense is also recognized to be an offense in the foreign country. The police can take Interpol's assistance too if need be. Further, the official informed us that despite arguments of lack of jurisdiction, the raid by the Mangaluru police on Facebook's office was possible because, during investigation police have ample powers and under Section 91 of CrPC[16], and the investigating officer can ask for even digital evidence to be produced. The officer can also summon anyone, any number of times, as long as it is reasonable.

To questions of private public partnerships (PPPs) in investigating cyber-crimes, Interviewee 3 responded positively. He thinks that PPP can be useful (he is not referring to equipment, but expertise) but must be backed by strict legal provisions (contractual) that will hold private actors accountable since they will be handling sensitive data. Thus, they must be legally bound.

When the interviewees were asked whether threatening messages that are not sexual in nature can be considered to be gender-based violence, Interviewee 4 disagreed. He blames the proliferation of gender-based cyber crimes on "globalization" and "the influence of western culture". Self-awareness and self policing, he believes, is key, and schools can be roped in to raise awareness not only about gender-based cyber violence, but also other kinds of cyber crimes.

Interview 5:

The fifth interview we conducted was with an official at the Katakana State Forensic Science Laboratory. She explained to us that the role of the lab was to assist the investigating officer (IO) by analyzing the digital evidence submitted.

She recounted a number of challenges in recovering digital evidence. One major problem is that IO's are poorly trained and as technology becomes more complex, so do the crimes that are

16 91. Summons to produce document or other thing.
(1) Whenever any Court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order

mediated through them. Senior IOs approaching retirement are less receptive to new training, and as a result, the knowledge fails to trickle down to the junior officers. She pointed to instances when the lab would receive monitors instead of the CPU and without access to the necessary hardware/ artifacts, she explained, recovery of data (evidence) was not possible. A greater effort is being made currently to train IOs properly, and experts from industry are also invited for these trainings.[17]

Next, she observed that as devices become more sophisticated, breaking through them to extract evidence becomes increasingly difficult. For mobile phones, especially the newer versions of Android and iOS, bypassing the password lock is itself a hurdle. Even if evidence is recoverable, victims are not always comfortable handing over their devices for the fear of unrestricted access to information (some which may have no evidentiary value), and consequently, their personal lives. She did note that when the devise is seized, information is extracted in read-only mode and hash value of the file is calculated. Both of these measures ensure that files are not tampered with. She made it clear that since extraction takes place through bit-imaging[18], it is impossible to be selective of what will be extracted, but only that evidence that the IO asks for is finally shared. Strict action is taken in case any evidence is leaked by law enforcement officials.

When queried about whether the forensic lab interacts with transnational corporations like Facebook or Google etc., to recover evidence, she answered in the affirmative, confirming what Interviewee 3 told that if information is required from foreign servers, the offense must be criminal in the foreign jurisdictions as well. The level of support these transnational digital corporations extend to law enforcement agencies varies. In the officer's experience, Facebook did not respond favorably to requests for take-down of material and blocking of profiles. She recounted an experience where the complainant approached the police to take down images of hers that were morphed to add traditional markings/symbols of being married, when she in fact she was not. Not understanding the cultural significance of the issue and moreover, not seeing it as a violation of community guidelines, Facebook refused to take the image down. The officer also told us that WhatsApp's end to end encryption policy also made it difficult for the police to work with them.

When asked about the steep incline on the occurrence of cyber violence, she pointed to the ubiquity of the smart phone and the increased access to the Internet, both brought about by the fall in their prices.

She concluded by stating that the forensic lab was receiving adequate funding from the state and is able to invest in state of art equipment.

17 Indian Computer Emergency Response Team (CERT-In), Centre for Development of Advanced Computing (CDAC) and the Cyber forensics training lab set up at the Training Academy of Central Bureau of Investigation (CBI) all conduct basic training of officers. http://mha1.nic.in/par2013/par2013-pdfs/ls-050313/LSQ.1335.Eng.pdf

18 Bit imaging ,also referred to as forensic imaging, is a method of evidence extraction to ensure the original media is not modified and that the copy accurately reflects the original. Further, following a chain of custody (documentation of who all have handled the evidence https://uppolice.gov.in/writereaddata/uploaded-content/Web_Page/28_5_2014_17_4_36_Cyber_Crime_Investigation_Manual.pdf Pg 37) and hashing the files can help evidence the integrity of data. https://www.forensicon.com/resources/articles/what-is-forensic-hard-drive-imaging/

Discussion and Recommendations

Based on the interviews conducted, some inferences and observations are discussed below.

1. Gendered biases and blindspots in the reading of the issue

The perceptions reveal gender biases at various levels of law enforcement. This is not to imply that an empathetic and sensitive approach to women victims is absent, but as has been discussed in other reports[19], it is an exception. Enforcement embedded in patriarchy results in actions whose characterization ranges from avuncular to dereliction. At the more benign end of the spectrum is the view that technology is a western tool that can corrupt women. In multiple interviews, we observed an approach that insists that women should apply their 'common sense' and self-police. The assumption of a lapse in judgment is tied to the perception that the complainant herself is complicit in the crime committed and hence not a 'genuine victim'. The extent of self-policing is infinitely extendable - 'do not share nude pictures'/'do not share phone number'/'do not accept the friend request'/'do not go online' and so is the blame. There is also the expectation that the woman should deal with the issue on her own because the technology allows for blocking the offender by intervention at the complainant's level itself. The inability to perceive culpability of male offenders, and the equality, dignity and privacy of women victims in such contexts, suggests a trivialization and naturalization of what in essence comprise criminal acts.

Towards the other end of the spectrum lies the denial of criminality brought on by the notion that gender-based cyber violence does not implicate the body. There is a perception that IPC deals only with harms against the body, and hence its provisions on violence against women do not apply to cyber violence against women (the cyber being thus construed as non-embodied). This is a major blow for those who do choose legal recourse and depend on the creative application of the IPC to the digital space. It also ignores criminality not attached to the physical body seen in several sections of the IPC such as those dealing with defamation, contempt, cruelty by husband and/or his family against the wife, etc.

There is also an assumption that technology is an equalizer that allows girls to behave just as boys are able to. Apart from obfuscating the particular vulnerabilities that women face in navigating the digital, this assumption also squarely pushes aside real concerns of patriarchal judgment meted out to women by law enforcement and that results in under reporting of gender-based cyber violence.

2. Difficulties with digital evidence

- Opening the floodgate of personal information

Officials investigating gender-based cyber crimes routinely have to deal with a range of complex factors that implicate intimate information about victims. Victims' willingness to be part of the investigation is vital. However, owing to the risk of loss of privacy and associated social stigma/ shame, victims often do not want to persevere on the long path to justice. Invasion of privacy during

19 https://internetdemocracy.in/wp-content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf, http://theladiesfinger.com/the-policeman-said-why-dont-you-tell-me-what-gaalis-he-whispers-in-your-ear/

the collection of digital evidence is of a different order because of the threat of instant publicity and public disclosure that it allows. In a landmark decision in 2014, the American Supreme Court observed the recovery of evidence from the modern phone has unprecedented implication on the right to privacy, drawing an analogy of the search of a mobile with that of an entire house.[20] In India, a wide berth is given to law enforcement, whether in the Criminal Procedure Code or the IT Act (and its rules) for the discovery of evidence, with only minimal restriction, such as the prevention of disclosure to unauthorized persons punishable under section 72 of the IT Act. Further, evidence collected in violation of the restrictions imposed is still admissible in court.[21] Post the Right to Privacy judgment, collection of digital evidence and its forensic examination is an area that is in critical need of re-evaluation.

- Non-cooperation by private actors

The responses about social media companies indicates a strong ambivalence. The police seem fairly confident of recovering digital evidence possessed by transnational digital corporations, even pointing out to forceful recovery by the Mangaluru police of evidence from Facebook's office in Mumbai. However, the all-too-common experience about delays in obtaining evidence, inability to get evidence because of end-to-end encryption and difficulties in overruling community standards of social media companies to take action suggests an impasse that can be costly for victims.

Corporations also refuse to abide by directives for evidence recovery from government agencies, citing jurisdictional immunity from the host country's laws because they are headquartered in a foreign jurisdiction or because the server where the evidence is stored is not located in the host country's soil.[22] MLATs have not always been effective, and the slow turn-around by the police, as pointed by the interviewees, can make evidence collection difficult.[23]

- Catch 22 in evidence collection, and the risk of inaction

The difficulty in collecting digital evidence is compounded by legal requirements for it to be produce-able in court. In a news report, a police officer from the cyber division in Bengaluru commented upon the court's lack of 'appreciation' for such evidence.[24] When costs of securing and producing digital evidence become prohibitively high, there is a likelihood that the police will stay away from cases where complaints cannot be converted to conviction,[25] aggravating the discounting of gender-based cyber violence.

20 http://www.transperfectlegal.com/downloads/pdfs/The_Cost_of_Privacy_Riley_V_California.pdf
21 https://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age
22 http://perry4law.org/clic/?p=66, http://perry4law.org/clic/?p=52
23 https://timesofindia.indiatimes.com/city/hyderabad/cyber-crime-cases-stuck-in-red-tape-info-from-global-servers-out-of-reach-for-cops/articleshow/62091706.cms
24 http://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html
25 https://scroll.in/article/860254/what-the-national-crime-records-bureau-report-does-not-tell-us-about-cyber-crime-in-india, http://www.livemint.com/Politics/St93190XdGvpiclGWwnX0I/For-victims-of-cyber-stalking-justice-is-elusive.html

The government has taken some positive steps to reconciling these difficulties, for instance early last year the government set up 'Examiners of Electronic Evidence' (as per Section 79A of the IT Act) who would authenticate the veracity of digital evidence when it is produced in court.[26]

Further, digital evidence is particularly vulnerable to manipulation and tampering. Its lack of authenticity is likely to lead to its dismissal by the court.[27] To override the court's concern, states must adopt a standard operating procedure while collecting digital evidence. The Central Board of Direct Taxes' 'Digital Evidence Investigation Manual'[28] and Data Security Counsel of India's (DSCI) 'Cyber Crime Investigation Manual' is a good starting point.[29]

- Insufficient capacity building

Although police officers we interviewed on the frontline seem well informed and interviewee 5 was optimistic about the training police officials were receiving, the capabilities are far from even. As a Metropolitan Magistrate in Delhi commented, "lack of knowledge about mobile/computer forensic not only scuttles the investigation, but adversely affects the administration of justice'.[30] Although Karnataka records the third highest instances of cyber crimes, as per the National Cimes Record Bureau's Crimes in India report[31], in 2016-17, only one cyber training was organised by the government. This was a refresher course -'Surveillance Intelligence and Cyber Crime Investigation' and had only 21 participants.[32]

The January 2018, Ministry of Home Affairs advisory on 'cyber crime prevention and control' has recommended capacity building measures for police officials, public prosecutors as well as judicial officers. Some of these measures include 'training in basic cyber awareness, forensic investigation, and legal analysis'. The advisory also recommends that states and UTs organize "capacity building programme for prevention of cybercrime against women and children"[33] While the advisory is timely and considering the layout has been made under the Cyber Crime Prevention against Women and Children Scheme through the Nirbhaya Fund[34] a well laid out plan that addresses in particular gender-based cyber violence is necessary

3. An incomplete law compounds the static interpretation of 'consent'

Section 66E of the IT Act is pivoted around privacy and consent of a person, but as stated earlier, the expectation of privacy is limited to when the person whose privacy is violated is unaware that their image is being captured. What is referred to as 'revenge porn'- where an intimate image

26 https://economictimes.indiatimes.com/news/politics-and-nation/india-to-finally-get-electronic-evidence-authenticators/articleshow/56370238.cms
27 http://www.tehelka.com/2017/03/e-evidence-gradually-becomes-a-crucial-part-of-prosecution/
28 http://www.itatonline.org/info/?dl_id=1692
29 DSCI in 2007 set up a Cyber Lab within the Cyber Crime Police Station,Bengaluru . We suspect the procedure for recovery of evidence already follows the manuals recommendations.https://uppolice.gov.in/writereaddata/uploaded-content/Web_Page/28_5_2014_17_4_36_Cyber_Crime_Investigation_Manual.pdf.
30 http://indianexpress.com/article/india/india-news-india/delhi-police-court-training-probe-electronic-knowledge-forensic-techniques-police-investigation-2817038/
31 http://www.thesoftcopy.in/20102016_leo_cyber%20crimes.html
32 http://home.kar.nic.in/download_files/Annaul%20Report%20English.pdf
33 http://www.mha.nic.in/sites/upload_files/mha/files/CyberCrimeprevention_15012018.PDF
34 http://www.mha.nic.in/sites/upload_files/mha/files/CyberCrimeprevention_15012018.PDF

maybe shared voluntarily in the first instance, but circulated without the consent of the person who shared it, is not covered by such a law, even though it should have been in its logical arc of action to do so. Further, while Section 354C IPC (penalizing voyeurism) deals with secret capturing of a woman in a place or a circumstance where she can expect privacy, and also when a woman 'consents to the capture of the images or any act', it does not cover non-consensual dissemination by third persons.

In respect Section 66A of the IT Act, law enforcement officials seem to adopt a literal interpretation, seeing non consensual dissemination that may follow consensual sharing as a social inevitability that cannot be booked under the Section. They believe that in such instances the loss of privacy and agency is a foregone conclusion.

However, beyond the first non-consensual circulation, further dissemination of the image by those who receive it is also a violation of the woman's privacy. Understandably, this may be difficult for the police to act upon. The stop-gap solution it seems is to criminalize the act under the existing law on obscenity. This fracture between the law's lexicon and definitions of criminal conduct on the one hand and the victim's experience of harm on the other must be addressed for law enforcement to be effective.

4. Culturally located interpretation of cyber crimes

The police tend view financial frauds on matrimonial sites as gender-based, as women tend to be the majority of the victims in these cases. There seems to be a greater recognition of 'victimhood' in such cases, given the economic nature of the harm. Possibly, the fact that these women were entering into a socially 'approved' relationship lends weight to their perception as 'genuine' victims. Multiple interviewees, as recounted above, believe cyber violence that was economic was more serious than gender based cyber-violence. Further, one interviewee also held that sexist hate speech not directed at a particular woman (but reflecting misogyny) cannot be counted as violence. The reading of the hate speech law is also similar. Structural discrimination by law and law enforcement is not recognized

5. Receptiveness to the involvement of private actors

Despite problems in dealing with foreign corporations to access citizen data or request take downs, the officials were keen on PPPs and foreign supply of forensic equipment backed merely by contractual protections. The Supreme Court's confirmation of the Right to Privacy and incremental steps towards a data protection framework in the country[35] leave us hopeful that we will not be left to the mercy of a contract.

35 http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf