Safecity's Submission on Online Violence against Women to the UN OHCHR

by Adriana Rakshana*, Sanaya Patel**, and Vandita Morarka***
Policy and Legal Team,
Safecity: Red Dot Foundation

The United Nations Human Rights Office of the High Commissioner put out a call for submissions on online violence against women:

"The Special Rapporteur seeks to collect existing good practices on law regulating violence against women and sexual harassment online. In order to inform her work on the topic, which will culminate in the presentation of a report to the Human Rights Council in June 2018, the Special Rapporteur wishes to secure from different stakeholders, including States, National Human Rights Institutions, Non-governmental organizations, as well as members of academia, input and views on the following topics:

- Existing legislative models, criminal or administrative, on prosecuting and punishing various forms of online violence against women;
- Existing policies that allow identification, reporting and rectification of incidents of harassment or violence against women via the internet services providers;
- Existing jurisprudence from international, regional, and national courts, on prosecution or administrative proceedings in such cases."

The Policy and Legal team at Safecity drafted the following submissions, under the provided themes, towards supporting the building of solutions to tackle online violence against women. A compilation of the three submissions is provided here.

*Adriana Rakshana is a Research Assistant at Safecity.
**Sanaya Patel is a Research Assistant at Safecity.
***Vandita Morarka is the Policy, Legal and United Liaisons Officer at Safecity.

I. Existing legislative models, criminal or administrative, on prosecuting and punishing various forms of online violence against women

Although India does not have extensive laws dealing specifically with online violence against women, there are cyber crime laws and sexual harassment laws that can be applied to prosecute and punish various forms of online violence against women.

Information Technology Act 2008

In India, the key law that deals with cyber crime is the *Information Technology Act, 2008* (IT Act), that punishes 'transmission of obscene as well as sexually explicit content in electronic form.' Thus, there does exist a limited legislative model that acknowledges sexual harassment online.

Sections 66 and 67 of The IT Act acknowledge the most common acts of internet violence, however once again not in a very specific manner which can be both a bane and a boon. A bane because a lot of different types of offences are not accounted for specifically, however, a boon because the broad wording allows for applicability to most general situations. Some of what is outlined in the IT Act includes identity theft[1], which can result in imprisonment of up to three years as well as a fine, and the transmission of obscene materials electronically[2], which can result in imprisonment of up to five years and a fine. Offences such as intimidation, insult,

[1] 66C. Punishment for identity theft. -
Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

[2] 67. Punishment for publishing or transmitting obscene material in electronic form. -
Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

annoying, harassment and defamation in the cyberspace were punishable only under the Indian Penal code till the 2008 amendment to the IT Act[3]. Nonetheless, the IT Act is very limited in its considerations. There is currently a section being drafted to consider "spoofs and hate speeches, as well as online voyeurism, online cheating, hoax calls, and permitting investigations by officers below the rank of inspector,[4]" given the section that previously dealt with such topics of offences through 'electronic communication services,' 66A, was deemed unconstitutional due to its vagueness that impeded general free speech. Email harassment is very similar to harassing through letters; however, it is fairly difficult to prosecute the culprits of crime in cyber harassment as often people create fake identities for such purposes which may or may not be a culpable offence depending on the use of the fake identities.

Cyber libel and defamation are also forms of injustice conducted against women. The credibility of the IT Act 2000 was improved upon by a well founded amendment of 2008 which incorporates a body corporate within its scope. In the 2008 Amendment to the IT Act, Section 43A was added to include a "body corporate" within its scope, allowing compensation in case a company or firm causes wrongful loss or wrongful gain to any person by way of handling sensitive information and maintaining the security of such. The body will face civil liability under negligence in case "reasonable security practices and procedures" are not followed[5].

'Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation.' The Act causes the corporate body to face civil liability under nuisance[6].

---

[3]LawRato. "Everything You Need to Know About Cyberbullying and How to Stop It." *The Better India*, 19 Oct. 2016, www.thebetterindia.com/71909/cyberbullying-it-act-2000-cyber-law-in-india/. Accessed 17 Aug. 2017.

[4]"Govt almost ready with 'more specific' replacement for Section 66A of IT Act." *CatchNews.com*, www.catchnews.com/national-news/govt-almost-ready-with-more-specific-replacement-for-section-66a-of-it-act-1456452719.html. Accessed 17 Aug. 2017.

[5] Furtado, Rebecca. "Cyberstalking: A Crime or A Tort." *IPleaders*, 8 Aug. 2016, blog.ipleaders.in/cyberstalking-crime-tort/. Accessed 17 Aug. 2017.

[6] Ibid.

The objective of the IT Act is clear from its preamble which confirms that it was formed largely for improving e-commerce hence it covers commercial or economic crimes i.e. hacking, fraud, and breach of confidentiality etc. but not as effective for the protection of net users.

The Indian Penal Code 1860

The *Indian Penal Code, 1860* (IPC) outlines how sexual harassment is dealt with in India, and its provisions are equally applicable to online sexual harassment.

Section 354-A of the IPC deals with sexual harassment. Its definition includes demands or requests for sexual favours, showing pornography against the will of a woman, or making sexually coloured remarks. This includes cases of online harassment, such as demands for nude pictures, sending pornography via the internet, and leaving unsolicited comments on a woman's social media page.

Section 354-C of the IPC deals with voyeurism. Voyeurism is an act done by a man, of watching or capturing the image of a woman engaging in a private act. A sexual act or the act of bathing or using the toilet would be covered, as these are acts not ordinarily done in public. The section also covers cases in which a woman may consent to being photographed, captured on video or watched by a man but does not consent to such content being disseminated. Cases of revenge porn would fall squarely within section 354-C.

Section 354-D of the IPC deals with stalking. Stalking is defined as the act of following and attempting to communicate with a woman despite clear indication of disinterest by such woman. The definition includes the act of any man who "monitors the use by a woman of the internet, email or any other form of electronic communication". Lewd messages sent over WhatsApp, Facebook, Twitter, would fall within the ambit of Stalking under section 354-D.

In a recent case, a security guard in Pune, Maharashtra, obtained the phone number of a woman and subsequently harassed her through continuous phone calls and Whatsapp

messages. The man was convicted under Section 354-D within 48 hours of the case reaching the court.[7]

Section 509 of the IPC deals with words, gestures and acts intended on insulting the modesty of the woman. Intrusion of the privacy of a woman is also dealt with under this section. In what is considered one of India's first cyberstalking cases, Manish Kathuria was arrested under Section 509 of the Indian Penal Code for stalking and harassing an Indian woman via the internet.[8]

In Maharashtra's first conviction of a cyberstalking case in 2015, a 35 year old man was convicted for sending obscene pictures and videos via email, to a woman he met on a social networking site. He was convicted under section 509 (word, gesture or act intended to insult the modesty of a woman) of the IPC and section 66 (E) (punishment for violation of privacy) of the Information Technology Act, 2008.[9]

It is key to note that in India, a large number of the current sexual harassment and stalking laws only apply to women given the prevalence of such crimes against women in India.
Section 499 of the IPC defines defamation, under which a person could be convicted for publication of content and imputations regarding a woman, with the intent to injure her reputation. This section can be invoked in cases of online harassment where the accused publishes information or obscene pictures or videos of a woman on a public forum such as a social networking website.

Section 503 of the IPC deals with criminal intimidation, which includes threats made to injure another person's reputation with the intent to either cause alarm to that person or to induce that person to do any act that he is not legally bound to do. Threatening messages sent via the

---

[7] Joshi, Yogesh. "Justice in 48 hours: Pune man sentenced to 2 years for molesting girl." *Hindustan Times*, 11 Jan. 2017, www.hindustantimes.com/mumbai-news/justice-in-48-hours-pune-man-sentenced-to-2-years-for-molesting-girl/story-fSmW6NOHuqF1HdpGmvYK8M.html. Accessed 17 Aug. 2017.

[8] Soman, Sandhya. "Cyberstalking makes first entry into legal debate." *Times of India epaper, 18 March 2013,* http://epaper.timesofindia.com/Repository/ml.asp?Ref=VE9JQ0gvMjAxMy8wMy8xOCNBcjAwNDAy, Accessed 27 October 2017.

[9] Kumar Yadav, Vijay & Shah, Charul. "35-yr-old first convict in a cyber-stalking case in state". *Hindustan Times,* http://www.hindustantimes.com/mumbai/35-yr-old-first-convict-in-a-cyber-stalking-case-in-state/story-sjIiVKJOGxwwUdr4UYyz6O.html. Accessed 12 August 2017.

internet would fall within the purview of this section. Cases in which a person may threaten to publish nude photographs of a person online, with the intention to cause distress to that person, would also fall within this section.

Revenge Porn Laws in India

'Revenge porn' is the publication of explicit material portraying someone who has not consented for the image or video to be shared[10]. There is no law in India specifically directed against revenge porn and its victims. In India, the IT Act and the Indian Penal Code work together to tackle revenge porn cases, primarily Sections 67 and 67A of the IT Act.

Sections 67 and 67A of the IT Act are against the publishing and circulation of what the act calls 'obscene' or 'lascivious' content. Section 67 states that "If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it." This can result in a jail sentence for up to five years and/ or a fine of up to 100,000 rupees. Section 67A extends the law to a person "who publishes or transmits images containing a sexual explicit act or conduct". Even PhotoShopped or morphed images are covered by this Act.This can result in a jail sentence for up to seven years and/ or a fine of up to 100,000 rupees.

If the victim of revenge porn is under 18 years, then the crime is treated as child pornography i.e. publishing or transmitting in electronic form of material depicting children in obscene, indecent or sexually explicit manner. The crime is punishable under Section 67B of the IT Act with a punishment of up to seven years in prison and a fine of up to a million rupees[11]. However, both sections 67 and 67A are aimed towards preventing the spread of pornography and hence

---

[10] Barrett, David. "What is the law on revenge porn?" *The Telegraph*, Telegraph Media Group, 13 Apr. 2015, www.telegraph.co.uk/news/uknews/law-and-order/11531954/What-is-the-law-on-revenge-porn.html. Accessed 17 Aug. 2017.

[11] Dasgupta, Piyasree. "Why We Need A Specific Law Against Revenge Porn In India Immediately." *Huffington Post India*, HuffPost, 14 July 2017, www.huffingtonpost.in/2017/07/13/what-can-victims-of-revenge-porn-in-india-do-to-punish-the-perpe_a_23027563/. Accessed 17 Aug. 2017.

the victim can also be booked under the law for taking the picture. However, fortunately, the police have not booked any victim of revenge porn under these sections as of yet. Nonetheless, it still is true that the decision of whether to charge the victim lies under the discretion of the police officer in charge of the case which is absolutely egregious.

Moreover, there is no ruling that makes it mandatory that a woman's complaint is heard and lodged by a female police officer which can be very uncomfortable for the victim who may not at all be comfortable discussing such personal information with anyone let alone a male police officer. It is important that the law be altered in order to make such investigation more comfortable for women by making it mandatory for female officers to be present and the primary point of contact for the victims.

Legislation to curb online harassment of women in India

Overall, majority of cyber-crimes are prosecuted under Sections 66 (Hacking), 67 (publishing or transmitting obscene material in electronic form), 72 (breach of confidentiality) or the provisions related to sexual harassment under the IPC[12]. The existing legislative models to prosecute online violence against women are very limited but do exist.

New Zealand's *Harmful Digital Communications Act, 2015*[13] was enacted for the twofold purpose of deterring and mitigating harm caused by digital communication, and to provide victims of such harm with speedy and effective redress. The Act states the factors which the court would consider in deciding cases of harm by digital communication. The Act also lays down conditions of liability of the online host[14] in instances of online harassment. Interestingly, the Act also lays down principles of digital communication in Section 6[15], which state that online communication should not be threatening, menacing, indecent or obscene, and should not be used to harass an individual.

[12]Misra, Rajat. "Cyber Crime Against Women." *SSRN*, 20 Sept. 2014, ssrn.com/abstract=2486125. Accessed 17 Aug. 2017.
[13] New Zealand. "Harmful Digital Communications Act." 2015.
[14] Section 23, Liability of online content host for content posted by user. New Zealand. "Harmful Digital Communications Act." 2015.
[15] Section 6, Communication principles. New Zealand. "Harmful Digital Communications Act." 2015.

Importing certain sections from New Zealand's law to build a comprehensive legislation in India related to online abuse would clarify the rules of conduct expected from all Indian citizens while interacting with fellow internet users. Identifying the major stakeholders - users, online hosts or internet providers, and the government, and defining their roles and liability in the event of online harassment would create an efficient system of justice and redressal of grievances for women who deal with online violence. The UK's *Sexual Offences (Amendment) Act, 1992*[16] contains a provision which mandates that the identity of the victim of sexual offences be concealed. No matter that is likely to lead to the identification of the victim (the complainant) is allowed to be published in England.

Introducing a legislative provision which allows for anonymity of victims of sexual offences in India, especially in cases of online violence, would greatly increase the feeling of safety amongst women who want to report such cases but refrain from doing so in fear of societal backlash or being subject to further abuse.

Safecity's work towards building solutions

Safecity is a platform that crowdsources personal stories of sexual harassment and abuse in public spaces. We are registered as a not for profit in the United States as Red Dot Foundation Global and in India as Red Dot Foundation. This data which may be anonymous, gets aggregated as hot spots on a map indicating trends at a local level. The idea is to make this data useful for individuals, local communities and local administration to identify factors that cause behaviour that lead to violence and work on strategies for solutions. Such crowdmapping helps us account for those numbers that do not find place in formal reporting, creating a larger data driven evidence base for advocating changes in law and policy.

Since our launch on 26 December 2012, we have collected over 10,000 stories from over 50 cities in India, Kenya, Cameroon, Nepal, Nigeria and Trinidad & Tobago and directly reached over 4,00,000 people. To ensure wide access, we also facilitate report collection by way of a missed call to +91 9015510510, where our team then calls the person back. Our report trends are submitted to police bodies in different states of India and help inform police action, such as increased vigilance and changing beat patrol timings Our interventions have also resulted in

[16] United Kingdom. "Sexual Offences (Amendment) Act." 1992.

municipal corporations fixing street lighting and in making safe public toilets available for women to reduce sexual violence, transportation authorities have also issued women only bus licences in Kathmandu as a result of our advocacy.

Our mission is to make cities safer by encouraging equal access to public spaces for everyone especially women, through the use of crowdsourced data, community engagement and institutional accountability. It is especially towards institutional accountability and evidence based policymaking, that Safecity engages with policy and legal reform to ensure greater access to justice for survivors of violence and to build a culture that systematically breaks down prevalent violence against women, both online and offline. .

Our work aids in creating widespread awareness about the law amongst different segments, while building conversations with these groups on the gaps in laws and legislative models. Knowledge of the law and understanding of it, especially laws related to the cyberspace is very restricted in India. The Policy and Legal team at Safecity has created a legal resource toolkit that explains laws relating to sexual violence and access to justice in an easy to understand format, with a separate section that explains cyberspace sexual violence and related laws and rights, this toolkit is being used by students, activists and lawyers towards expanding access to rights for survivors and by individuals to empower themselves. Furthering such awareness, Safecity hosts Legal Roundtables in different cities of India, where it creates engagement between legal experts and young students, towards creating a better understanding of the law amongst our youth and developing solutions to supplement gaps in the law, both legal and otherwise. These compiled recommendations are then submitted to various stakeholders for action. We also undertake similar legal awareness and capacity building sessions in communities. Our belief is that knowledge of the law and a platform for engaging with and recommending changes to the law is the first step towards access to justice and that it forms a key component towards supporting existing legislative models to address sexual violence, both online and offline.

Safecity also undertakes policy projects where we assess locations through safety audits to determine harassment type, timings and other incidental details, and work to create location based policy solutions to reduce such harassment. Our previous policy projects have been covered by Sweden TV and referred for action by the Union Railway Minister of India. These

policy projects also help us gauge the awareness of laws amongst people and build solutions around it.

Alongside building awareness regarding laws and engaging in advocacy for changes in laws, policies and legislative models, Safecity also engages in digital advocacy to create safe spaces and provide a medium for dissemination of information and support, through online channels. We have an online community of over 170k followers on Twitter and 44k followers on Facebook, that is actively engaged in finding solutions, providing support and taking collaborative action.

The Safecity app has been recently launched and is available on iOS and Android platforms. The app equips individuals to become community leaders for driving change and action against violence against women. This app helps facilitate conversations and dialogue, offline and online, build community engagement and push for action oriented change to support existing legal models. It is also an immensely helpful tool for creating larger awareness of rights and laws amongst the populace.

Safecity is constantly engaged in ways to advocate for better, more stringent laws towards ending violence against women while undertaking capacity building, awareness and community interventions to supplement such advocacy.

II. Existing policies that allow identification, reporting and rectification of incidents of harassment or violence against women via the internet services providers

For the specific aspects of prosecution through internet service providers (ISPs) in India, 'Acceptable Use Policies[17]' (AUPs) are the main focal point for analysis. The following are the standard terms included in AUPs in India, which could be implicated in incidents of online violence.

a. In General

Users shall not use the service to transmit or store material that is in violation of any applicable law or regulation. Users are prohibited from facilitating the violation of the AUP or another provider's AUP or otherwise making any product or service available, that violates the AUP or another provider's AUP. Users shall not use the services in a manner that threatens public health, safety, or welfare. Users agree to assume total responsibility and risk of using internet services.

b. Inappropriate Content

Users shall not use the service to send material that is inappropriate, as reasonably determined by the service provider. Users shall not send material that is offensive, obscene, defamatory, libelous, threatening, abusive, hateful, invasive of privacy, or excessively violent.

[17] *Terms and Conditions of BSNL BROADBAND Service (DataOne). BSNL Broadband Service*, http://www.calcutta.bsnl.co.in/forms/BB_Terms_Conditions.pdf. Accessed 7 August 2017; *Acceptable Usage Policy for Internet. Reliance Communications*, http://www.rcom.co.in/Rcom/personal/pdf/AUP.pdf. Accessed 7 August 2017; *Network Abuse Policy.* 2017. *JetSpot Networks Pvt. Ltd,* https://www.jetspot.in/network-abuse-limit-jetspot/. Accessed 7 August 2017; *Acceptable Use*. 2017. Tata Communications Ltd., http://www.tatacommunications.com/policies/acceptable-use/. Accessed 7 August 2017; *Terms, Conditions, Acceptable Use Policy*. 2016. *HostIndia.net*, https://www.hostindia.net/policy.php. Accessed 7 August 2017; *Terms and Conditions.* 2016. *Airtel talk,* http://airtel.com/airteltalk/terms_conditions.html. Accessed 7 August 2017; *Terms and Conditions*. 2016. *Telenor*, https://www.telenor.in/p/term-condition. Accessed 7 August 2017; *User Content and Conduct Policy.* 2017. *Google+,* https://www.google.com/intl/en_in/+/policy/content.html. Accessed 7 August 2017.

Inappropriate content includes that of child pornography, pedophilia, bestiality, and non-consensual sex acts. It also includes material that is anti-national, or of satanic nature. Harassment, whether through language, frequency, or size of message, is prohibited.

c. Fraudulent or Misleading Content

Users are prohibited from submitting or sending material or making statements which are false, misleading, or deceptive.

d. Email and unsolicited messages

Users are prohibited from sending emails or messages likely to cause distress, annoyance, inconvenience, anxiety, or harassment to the recipient, including continuing to contact a recipient after receiving information that they do not wish to be contacted. Users are prohibited from sending malicious emails, spamming or 'mail bombing' other users, i.e. to deprive others of service.

e. Illegal Activity

Users agree to use the service only for lawful activities.

Users are prohibited from transmission of any material that constitutes an illegal threat, or is obscene (or vulgar or profane), defamatory, invasive of privacy or publicity rights, or otherwise objectionable, which encourages conduct that would constitute a criminal offence, give right to civil liability or otherwise violate any law.

f. Liability

User agree to indemnify, defend, and hold the ISP and its affiliates harmless from and against all claims resulting from their (users') violation of this AUP, misuse or abuse of services.

Users will cooperate as fully as required in the ISP's defense of any claim in this regard.

g. Reporting Incidents of Violation

Most AUPs contain an email address on which users may report incidents, however, none specify a process of reporting incidents related to violation of terms.

h. Monitoring and Enforcement

The ISP reserves the right to but does not always assume the obligation to enforce the terms of the AUP. Instances of violation result in termination of services, at the discretion of the ISP.
The ISP may further investigate into violations of its AUP if required, and may report activities which it suspects violate provisions of laws and regulations to the concerned authorities, regulators, or third parties.

The ISP may assist such authorities or regulators in their investigation and prosecution of illegal conduct by providing information related to the violation of the AUP.

Gaps in user policies of ISPs in India

The terms included in the ISPs are once again not specifically in place to prevent against online violence against women but does allow for prosecuting and monitoring any inappropriate and violent behaviour when incited. However, there is quite a lot of room for improvement in the policies which have been outlined below -

a. Lack of standard policies
There is no uniform standard or policy to be followed by ISPs while drafting their AUPs. As a consequence, designation of material as ‘inappropriate’ or ‘obscene’ or ‘abusive’ is left to the discretion of the service provider. Loose definitions, for example – of what consists of harassment, may serve as loopholes for offenders.

b. Arbitrariness
The direct result of a lack of standard policy is the arbitrariness of AUPs. Some are comprehensive, detailing the actions which amount to illegal conduct, and containing clauses related to monitoring and enforcement. Others include terms such as ‘hard-core’ actions and actions of ‘satanic’ nature, without adequate explanation on what these terms mean.

c. No process identified for the reporting of abuse
Incidents of violation of terms are to be reported to the ISP via an email address which is provided in the AUP. There is no explanation in these policies of the process of identification of such violations. AUPs do not list the details required at the time of reporting incidents of abuse

or violation of terms. There is no mechanism that holds the complainant accountable for making the complaint.

d. No fixed obligation of ISPs to investigate incidents of abuse

Further, ISPs are not obligated or mandated by law to investigate the incidents of abuse. There is no fixed process identified, either in the AUP or on the ISP's website, for what happens after an incident of abuse is reported to the service provider.

e. No policies specific to women

Internet service providers do not have policies specific to online harassment or abuse of women.

Best practices for ISPs to limit online harassment of women

Some practices for ISPs to adopt in order to reduce online harassment and violence include -

a. Providing comprehensive, illustrative definitions of terms in AUPs

Defining important terms such as abuse, harassment, hate speech, sexual violence, clarifies the conditions of use of internet services. Examples to illustrate different types of online violence helps users understand what kind of conduct is expected of them while using the internet. A comprehensive AUP leaves little scope for doubt.

b. Creating awareness amongst users

Users must be made aware of what constitutes online abuse. Creating a 'Support' page helps users to understand the different kinds of abuse that one could face, online. For example, YouTube's Policy Center[18] contains a comprehensive list of guidelines to help its users identify harassment and cyberbullying, threats, hate speech etc. Facebook's Help Center addresses common questions such as, "What should I do if I am being bullied, harassed or attacked by someone on Facebook?"[19] Facebook also recently implemented new protection for profile pictures for users in India, in a bid to stop people from copying, sharing, or otherwise misusing

[18] *Policy Center*. 2017. *Youtube,* https://www.youtube.com/yt/policyandsafety/policy.html. Accessed 7 August. 2017.

[19] Facebook Help Center. 2017. Facebook, https://www.facebook.com/help/116326365118751. Accessed 7 August. 2017.

images. Users who elect to guard their profile through the new system will ensure that others can't send, share, or download their picture, and will keep strangers from tagging themselves in the image[20]. This was done because many women choose not to upload a profile picture at all owing to safety concerns, a small yet significant step towards combating online harassment.

c. Collecting information related to online abuse

When an internet service provider receives a complaint, it must ensure that the complaint consists of relevant details which would help the ISP to take action. One such measure could be a questionnaire to be filled by the user, while reporting incidents of online abuse. Such a questionnaire would ask for information related to the name, age, location of the complainant, the nature of the complaint, details of the offender/user. The ISP must ensure that the information given by the complainant is safeguarded.

d. Rectification of incidents of online abuse

The AUP of an internet service provider should contain a clearly defined review procedure to be followed once a complaint is made to the service provider. This ensures transparency and holds the ISP accountable as a stakeholder in incidents of online harassment and abuse. ISPs must publish information related to:

- Appropriate authority investigating incidents of online harassment
- Time period in which complaints must be addressed and/or resolved
- Procedure of investigation (what kind of information is being collected)
- Reference to local and national legislation
- In case of a higher degree of online abuse, approaching the local law enforcement

e. Working with civil society partners to ensure online safety

Twitter works with local grassroots advocacy organisations, academics, and researchers who specialize in media literacy, youth, and citizenship.[21] The platform has identified such non-state actors in each country, which provide feedback on Twitter's safety mechanisms.

---

[20] McCormick, Rich. The Verge. "Facebook introduces profile picture protections to stop people from misusing images." https://www.theverge.com/2017/6/22/15851662/facebook-profile-picture-protection-india. 22 June. 2017.

[21] Twitter Safety Partners. 2017. Twitter, Inc. https://about.twitter.com/en_us/safety/safety-partners.html.7 August. 2017.

ISPs in India can identify local partners to check and provide feedback on their safety mechanisms and user policies.

f. Flagging content as abusive

Facebook and Twitter, as well as email providers such as Gmail, allow users to flag or report content as 'abusive' or 'spam'. ISPs could create such a mechanism, for easier reporting of incidents of online abuse. In case of persistent offenders, users can be redirected to a page online which allows them to report the incident in detail.

g. Legislative measures to hold ISPs accountable for limiting online harassment

New Zealand's *Harmful Digital Communications Act, 2015*[22] establishes an agency to which victims can report incidents of online abuse. Court orders may also be served against internet service providers upon referral by the agency. The Act also provides for a 48 hour takedown process which allows individuals to demand that harmful content be removed by the ISP.

South Africa's *Protection from Harassment Act. 2013*[23] mandates that electronic communications service providers must assist the Court in identifying perpetrators responsible for harassment. It penalises service providers which fail to provide the requisite information.

India could incorporate parts of both New Zealand and South Africa's legislations into a new, comprehensive law dealing with online harassment. A central agency could be established to which cases of online harassment can be reported by women and men. An online form can be made available on the agency's website, just like the ones used by YouTube to report abuse, to ensure transparency and limit misuse of the forum. A legislation that mandates cooperation of ISPs with the courts will recognise ISPs as major stakeholders in the process of rectification of online harassment.

Safecity's work towards building solutions

Safecity is a platform that crowdsources personal stories of sexual harassment and abuse in public spaces. We are registered as a not for profit in the United States as Red Dot Foundation

[22] New Zealand. "Harmful Digital Communications Act." 2015.
[23] South Africa. "Protection from Harassment Act." 2013.

Global and in India as Red Dot Foundation. This data which may be anonymous, gets aggregated as hot spots on a map indicating trends at a local level. The idea is to make this data useful for individuals, local communities and local administration to identify factors that causes behaviour that leads to violence and work on strategies for solutions. Such crowdmapping helps us account for those numbers that do not find place in formal reporting, creating a larger data driven evidence base for advocating changes in law and policy.

Since our launch on 26 December 2012, we have collected over 10,000 stories from over 50 cities in India, Kenya, Cameroon, Nepal, Nigeria and Trinidad & Tobago and directly reached over 4,00,000 people. To ensure wide access, we also facilitate report collection by way of a missed call to +91 9015510510, where our team then calls the person back. Our report trends are submitted to police bodies in different states of India and help inform police action, such as increased vigilance and changing beat patrol timings Our interventions have also resulted in municipal corporations fixing street lighting and in making safe public toilets available for women to reduce sexual violence, transportation authorities have also issued women only bus licences in Kathmandu as a result of our advocacy.

Our mission is to make cities safer by encouraging equal access to public spaces for everyone especially women, through the use of crowdsourced data, community engagement and institutional accountability. It is especially towards institutional accountability and evidence based policymaking, that Safecity engages with policy and legal reform to ensure greater access to justice for survivors of violence and to build a culture that systematically breaks down prevalent violence against women, both online and offline. .

Our work aids in creating widespread awareness about the law amongst different segments, while building conversations with these groups on the gaps in laws and legislative models. Knowledge of the law and understanding of it, especially laws related to the cyberspace is very restricted in India. The Policy and Legal team at Safecity has created a legal resource toolkit that explains laws relating to sexual violence and access to justice in an easy to understand format, with a separate section that explains cyberspace sexual violence and related laws and rights, this toolkit is being used by students, activists and lawyers towards expanding access to rights for survivors and by individuals to empower themselves. Furthering such awareness, Safecity hosts Legal Roundtables in different cities of India, where it creates engagement

between legal experts and young students, towards creating a better understanding of the law amongst our youth and developing solutions to supplement gaps in the law, both legal and otherwise. These compiled recommendations are then submitted to various stakeholders for action. We also undertake similar legal awareness and capacity building sessions in communities. Our belief is that knowledge of the law and a platform for engaging with and recommending changes to the law is the first step towards access to justice and that it forms a key component towards supporting existing legislative models to address sexual violence, both online and offline.

Safecity also undertakes policy projects where we assess locations through safety audits to determine harassment type, timings and other incidental details, and work to create location based policy solutions to reduce such harassment. Our previous policy projects have been covered by Sweden TV and referred for action by the Union Railway Minister of India. These policy projects also help us gauge the awareness of laws amongst people and build solutions around it.

Alongside building awareness regarding laws and engaging in advocacy for changes in laws, policies and legislative models, Safecity also engages in digital advocacy to create safe spaces and provide a medium for dissemination of information and support, through online channels. We have an online community of over 170,000 followers on Twitter and 44,500 followers on Facebook, that is actively engaged in finding solutions, providing support and taking collaborative action.

The Safecity app has been recently launched and is available on iOS and Android platforms, the app equips individuals to become community leaders for driving change and action against violence against women. This app helps facilitate conversations and dialogue, offline and online, build community engagement and push for action oriented change to support existing legal models. It is also an immensely helpful tool for creating larger awareness of rights and laws amongst the populace.

Safecity is constantly engaged in ways to advocate for better, more stringent laws towards ending violence against women while undertaking capacity building, awareness and community interventions to supplement such advocacy.

III. Existing jurisprudence from international, regional, and national courts, on prosecution or administrative proceedings in such cases.

Violence against women is an ideological debate that has been in play since time immemorial, even in the current day and age of change and progress. The Indian Jurisprudence is quite rigid in this respect. It is largely governed by the the Nirbhaya Rape Case and the Shakti Mills Case that have left many distraught at the current situation regarding violence against women.

Violence against women earlier was limited to a concrete bodily and tangible harm. Yet, the changing times and evolution in the ideology has carved out another form of sexual harassment and violence against women. In the present technological and computerized world, women have been facing this issue through the medium of internet which has been increasing proportionally to the economy's progress rate.

A research conducted by Feminism in India (FII) and part of Freedom House Hyperlinkers on 'Violence online in India: Cyber crimes against women and minorities on social media,' has found that nearly 50 per cent of women in major Indian cities have experienced online abuse.[24] According to National Crime Records Bureau, India's agency for collecting and analysing crime data, cyber crimes are "A new class of crimes is rapidly increasing due to extensive use of Internet and IT enabled services".[25]

The response to a threat of a significant cyber activity in the Indian Legal System is filing a complaint with the respective Police Station. In presence of a Cyber Crime Cell in the respective city, the complaint has to be lodged with the said Cyber Crime Cell. The Police Department dealing with Cyber Crimes including online crimes or offenses against women have to be

[24] Shreya Kalra, "Survey Finds Nearly 50% of Women In Indian Cities Face Online Abuse, Fewer Report Them" *Indiatimes,* 24 November 2016, http://www.indiatimes.com/news/world/survey-finds-nearly-50-of-women-in-indian-cities-face-online-abuse-fewer-report-them-266051.html. Accessed 19 Aug. 2017.
[25] *Ibid.*

educated to deal with such complexities. With the rise in technological development, there has been an astronomical increase in cyber crimes committed against women which in turn results in a shortage of staff and manpower.

FII's research also found that majority of women do not report cases of online harassment because of fear of not being taken seriously. Awareness around harassment needs to go beyond eve-teasing and rape and include condescending sexist chatter, trolling and defamation both offline and online in order to help victims reach out for support, and not to be shut down by society when they do.[26]

Also, when the victims approach the Police for help and safety against the perpetrators, the Police are at times not well equipped with the software and tools required in neutralizing the threat. In such circumstances, there is indeed a necessity of the softwares and tools which might be functional in dealing with such cases.

Apart from detection, conviction is also important in such cases. And for better conviction rate, special courts will be set up. Mumbai police will also work closely with public prosecutors and magistrates, and the judiciary will be kept in the loop about the training and various cyber cases.[27] Experts say that government initiatives need to go hand-in-hand with what happens on the ground. Women and men should be educated about online harassment in order to be able to recognise and report it.[28]

Reported cases where online violence against women has been dealt with in any way or form are limited but include:

---

[26] Shreya Kalra, "Survey Finds Nearly 50% of Women In Indian Cities Face Online Abuse, Fewer Report Them" http://www.indiatimes.com/news/world/survey-finds-nearly-50-of-women-in-indian-cities-face-online-abuse-fewer-report-them-266051.html 2016.

[27] Divyesh Nair, "Mumbai Police gear up to take on Cyber Crimes", *DNA India,* 23 Jan. 2015, http://www.dnaindia.com/mumbai/report-mumbai-police-gear-up-to-take-on-cyber-crimes-2054859. Accessed 19 Aug. 2017.

[28] Shreya Kalra, "Survey Finds Nearly 50% of Women In Indian Cities Face Online Abuse, Fewer Report Them" http://www.indiatimes.com/news/world/survey-finds-nearly-50-of-women-in-indian-cities-face-online-abuse-fewer-report-them-266051.html 2016.

The case where Yogesh Prabhu was sentenced to 3 months in prison for sending a series of emails from an anonymous address to a colleague who had earlier rejected his proposal was one of the first cyber stalking cases in India that led to a conviction based on the Information Technology Act.

In order to remedy sexual harassment at the workplace to an extent, it is required for any establishment larger than 10 employees to have an Internal Complaints Committee that addresses such grievances.

Japleen Pasricha wrote a paper[29] on the topic of online violence in India and discusses the legal background of such violence as well as the recommendations. Some of which include “Educate officers that the response to online harassment is not to stop the victim using the internet” and “Create ways for women and representatives of minority groups to escalate reports of harassment, particularly incidents involving multiple accounts or lasting several days, indications that the activity is organized.”

The existing cyber law was inept to protect and prevent cyber crimes against women in India. However, the amended version has removed many difficulties satisfactorily. Even though the new law can not be given full marks on highly appropriate measure to stop atrocities against women online, it is indeed a solace to victim prone women users.[30]

Also, there was a statement made by Mr. Satyapal Singh, the Former Police Commissioner of Mumbai, where he makes a comment stating since cops don't have the right to slap criminals, women could do so and police will bring the criminals to book. Additionally, forty officers from across ranks and police stations are attending the three-day workshop to learn how to be more sensitive and responsive to crimes against women. Hence, these initiatives by the enforcement agencies are a corroboration of the fact that the legislative wing along with the enforcement agencies have indeed helped women to get justice for the crimes and offences committed

---

[29] Pasricha, Japleen. ““Violence” Online In India: Cybercrimes Against Women & Minorities on Social Media.” *Feminism In India*, “Violence” Online In India: Cybercrimes Against Women & Minorities on Social Media. Accessed 19 Aug. 2017.

[30] Debarati Halder, *CyberLawTimes,* “Cyber cime against women, Part II: From the perspective of amended IT Act” http://cyberlawtimes.com/articles/115.html. Accessed 19 Aug. 2017.

against their body, mind and person. If there are laws specifically and particularly dealing with the emerging categories of Cyber Crime and Offences against women the conviction ratio would definitely rise along with a fall in the ratio of the committed crimes.

Safecity's work towards building solutions

Safecity is a platform that crowdsources personal stories of sexual harassment and abuse in public spaces. We are registered as a not for profit in the United States as Red Dot Foundation Global and in India as Red Dot Foundation. This data which may be anonymous, gets aggregated as hot spots on a map indicating trends at a local level. The idea is to make this data useful for individuals, local communities and local administration to identify factors that causes behaviour that leads to violence and work on strategies for solutions. Such crowdmapping helps us account for those numbers that do not find place in formal reporting, creating a larger data driven evidence base for advocating changes in law and policy.

Since our launch on 26 December 2012, we have collected over 10,000 stories from over 50 cities in India, Kenya, Cameroon, Nepal, Nigeria and Trinidad & Tobago and directly reached over 4,00,000 people. To ensure wide access, we also facilitate report collection by way of a missed call to +91 9015510510, where our team then calls the person back. Our report trends are submitted to police bodies in different states of India and help inform police action, such as increased vigilance and changing beat patrol timings Our interventions have also resulted in municipal corporations fixing street lighting and in making safe public toilets available for women to reduce sexual violence, transportation authorities have also issued women only bus licences in Kathmandu as a result of our advocacy.

Our mission is to make cities safer by encouraging equal access to public spaces for everyone especially women, through the use of crowdsourced data, community engagement and institutional accountability. It is especially towards institutional accountability and evidence based policymaking, that Safecity engages with policy and legal reform to ensure greater access to justice for survivors of violence and to build a culture that systematically breaks down prevalent violence against women, both online and offline. .

Our work aids in creating widespread awareness about the law amongst different segments, while building conversations with these groups on the gaps in laws and legislative models. Knowledge of the law and understanding of it, especially laws related to the cyberspace is very restricted in India. The Policy and Legal team at Safecity has created a legal resource toolkit that explains laws relating to sexual violence and access to justice in an easy to understand format, with a separate section that explains cyberspace sexual violence and related laws and rights, this toolkit is being used by students, activists and lawyers towards expanding access to rights for survivors and by individuals to empower themselves. Furthering such awareness, Safecity hosts Legal Roundtables in different cities of India, where it creates engagement between legal experts and young students, towards creating a better understanding of the law amongst our youth and developing solutions to supplement gaps in the law, both legal and otherwise. These compiled recommendations are then submitted to various stakeholders for action. We also undertake similar legal awareness and capacity building sessions in communities. Our belief is that knowledge of the law and a platform for engaging with and recommending changes to the law is the first step towards access to justice and that it forms a key component towards supporting existing legislative models to address sexual violence, both online and offline.

Safecity also undertakes policy projects where we assess locations through safety audits to determine harassment type, timings and other incidental details, and work to create location based policy solutions to reduce such harassment. Our previous policy projects have been covered by Sweden TV and referred for action by the Union Railway Minister of India. These policy projects also help us gauge the awareness of laws amongst people and build solutions around it.

Alongside building awareness regarding laws and engaging in advocacy for changes in laws, policies and legislative models, Safecity also engages in digital advocacy to create safe spaces and provide a medium for dissemination of information and support, through online channels. We have an online community of over 170k followers on Twitter and 44k followers on Facebook, that is actively engaged in finding solutions, providing support and taking collaborative action.

The Safecity app has been recently launched and is available on iOS and Android platforms, the app equips individuals to become community leaders for driving change and action against

violence against women. This app helps facilitate conversations and dialogue, offline and online, build community engagement and push for action oriented change to support existing legal models. It is also an immensely helpful tool for creating larger awareness of rights and laws amongst the populace.

Safecity is constantly engaged in ways to advocate for better, more stringent laws towards ending violence against women while undertaking capacity building, awareness and community interventions to supplement such advocacy.

You can write to us at info@safecity.in with any queries.