



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ABUSE OF WOMEN THROUGH SOCIAL NETWORKING SITES DURING LOCKDOWN –IS LAW INADEQUATE?

Dr. Shashirekha Malagi¹

¹ Assistant Professor of Law, Sir Siddappa Kambali Law College [Formerly University College of Law], Karnataka University, Dharwad, Karnataka.580001.

ABSTRACT

The paper identifies common forms of cyber-crimes against women, such as cyber stalking ,cyber pornography, circulating images / video clips of women engaged in intimate acts, morphing, sending obscene / defamatory / annoying messages, online trolling / bullying / black mailing threat or intimidation, and email spoofing and impersonation. Facebook, Twitter, Instagram, LinkeIn, Youtube, whatsApp and Snap chat are some of the more popular social networking sites in India.This phenomenon is closely linked to the increasing incidence of cyber abuse against women. In may 2016,the Union minister for women and child Development, Ms.Maneka Gandhi observed that the online abuse of women in India ought to be treated in the same manner as violence against women in the world. The paper identifies common forms of cyber abuse against women and analyses the provisions of the IPC are relevant to cyber abuse against women via legislative amendments and judicial interpretations. The Information Technology Act covers majorly commercial and economic crimes but there are no specific provisions to cover cyber abuse against women.

Keyword-Cyber abuse , Social networking sites, Lockdown,Cyber Harassment, Cyber stalking, Cyber law

Introduction

With the passage of time, internet has become a major part of lifestyle. From using social networking sites for updating about life events to connecting people across the globe with a use of single click, internet has become a cornerstone of humans. Right to internet has been recognized as fundamental right by Hon'ble Supreme Court under article 19 of the constitution to bring it parallel with United Nations recommendations. Indian Constitution gives equal status to women by conferring upon them right to equality under Article 14. This right is further improved upon by conferring special provisions under Article 15 (3) of the Constitution by providing reservations to women in matters of employment and education. In 1992, the Constitution was amended to reserve 33 percent of the seats infavour of women in panchayats and municipalities. These legal provisions are regarded as a major step for the socio-economic empowerment of women in India. Nevertheless, the status of equality has been still a myth to millions of women. Even today, they are victims of various forms of violence or harassment within houses, in the educational field and at work places, even on the cyberspace. Further, with the advent of technology, the victimization of women has increased posing a major threat to the security of their person as a whole in the form of cybercrimes. India enacted its Information Technology Act 2000 and thereafter amended the said Act in 2008 to combat cybercrimes. However, issues pertaining to online abuse of women still remains untouched under the said Act.²This paper seeks to introspect the gaps between abuse of women through social networking sites and the laws made to protect them.

ABUSE OF WOMEN THROUGH SOCIAL NETWORKING SITES DURING LOCKDOWN

There has been a significant increase in cybercrime against women, especially sextortion, during the COVID-19-induced lockdown with "caged criminals" targeting them online, say experts. The nationwide lockdown imposed from March 25 to April 14, and then extended to May 3, aims at preventing the spread of the novel coronavirus that has claimed 1,147 lives and infected 35,043 people in the country.³

According to National Commission for Women (NCW) data, 54 cybercrime complaints were received online in April.⁴The panel is taking complaints online due to the lockdown. Cyber experts, however, said the numbers are just the 'tip of the iceberg'. "We received a total of 412 genuine complaints of cyber abuse from March 25 till April 25. Out of these, as many as 396 complaints were serious ones from women, indecent exposure, unsolicited obscene pictures, threats, malicious emails claiming their account was hacked, ransom demands, blackmail and more.

²<https://www.newindianexpress.com/nation/2020/may/01/significant-increase-in-cybercrime-against-women-during-lockdown-experts-2137987.html>, (Visited on 5/2/2021)

³ *Ibid.*

⁴ *National Commission for Women (NCW)*

Vineet Kumar, founder and president of Cyber Peace Foundation⁵, observed specially the cases of 'sextortion' have increased during the lockdown. Sextortion is extorting money or sexual favours from someone by threatening to reveal evidence of their sexual activity through means like morphed images. "People are getting into relationships online as they are under lockdown and sextortion cases are being reported to us," Kumar observed in these times people are connecting through technology but forgetting the security component. "Immediately after lockdown, we saw a rise in cases of misinformation, fake news and women getting duped online when they click on malware links which gets all their information on phone, turns on the camera and microphone, and captures their intimate moments. These are then used for blackmailing," he added. Many women do not want to make official complaints in these cases, he said. "Cyber Peace has been receiving complaints through its channels and it has been seen that people are reluctant in filing complaints. They want us to handle things unofficially, "Whatever official figure that is being quoted is just the tip of the iceberg as a majority of women do not report cybercrime because they worry about the social stigma associated with it," he said.

The founder of InfoSec Girls⁶, observed when the whole country is locked down, people are working from home and spending a lot of time on the internet. So, even cyber criminals are becoming innovative and craftier in their techniques. "Like sending specific phishing emails or themed emails for the current COVID-19 situation to people and getting their confidential details like address, phone numbers. These emails appear to have come from legitimate sources like the government in the form of advisories when they are not at all related to the government in any form,"⁷

Major reasons for the growth of cyber abuse against women

The constant increment in cyber violence against women is due to the following reasons:

- a. Easily available information of the victims: Social networking websites are made for people to connect to each other even at long distances and also to let people know each other. To show the presence of a profile, the users have to put their personal data like age, phone number, residential address, marital status, and so on. Though some of these websites give users the publication of their information as an option and even making profiles with fake names is totally allowed but the first-time registrants, including females give away their private information on the internet through these websites without even knowing the menacing effect of publishing such information. This information is visible to the public and is then used by the perpetrator to victimize women.⁸

⁵ Founder and President, Cyber Peace Foundation, <https://www.cyberpeace.org/founder/>, (Visited on 11.2.2019)

⁶ <https://www.infosecgirls.in/>, (visited on 11.2.2021)

⁷ <https://yourstory.com/2020/12/cyber-space-foundation-vineet-kumar-secure-digital-era>, (Visited on 10/1/2022)

⁸ Mayura U. Pawar, Archana Sakure, Cyberspace and Women: A Research, <https://www.ijeat.org/wp-content/uploads/papers/v8i6S3/F13130986S319.pdf>, (Visited on 10/2/2021)

- b. Ignorance and carelessness of the users: The social networking websites provide for several options to keep the profiles secure and keep oneself protected from being harassed in numerous ways such as putting up security measures and giving options to lock the personal photos, albums as well as messages. A user can also block a harasser which permanently hides the profile and cannot be found on the website by the harasser. Further, there are options like with whom to share information, a user can select to share it with only the members or with the public or with just oneself. Even after all these security measures provided by the social networking websites, women are prone to all types of cyber violence such as stalking, morphing, hacking, cheating, defamation and sexual abuse on the online platform.⁹
- c. Hiding one's real identity under fake profiles: The fundamental right of freedom to speech and expression has encouraged the right to be unidentified on the social media. These websites provide space for changing names, addresses and other personal details regularly. This was done by social networking websites to allow a user to change their physical condition and geographical location from time to time so as to get in contact and interact with the other member on that website but, this has resulted in the other way around where the perpetrators commit crimes and get a blanket to hide under different identities which are fake. These fake account users have put females in more danger and risk on the social media.¹⁰
- d. To rapid reaction of social networking websites: Cyber socializing is dangerous because of the lackadaisical response of the social networking websites. Almost all of these websites have the option of reporting the abuse of any of the services provided by them, i.e., harassment, bullying, threatening, pornography on these websites can be reported by the users. But in maximum of the cases, social networking website have their own policies to declare that a post is defamatory or harassing. It is not virtuous on their part that most of these websites put up in their privacy policies that any type of harassment caused by one user to the other user is not their responsibility and they won't be responsible in any way for the same. However, these websites do provide important safety tips for the users in their settings menu bar which give a warning to the users that their profile might be removed if it is found harassing other users or creating hate campaigns which request pornographic material and so on, but unfortunately, these guidelines are not adhered to properly.¹¹
- e. Lack of adequate laws, statutes and legal provisions: The most usual types of abuses on the social networking websites are not identified by any uniform statute, convention or rules. Furthermore, most of these socializing websites are registered in the United States and so they are governed by their laws. In India, the Information Technology Act which was enacted in 2000 and later amended

⁹ *Ibid.*

¹⁰ *Ibid*

¹¹ *Ibid*

in 2008 and the Indian Penal Code take into consideration these offences but they are not adequate enough as they do not recognize all the offences. The offences of bullying, harassment, profile cloning, etc. have not been recognized by these statutes. Therefore, the lack of adequate laws to govern the social networking websites, lack of identification of offenses against women and award sentences for the offences committed in cyberspace is a vital reason for the increment of abuse of women in cyberspace.¹²

Abuse of women through Social Networking Sites

Women are the most vulnerable targets in the internet. They have been victimized more specifically in the social networking websites. The major type of cybercrimes which are directed against women are harassment via emails, cyber stalking, cyber pornography, obscenity, defamation, morphing and email spoofing. Various factors could be attributed towards abuse of women through social networking sites.

Cyber Stalking

“Cyber stalking” is defined as a crime where the stalkers use internet or any other electronic device to stalk someone. Cyber harassment and abuse are synonymously used for cyber stalking.¹³ One of the most common cyber crime nowadays against women is Cyber stalking which includes following someone or tracking someone's activities in an online or offline mode for gathering knowledge or personal information of other person without their consent. Stalking means intrusion in person's privacy in order to terrorizes, harass, torture or to intimidate the victim. The offender tries to contact the victim and forms a relationship without his or her consent. This term is mainly defined under section 354D of the Indian Penal Code. It provides for the punishment of stalking which further includes cyber stalking. It states that any man who intentionally follows any woman and contacts her or try to contact her for personal information after several warnings by that woman with clear intention to stop that person from taking such steps will be accused of this offence.¹⁴

It will include cyber crime when such actions are done purposefully through internet, email or by any other electronic form of communication which includes cracking or hacking any password for the same purpose or someone uses identity of the woman for the same. In many incidents, devices of victims are hacked in order to obtain private content on any electronic device which is later used to blackmail them or to keep a check on them. In some case, mobile phones are hacked to destroy the evidence against the

¹² *Ibid*

¹³ Ms. Heena Keswani, CYBER STALKING: A CRITICAL STUDY, Bharati Law Review, April – June, 2017, <http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf>, (Visited on 6.2.2021)

¹⁴ *Ibid*

offender. It all includes imprisonment up to three years and fine when it is committed for the first time. And it can increase up to five years of imprisonment and fine when done on a subsequent basis.¹⁵

In India's first case of cyber stalking was reported in the year 2000 wherein the Crime branch arrested *Manish Kathuria*, a 30 year-old-software engineer for harassing a woman by chat on internet. He used obscene and obnoxious language and distributed her residence phone number inviting people to chat with her on the phone. As a result of which the lady kept getting obscene calls from everywhere and people promptly talked dirty with her. In the state of shock, she called the Delhi Police and reported the matter. The Police traced the culprit and slammed a case under Section 509 of the Indian Penal Code for outraging the modesty of the woman. Women's photographs were flashed on porno portals along with their mobile numbers. In 2008, a fast track court in Chennai sentenced a well-known orthopedic surgeon to life imprisonment in a case relating to taking obscene pictures of women and uploading them on the Internet. The doctor manipulated his women patients in various ways forcing them to exhibit sexual poses before the camera.¹⁶

In the case of *Yogesh Prabhu v. State of Maharashtra*,¹⁷ In this case the woman chatted with this person and when he proposed her for marriage, she turned it down and stopped talking to him. She also removed him from her friend list .However he continued to stalk her and kept knowledge of her.Months later, he started sending her obscene videos and photographs via email from an anonymous ID. She later filed a complaint to the police and the Cyber Crime Investigation Cell started investigation on the same. Later prabhu was charged under sections 509 IPC and S. 66E of the Information Technology Act, 2008 as section 354 D was enacted in 2013 and was not allowed to apply retrospectively to a crime of 2009.

Cyber pornography

It is a conduct of creating, publishing, communicating pornographic materials by using the cyber space. Earlier this law was governed under section 292 of IPC which dealt with the crime of obscenity and included anything which is lascivious or is appealing to the voyeuristic interests or is intended to degrade and corrupt people. Hence, now this section includes the sell, distribution, communication, publically displaying or earning any profits from such business and makes it a crime which is punishable under law .It is punishable with five years of imprisonment and a fine of Rs. 5000. Also, Section 354A of the IPC includes sexual harassment and states that any man who intentionally pornographic material to a woman without her will by sending it through Whatsapp, email or any other mode is punishable under law.¹⁸

¹⁵ *Ibid*

¹⁶ <https://www.pathlegal.in/Cyber-crime-against-women-in-India-blog-1004950>.

¹⁷ 2006 (3) MhLj 691.

¹⁸ <https://www.sciencedirect.com/science/article/abs/pii/S0267364911001798>,(Visited on 2.2.2021)

Section 67A of The Information Technology Act further prevents such act where such materials are distributed or published in any electronic form which are sexually explicit conduct or treats such conducts. The punishment under provisions of Information Technology Act includes imprisonment up to 5 years and a fine which can exceed up to 10 lakhs in case of first conviction and imprisonment of 7 years and a fine up to 10 lakhs in case of subsequent conviction.¹⁹

In the case of *Suhas Katti v. State of Tamil Nadu*²⁰, the woman who was a divorcee, filed a complaint that a man is sending her obscene, defamatory messages in a Yahoo message group. It happened after she did not accept his marriage proposal. Therefore, the man created a fake email account by the name of the woman and forwarded emails that were received in that account. Further various phone calls were received by her by the people who alleged that she was a sex worker. Hence, *Katti* was punished with two years of rigorous imprisonment with a fine of Rs. 500 under section 469 IPC (forgery in the case of harming reputation), one year of imprisonment and fine of Rs. 500 for offence under section 509 IPC (words, gestures or conduct done for the purpose of insulting the modesty of a woman) and two years' rigorous imprisonment and Rs. 4000 fine for offence under Section 67 of Information Technology Act 2000 (punishment for publishing or communicating obscene material in electronic form).

Circulating images / video clips of women engaged in intimate acts

As we know certain acts of prurient conduct which are especially pointed to intimate acts of women are increased in the modern times under Information Technology Act, which provides for pictures and videos to be easily captured on a single click and can be communicated as widely as one can reach through porns and social networking sites via internet. These are mostly made and distributed without the consent or knowledge of the woman. This also includes violent assault on the woman's private parts by a man as one can see in other sexual crimes. It prevents a woman of maintaining body autonomy and sensing agency. Section 354C of the IPC states the crimes of voyeurism.²¹

Its punishment includes 1-3 years of imprisonment and fine in case of the first conviction, and 3-7 years of imprisonment including fine for subsequent convictions. Under Information Technology Act, S. 66E deals with such matter which include violating privacy by capturing, communicating or publishing such information without the consent. The most famous case relating to this type of act was the Delhi Public School MMS case of 2004, which included the making of MMS which involved pornographic video of two students in a sexual activity and it was distributed illegally as well as was auctioned on the eBay website. Later, the Chief Executive Officer of the website was prosecuted immediately. It can also include situations where victim consents for the videography but not for the distribution. This will also be covered

¹⁹ Section 67A of The Information Technology Act

²⁰ Tamil Nadu v. Suhas Kutt, 4680 of 2004 Criminal Complaint.

²¹ <https://docs.manupatra.in/newslines/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf>, (Visited on 8/2/2021)

under this section. In other cases, the videography takes place with the consent of the woman but when the relationship turns out to be bitter, the partner for the purpose of revenge or for the purpose of blackmailing, leaks that video in the public can further be included under this section.²²

Morphing

Morphing includes improvising or editing the real picture by a fake or an unauthorized user by the way of creating fake profile and then downloading the victim's photograph from internet and then edits it in a manner which harms the original identity of the victims and posts it on the social networking sites or by any mode which can harm the reputation of the victim. It is now so common process that anyone can use such process for taking revenge or for fun purpose which dangers the modesty of the woman. It includes attaching the photograph of the victim to a photograph which have nudity or skimpy clothes of another woman by the use of such automated software which are available easily and can malign the image or the character of the victim easily in front of a larger public. Celebrities are the most common target of all the time for the sake of fun. These offences are covered under section 43 (acts that include unauthorized downloading/copying/extracting and destroying/altering data) and Section 66 of the Information Technology Act (computer-related offences). Also, the accused can be charged under various sections of the IPC such as sexual harassment under S. 354A, public nuisance under Section 290, obscenity under Section 292A and Section 501 for defamation.²³

Sending Obscene / Defamatory / Annoying Messages

Circulating private pictures of a woman, posting her pictures with contact details on websites with obscene content amounts to cyber-crime against women. This also amounts to defamation as it affects the privacy of the women which is a fundamental right. Sending of obscene, annoying messages can be through whatsapp, mail or any other social media platform. In cases where the offence does not fall under the defined crime under Information Technology Act, the women generally takes recourse under The Indian Penal Code under section 499 for defamation and section 509 for insult the modesty of women.²⁴

Online trolling / bullying / blackmailing / threat or intimidation

The list of cyber-crime against women includes online trolling/bullying/ blackmailing/ threat or intimidation. This is most prevalent in recent times. Bullying means a repetitive behavior of a person against another with an intention to harm the reputation or demean the same with superior strength or dominant position. It is done by using mobile phones or computer with internet connection. In such situation, internet

²² The Delhi Public School MMS case of 2004

²³ Aakanksha Patel, A Basic Knowledge of Image Morphing, International Journal of Engineering and Sciences (eISSN-2394-6180), Volume -1 Issue-2, Feb-2015, Available at www.knowledgecuddle.com.

²⁴ Ms. Saumya Uma, OUTLAWING CYBER CRIMES AGAINST WOMEN IN INDIA, Bharati Law Review, April – June, 2017, <https://docs.manupatra.in/newslines/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf>, (Visited on 10.2.2021)

acts as more like a bane than boon. As anonymous identity can be withheld by the person, therefore this provides with courage to do such acts. It is not surprising to note that India stands at third position after China and Singapore in cyber bullying. Social Media platforms leaves no stone unturned when it comes to making memes are against either against a women or men. However, our patriarchy leads way to more women trolling as compared to men. The word trolling is originated in 1992 and is often used in relation to internet. Trolling means a creation of discord on the internet by using abusive language, likely to quarrel or criticize other with inappropriate language with an intention to gain cheap publicity. A social media troll is a person who intentionally speaks something controversial and tries to get the attention of other user. The hunger for attention is so great in these cases that the troll often uses very vulgar language, abuses in their comments. Many times these comments which were made often were unrelated to the topic. Online trolling against women includes threats of acid attack, rapes and other form of grave hurt because a woman had raised her voice against the opinion of the mass.²⁵

The recent case of threat which came in highlight was rape threat against *Mahindra Singh Dhoni's daughter*. This is not the only case and they are plethora of cases which comes on daily basis. However, generally the attitude of people in India is to neglect such acts and block the person until the matter goes out of hand. The issue is not only with the law but with the lack of morality in our citizens. Such cases are increasing with the speed of light. It is common occurrence in case of political issues. Online complain mechanism on Facebook, Instagram and Twitter are also not always effective tool for curb such activities. An action against troll can be brought under section 67 of The Information Technology Act 2000, if the posts amount to be offensive in nature on the internet. It is important to note that the language used in section is “whoever uses Lascivious or appeals to the prurient interest or which may tend to deprave or corrupt persons. These words are extensive adequately to include any belligerent comment; even it may not be sexual in nature.”²⁶

IS LAW INADEQUATE?

The main reason for the increased number of cyber abuse against women in India is mainly due to lack of legal security. Also, most such crimes go unreported because women either fear or feel embarrassed to report their case to the police on account of family prestige and societal stigma. Humiliation, mental

²⁵ WOMAN HARASSMENT IN DIGITAL SPACE IN INDIA, International Journal of Pure and Applied Mathematics Volume 118 No. 20 2018, 595-607, <https://acadpubl.eu/hub/2018-118-21/articles/21b/68.pdf>, (visited on 9.2.2021)

²⁶ <http://www.legalserviceindia.com/legal/article-4112-female-abuse-through-social-networking-sites-a-critical-analysis-of-it-act-2000.html>, (Visited on 10.2.2021)

torture, stress, depression aggravates the situation. On account of delayed justice, people have lost faith in the law enforcement authorities.²⁷

The State and law enforcement authorities are accountable to take effective measures to curb cyber abuse against women. Article 14 of the Constitution of India provides for 'equality before law'. We can see that our Constitution provides equality but when we read the legislative provisions, we can see that there is too much gender inequality. The provisions are more inclined towards protection of women considering them to be the weaker section of the society. However, such gender inequality doesn't hold good when it comes to present scenario. Article 21 of Indian Constitution "No person shall be deprived of his life or personal liberty except according to procedure established by law."²⁸

At the same time, one should also bear in mind that, most of the popular websites declare their privacy policies that they will not take any responsibility for any sort of harassment caused to the users by other users. They provide safety tips in the menu bar and warn the users that their profile may be deleted if it is reported that they are harassing other users by creating hate operations and soliciting pornography. Therefore, women should register on the social networking websites only after reading the privacy policies or after being aware of the safety precautions of such websites. In most cases, negligence serves as a root cause for women being often trapped and victimized in incidents of cyber obscenity. Majority of the women join the social networking websites without checking the safety regulations.

Cybercrime against women in India is on at alarming stage and it may pose as a major threat to the security of a person as a whole. In India the term "cybercrime against women" includes sexual crimes and sexual abuses on the internet. India is considered as one of the very few countries to enact IT Act 2000 to combat cybercrimes; This Act widely covers the commercial and economic crimes which is clear from the preamble of the IT Act. Laws in India do not directly acknowledge many of the offences like cyber bullying, cyber eve teasing, cyber harassment, cloning of profile etc. in the Information Technology Act, 2000. However, it does not include any provisions pertaining to cyber obscenity, cyber stalking, cyber pornography, obscenity, defamation, morphing and email spoofing in relation to women.²⁹

Various forms of cyber crimes are experienced by Indian women who use the internet in the contemporary context. Neither the IPC provisions nor the provisions of the Information Technology Act fully reflect the ground realities of women's experiences. In many situations, such as morphing, email spoofing and trolling, IPC provisions are applied by extrapolation and interpretation for the want of

²⁷ Pulkit Kaushik, Cyber Laws to Curb Cyber Victimization of Women in India and other Developing Countries: A Comparative Critical Legal Analysis, Cyber Laws to Curb Cyber Victimization of Women in India and other Developing Countries: A Comparative Critical Legal Analysis, Downloads/0069-kaushik-full_text-en-v2%20(4).pdf,(Visited on 8.2.2021)

²⁸ Ibid.

²⁹ The Information Technology Act 2000, Ministry of Law, Justice and Company Affairs (Legislative Department).

more specific provisions of law. Although the Information Technology Act contains a chapter on offences, including computer-related offences, the provisions deal mainly with economic and financial issues; there are no specific provisions on cyber abuse against women.³⁰

The Information Technology Amendment Act, 2008 added a new section i.e., Section 66A. This section addressed the issue of cyber stalking but was eventually struck down by the Supreme Court of India in the case *Shreya Singhal v. Union of India*³¹. The reason behind putting down this section was the vagueness in the wording of the section. Thus, there is a need for a new amendment to this Act with respect to protection of women against cyber abuse. There is a direct need of encouragement for women to come up when their rights are violated online. Further, the government needs to ensure effective working of Cyber Crime Prevention against Women. Also, privacy of complainant needs to be protected. Implementation of provisions under Information Technology Act law is not efficient to meet these requirement. However, the need for legislative provisions cannot be ignored in the light of taking precautions. There is a requirement of effective legislative provisions to deal with such cybercrimes.

Conclusion

The commission of this crime is very easy whereas its effects are very long-lasting. It can badly affect the victim's mental and physical health. The penalty provided under existing provisions must be increased keeping in mind the well-being of the victim. Proper implementation of laws along with public awareness and education of women concerning their rights and legal remedies can play a crucial role in eradicating cybercrimes from our society. Such crimes cannot be curbed solely by enacting laws. The digital technology has grown faster than the laws governing the technology. Hence the existing laws fall short to tackle the situation. It is important to acknowledge that law does not have the potential to provide all solutions to the issue of cyber-crimes against women in India. Women themselves should be trained to take preventive measures, such as caution in posting their and their loved ones' photographs and video clips online, caution in communicating with strangers online, and protecting passwords and other vital information which may compromise with the woman's security and privacy. Women internet users in India require an increased awareness of enhancing privacy settings in social networking sites as a preventive measure.

³⁰ The Information Technology Act 2008, Ministry of Law, Justice and Company Affairs (Legislative Department).

³¹ (2013) 12 S.C.C. 73