# Cyber Laws to Curb Cyber Victimisation of Women in India and other Developing Countries: A Comparative Critical Legal Analysis

By Pulkit Kaushik[1]

Abstract

The research paper attempts a comparative critical analysis of legal provisions against cyber victimisation of women from an Indian legal standpoint with parallels drawn to developing countries viz. Pakistan, Jordan, Jamaica and South Africa. The research paper is divided into four parts. Part one provides an overview of the various slants of cyber victimization with emphasis on stalking, hacking, pornography and voyeurism. With part two the paper advances to a situational and legal analysis of the various statutory laws available to women in India to counter cyber victimisation. Offences such as indecent communication, obscenity, cheating by impersonation, indecent representation of women on cyber space are discussed in detail with support from cases decided by Indian Courts. All offences are discussed in conformity with and according to provisions of Indian Penal Code, 1860 and Information Technology Act, 2000 of India, strongly influenced by the Model Law on Electronic Commerce, adopted by the General Assembly of the United Nations. The third part of the research paper draws parallel to cyber victimisation laws in other aforementioned developing countries and explores them in light of their pros and cons keeping practical application in mind. The last part of the research focuses on legal loopholes, shortcomings and real life impediments faced by the provisions dealt with at the time of implementation. The author then utilises the comparative analysis with the other countries to suggest changes to be incorporated in further amendments to make cyber laws to curb victimisation of women infallible

Keywords: Cyber Laws, IT ACT 2000, Cyber victimisation, cyber space

## Introduction

Cyber crime is much like climate change; it's global phenomenon. The security and privacy of a person is at stake due to development and spread of technology. This technology has taken advantage of the basic animalistic characteristics of man and now poses a major threat to women on cyber space. India is one of the first and few countries to enact legislations to combat cyber crimes. However, the issues of women still majorly remain untouched. The act does identify a number of cyber based crimes, but much is left to be desired of provisions for victimisation of women. United States report on Internet and Computing Trends says Indians are the second largest sharers of personal information over the internet after Saudi-Arabians. With the objective of protection and promotion of e-commerce, Government of India enacted the Information Technology Act 2000, but in terms of computer socializing communication and cyber crimes, this act is a mere gap filler (File & Ryan, 2014).

First appearing in William Gibson's science fiction "*Necromancer*", 'Cyber Space' is an amalgamated term for the interweb of consumers, computers and networks that aid in the interconnectivity of the world. This cyber space is "the total interconnectedness" of human beings through computers and telecommunications, without regard to the physical geography. On the other hand internet was cloned from the word "interconnection" and "network".

[1] Student, Hidayatullah National Law University, Raipur, India.

Internet is the work of hundreds of connecting networks made up of different types of computers all over the world that can share messages and information with each other (Blane, 2001).

Classification of Cyber Crimes-In layman language computer wrongs includes both civil wrongs and criminal wrongs. Cyber Crime issued in generic sense which tends to cover all kinds of civil and criminal wrongs related to computers. It would include any tort or civil wrong done which relates to a computer as well as any criminal activity relatable to a computer (2008).

Synoptic view of classification of cyber crimes (Viswanathan, 2008; Ahmad, 2005; Paranjape, 2010).

| | **Crimes against person or Individuals** | | **Crimes against Property** | | **Crimes against State/ Society** |
|---|---|---|---|---|---|
| 1 | Harassment via email | 1 | Computer vandalism | 1 | Intention to extract secret information from computer system |
| 2 | Cyber Stalking | 2 | Virus transmission | 2 | Cyber terrorism |
| 3 | Dissemination of obscene Material | 3 | Denial of service attacks | 3 | Distribution of private |
| 4 | Defamation | 4 | Unauthorized access over computer system | 4 | Polluting youth through indecent exposure |
| 5 | Unauthorized control/access over computer system | 5 | Intellectual property Crime | 5 | Illegal human trafficking online. |
| 6 | Indecent exposure 6 Internet time theft 6 | 6 | Financial scams and Frauds | 6 | |
| 7 | e-mail spoofing | 7 | Sale of illegal articles | 7 | Sale of illegal articles |
| 8 | Pornography including (Child pornography) | 8 | Hacking | 8 | Online gambling |

## India's Stance on Cyber Crimes

The Ministry of Information Technology was formed in 1999, burdened with the enormous duty of making India an IT superpower by 2008. In less than a year, India witnessed the enactment of its first statute relating to Information technology based on the pattern of Model Law on Electronic Commerce, 1996, adopted by the United Nation commission on International Trade law (UNCITRAL). Another act used significantly for guidance was Electronic Transaction Act of 1998 Of Singapore. The Information Technology Act, 2000 was passed by the parliament on May 15, 2000 and notified to come into force on October 17, 2000.The Act, seeks to protect this advancement in technology by defining crimes,

prescribing punishments, laying down procedures for investigation and forming regulatory authorities (Malik, 2010).

Two kinds of definition of cyber crimes can be given. In narrow terms cyber crime consists of only offences mentioned under the IT Act, 2000, whereas broadly speaking cyber crime can be said to be an act of omission, commission or committed on or through or with the help of internet, whether committed directly or indirectly and which is prohibited by any law for which punishment corporal or monetary is provided (Kashmiria, 2014). The author restricts the scope of his research only to cyber crimes caused to women and mentioned in the IT Act, 2000.

## 1. Cyber Defamation

Defamation under Indian laws is both a tortuous and criminal liability. It describes an act with intention to lower the reputation of a person in the eyes of right thinking members of the society, or be the cause of ostracisation or introduce him to hatred, contempt or ridicule. When such defamation is carried out using a computer or internet, it is identified as cyber defamation.

Cyber defamation is considered more of a menace owing to its expeditious nature. A defamatory material could be distributed among a large number of persons without much hassle. A concrete proof of the gravity of the offence comes to light when corporate cyber defamation takes place. A single false rumour spread through the internet possesses the ability to cause unanticipated and unprecedented change in the company's stocks. Such a form of cyber defamation can be used by competitive businesses to their advantage. E-mails and social networking websites are the most frequently used methods of committing cyber defamation.

Women suffer most from it as the Indian societal structure is such that the modesty, reputation and social standing of women are delicate. The same can be utilised to cause havoc in a woman's life.

S.499 of Indian Penal Code provides tackles the law of defamation. S.4 of IT Act gives recognition to electronic records. Therefore S.499 of IPC read with S.4 of IT act bridges the gap and provides relief in situations of cyber defamation. Hence, defamatory material posted on the internet using emails or social networking websites, it could draw the attention of S. 499 of Indian Penal Code.

## 2. Cyber Pornography

Pornography is a cyber offence with grave moral implications. It is however an offence with no settled definition under any law. The Miller Test developed by the US Supreme Court (Miller v. California, 1973) is used to judge whether a given pornographic ‘work’ is obscene. The test poses three fundamental questions related to the work in question:

- Whether the average person, applying ‘contemporary community standards’, would find that the work, taken as a whole, appeals to the prurient interest.
- Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by applicable state law.
- Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Conventional law of obscenity is contained under sections 292 and 293 of Indian Penal Code. Section 292 deals with the sale of obscene books, drawing or any other object and section 293 provides punishment to person dealing in cyber pornography that is accessible to person under twenty years of age. S.292 of the Indian Penal Code defines obscenity as that which is 'lascivious or appeals to the prurient interest or tends to deprave or corrupt persons'. A major breakthrough was witnessed when the Indian Supreme Court held (Aveek Sarkar & Anr. Vs. State Of West Bengal, 2014) that a nude picture of a woman is not obscene if the picture has no tendency to deprave or corrupt the minds of people in who view it.

S.354A of the Indian Penal Code forcibly showing pornography to a woman is included under sexual harassment. S.354C of the Indian Penal Code deals with voyeurism. The offences included are capturing image of a woman in a private or sexual act with a hidden device, without her consent. If consent is taken to the capture of the images but not to its distribution, then also it is an offence.

S.67 of IT Act provides punishment for publishing or transmitting obscene material in electronic form. S.67-A of IT Act deals with mainstream pornography and provides punishment for publishing or transmitting material containing sexually explicit act in electronic form. 67-B provides punishment for publishing or transmitting of material depicting children in sexually explicit act in electronic form or induces children for online relationship with one or more children or facilitates abusing children online. This section even makes searching for child pornography related material on Google a non-bailable and cognizable offence.

With sections 66-E (violation of privacy), 67, 67-A and 67-B obscenity has been brought under legal dominion. Further by implications of the law, mainstream pornography has been differentiated from child pornography.

Air Force Bal Bharti case was the first case Delhi Police Cyber Crime Cell registered a case under section 67 of the IT act. The accused was a juvenile student of Air Force Bal Bharati School, and in retaliation to being mocked by fellow classmates for having pockmarked face he created a website containing lucid, explicit, sexual details about various girls and teachers of the school. Classification of fellow female students and teachers were made on their physical features and sexual preferences. As the word about the website spread, the website became an adult boys' joke amongst students. He was later charged under:

- S.292 and S.509 of Indian Penal Code (act intended to insult the modesty of a woman).
- S.4 of Indecent Representation of Women (Prohibition) Act, 1986 (Circulation of material containing indecent representation of women).
- S. 67 of the Information Technology Act.

Young Persons (Harmful Publication) Act, 1956 is another act having an impact on cyber pornography.

## 3. Cyber stalking

According to Oxford Dictionary Stalking means "pursuing stealthily" (Augarde, 1981). .In simple terms, it refers to extension of physical form of stalking where electronic medium such as computer, internet, e-mail or any other electronic device is used to pursue, harass or contact another person in an unsolicited manner. I generally involve harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's house or place of business, making harassing phone calls, leaving written messages

or objects or vandalizing a person's property. These crimes are done with the sole motive of gaining control over the victim and thus targets women in most of the cases. Domestic violence victims are one of the most vulnerable groups to traditional stalking. So it's no surprise they are vulnerable to cyber stalking as well. It's a myth that if women “just leave” they will be okay. Cyber stalking is a way to continue to maintain rigid control and in still fear into a domestic partner, even when she has already left the relationship.

Main causes and reasons for cyber stalking are (K, 2014):

1. Sexual harassment
2. Obsession for love
3. Revenge and hate
4. Ego

Sending messages, advancing threats to the victim and following the victim's movements across the internet comprises of cyber stalking. Victims mostly are women and children, being pursued by men and paedophiles. Cyber stalking can be classified as

1. Harassment or stalking or both through internet
2. Harassment through internet and stalking continued off-line.

Necessary personal information of the victim is collected by the stalker and then utilised in the pursuit. The information can be extracted through social networking sites. Information could also be uploaded to porn sites or chat rooms.

Cyber stalking under Indian criminal law is simply criminal intimidation with so separate provisions. This was made clear in a case wherein the victim Ritu Kohli received obscene calls from every part of the country as Manish Kathuria, her online stalker had distributed her number through a chat website. Delhi Police slammed a case under S.509 of Indian Penal Code (outraging modesty of a woman). A computer or internet is hence simply used as means to carry out stalking and harassment but cyber stalking is not considered a crime independently.

## 4. E-mail Spoofing

A spoofed e-mail may be said to be one, which misrepresents its origin. A trusted origin is shown rather the original source of inception. By changing certain properties of the email, such as its header, from, Return-Path and Reply- To fields etc., hostile users can make the email appear to be from someone other than the actual sender. Email spoofing is possible because the main protocol used in sending email i.e. Simple Mail Transfer Protocol (SMTP), does not allow an authentication mechanism. Email spoof can cause monetary damage also. In case of women, the above mentioned crimes could ensue based on if email spoofing is successfully done (Kaushik & Aggarwal, 2014).

## 5. Morphing

Morphing is editing of picture without permission. Morphed images are used to create fake profiles on social networking websites or are distributed through WhatsApp. Websites to download a woman's picture can itself be a social networking site. These images can later also be uploaded to pornographic websites.

Such acts amount to violation of I.T Act, 2000. S.43 (computer sabotage) and S.66 (identity theft) of the said act. S.66Ddeals cheating by impersonation and can also be invoked. S.66E (Privacy violation by publishing image of private area) also provides for punishment if it can be evoked.

## Jordan

Investigation and prosecution of cyber crimes in Jordan was introduced by the Electronic Transactions Act, 2001. However, it focused primarily on e-commerce and suffered from a lot of legal lacunae, particularly in the field of criminal culpability in cyberspace offences. In 2010, the Jordan Information Systems Crimes Act (ISC Act,2010) was introduced as a necessary amendment to plug the loopholes in the ET Act. The Jordanian ISC Act, 2010, therefore, became the first domestic substantive law, dealing with computer and electronic devices enabled offences. Although it has drawn flak because of paucity of procedural supports, it has successfully guaranteed and formulated a fundamental framework that enumerates and defines cyber offences. Ergo, certain positive aspects of the Act with regard to the aforementioned crimes cannot be overlooked.

The ISC Act, 2010, amends the legal inadequacies for curbing international crimes committed using information systems or informatics networks, like promotion of prostitution. Child pornography, online sexual abuse and prostitution, have been recognized as cyber offences with prescribed sanctions.

However, the Act takes a negative stance or fails to redress a lot of cyber issues. It pays no heed to pertinent problems of cyber stalking and harassment, online extortions, spamming, e-mail spoofing and circulation of obscene content. There are no provisions for criminalizing acts of cyber fraud, forgery, counterfeiting and impersonation in the scope of this Act. There is an absence of an organised mechanism to deal with cyber threats. These deficiencies translate not only to ambiguous penalties and punishments, but also to a vague interpretation of privacy and freedom of speech. Moreover, the absence of procedural norms (or reliance on a half-century old Criminal Procedure Code) jeopardises the application of this Act in the face of rapidly advancing technology and reveals a shortage of coverage.

To conclude, the Act suffers from multi-faceted problems from procedural deficiency to obscure mechanisms to deal with most present and future cyber crimes, with the CrPC, 1961 making it all the more indeterminate and convoluted for the judicial authorities to implement it (Faqir, 2013).

### Jamaica

The importance attached to cyber laws in Jamaica can be reasonably gauged from the fact that the first book on the issue was published as recently as in April, 2013. Like Jordan, Jamaican cyber law is rife with shortcomings, but the most critical is the time lag between emergence of a legal issue, and the response of the legal framework to redress the same.

In 2010, The Cybercrime Act was passed which enumerates sanctions for criminal liability arising out of misuse of computer systems. Though the provisions and punishments for cybercrimes are detailed and stringent, cyber victimisation of women is outside the scope of the Act. Moreover, the terms used in the act are either undefined or incoherently defined, displaying an ostensible apathy regarding cyber crimes against women.

However, with changing times, the current zeal of development and advancement provides a ray of hope. This act is set to be repealed (Henry, 2015) and will be overruled by a new one

with substantial overhauls and updates comprising cyber bullying and online harassment and intimidation laws (Antigua Observer, 2015).

A bird's eye view would undoubtedly suggest that Jamaica lags behind in providing cyber security. But owing to its progress and a tiny population, Jamaica should soon implement an unassailable and more comprehensive law to provide relief to cyber crime victims.

## Pakistan

One of the modern curses, that have further complicated security issues in Pakistan, is that of cyber crimes. Aggravating the situation more is a serious lack of knowledge regarding national and international cyber laws and rights, with both, the people and authorities, turning a blind eye towards these crimes (Avais, 2014).

Cyber stalking and crimes against dignity and modesty of "natural persons and minors" have been given substantial importance in the Prevention of Electronic Crimes Act, 2015 bill proposed to the National Assembly.

In S.18 of the bill, an earlier attempt to impose criminal liability for defaming a woman has been expanded to "offences against the dignity of natural persons". However, there seems to be a real risk of increased surveillance and snooping by virtue of this section even though the attempts at protecting privacy seem legitimate.

S.21 of the bill criminalises the use of the Internet or other information systems etc. to: (a) communicate "obscene, vulgar, contemptuous, or indecent intelligence", or (b) "to make any suggestion or proposal of an obscene nature; or (c) threaten to commit any illegal or immoral act; or (d) take a picture or photograph of any person and display or distribute without his concern or consent or knowledge in a manner that harms the person; or "display or distribute information in a manner that substantially increases the risk of harm or violence to any person", with intent to coerce, intimidate or harass any person.

The provision of the "mens rea" requirement i.e., the intent to commit a criminal offence, is commendable, but the kind of content that would suffice as "obscene", "vulgar", etc., has not been defined anywhere. With no definitions, the application will always be inconsistent and vague.

Given all these concerns, the bill, as it stands today, seems to undermine the rights of victims of cyber crimes. It appears to be strengthening cyber surveillance more than cyber security.

## South Africa

2012's National Cybersecurity Policy Framework by State Security Department was made public in December 2015. Until then, the document which was expected to revolutionarise the cyber space was kept confidential. It was expected that the new bill would put forward the issue of women security also. However, the only issue surrounding women that was dealt with was child pornography. Cyber bullying has now come under the spotlight with the passing of the Cybercrimes and Cyber Security Bill 2015. It is also said that South Africa Cybercrimes Bill will be impossible to implement without violating rights (APC, 2015).

The Sexual Offences Amendment Act 2007 includes display of child pornography and creation of child pornography as an offence. Provisions relating to trafficking for sexual purposes have been included. The Protection From Harassment Bill 2009 defines harassment

done verbally or electronically. The Children's Act 2005 as well as Children's Amendment Act 2007 provides provisions for child pornography (Sheeron, 2009).

Stalking and harassment through telephone calls and electronic mail by the Domestic Violence Act 1998. lt does not however make provisions to address new avenues like chat, Social Networking websites and text messages. For instance, sexually explicit materials whose dissemination is aided by developing technologies and Web 2.0 tools like pornography on the internet, or sexual harassment of women via cell phones and social networking sites. The Convention on Cybercrime adopted by the Council of Europe on November 8, 2001 and signed by other countries including South Africa, addresses the issue of child pornography but is silent on violence against women (Munyua). The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright and neighbouring rights (IBP Inc., 2013).

However, change is impending in South Africa. Women'sNet is a feminist organisation that works to advance gender equality and gender justice in South Africa. The medium they spread awareness about and through is Information Communication Technologies. South Africa's National Policy Framework for Women's Empowerment and Gender Equality also makes a commitment to redress inequities in the ICT sector and support women's participation.

## Loopholes in Indian Laws

No doubt Information technology act, 2000 has been passed by the Indian Parliament with the objective to facilitate to prevent Cyber Crimes. However:

1. Information Technology Act, 2000 nor defines "cyber crimes" neither uses this expression, but only provides the definition of and punishment for certain offences. Thus two kinds of definition of cyber crimes can be given. In narrow terms cyber crime consists of only those offences which are mentioned under the Information Technology Act,2000, whereas broadly speaking cyber crime can be said to be an act of omission, commission or committed on or through or with the help of internet, whether committed directly or indirectly and which is prohibited by any law for which punishment corporal or monetary is provided. In this context it can be concluded that Information Technology Act, 2000 provides punishment for only certain offences and is not exhaustive of all cyber crimes.
2. S.79 of IT Act, 2000 lays down conditions under which ISPs or intermediaries are exempt from culpability for offensive content uploaded by a third party. It obligates the intermediaries to exercise "due diligence", and to act on the orders of the court or the government and its agencies to qualify for immunity.
3. Cyber defamation has been defined under the Indian Penal code but not in the IT Act, 2000. S.67, 67A, 67B, and 67C cannot be said to cover book, pamphlet, paper writing, drawing, painting, representation or figure in electronic form if there is any public good defence like object being of general concern or kept for confide religious purposes is put forward.
4. Again, under no section in IT ACT 2000, Obscenity – personal viewing – Is an offence, infact like in IPC 292 again if it is proved that you have published or transmitted or caused to be published in the electronic form only then under Section

67 it can be an offence. Last but not the least, the IT Act 2000 does not mention the typical cyber crimes like cyber stalking, morphing and email spoofing as offences (Aggarwal, 2010).

5. A difference between pornography and child pornography has been recognised in United States of America's Communications Decency Act, 1996 and United Kingdom Obscene Publications Act, 1959. Similar differentiations is provided under the. No such differentiation exists under Section 292 of Indian Penal Code, 1860 related to criminal intimidation but the IT (Amendment) Act, 2008 has made child pornography as specific offence under Section 67B (Kashmiria, 2014).
6. Cheating by impersonation has not been defined and it is not clear whether it refers to cheating as referred under the Indian Penal Code, 1860 as conducted by communication device or whether it is creating a new category of offence. Moreover the term fraud is neither defined under the IT Act, 2000 nor under the Indian Penal Code, 1860.It more being recognized as a mental condition under Indian Penal Code, 1860
7. IT offences are extremely technical in nature which only an expert or well-read person can deal with. Cyber Regulation Appellate Tribunal (CRAT) is one man commission requiring only a person with degree of law, specifying no IT background.

## Conclusion

India by far has a relatively robust cyber law in comparison with Pakistan, Jamaica and Jordan. However, Indian cyber laws itself lack behind contemporary times. When Indian laws fail to counter the changing scenarios of the cyber space, the impending crisis to be faced by other countries can only be imagined. All these other countries have cyber law bills in the process, but these future acts are not foolproof themselves. Political impediments, privacy issues, moral argument of restricting speech and expression on the internet, practical implementation of real laws in the virtual world all are severe obstacles standing between a iron clad act and cyber crimes. Cyber victimisation of women is a part of the picture, but dealing firsthand and on priority basis with this picture can do a great deal of helping in curbing the gap and reducing cyber crimes. While Indian lawyer makers have a lot to learn from some countries, there are countries like Jordan, Pakistan and Jamaica which must utilise Indian to get influenced and borrow ideas to safeguard their women on the internet.

## References

Aggarwal, Nidhi, and Neerja Kaushik, Dr. "Cyber Crimes Against Women." *Global Journal of Research in Management* 4.1 (2014): 37-49. Web. <http://www.publishingindia.com/GetBrochure.aspx?query=UERGQnJvY2h1cmVzfC8yMjE3LnBkZnwvMjIxNy5wZGY=>.

Aggarwal, Rohit. "Cyber Crime Against Women And Regulations In India." *Http://www.tmu.ac.in/gallery/viewpointsdcip2013/pdf/track4/t-403.pdf*. Web.

Ahmad, F. (2005). *Cyber law in India: Law on Internet*. Delhi: New Era Law publications.

APC. "South Africa Cybercrimes Bill Will Be Impossible to Implement without Violating Rights." *Association for Progressive Communications*. 2 Dec. 2015. Web. 5 Dec. 2015. <https://www.apc.org/en/news/south-africa-cybercrimes-bill-will-be-impossible-i>.

Augarde, A. J. *The Oxford Dictionary*. Oxford: Oxford UP, 1981. Print.

Avais, Muhammad Abdullah, Aijaz Ali Wassan, Hameeda Narejo, and Jameel Ahmed Khan. "Awareness Regarding Cyber Victimization Among Students of University of Sindh." *International Journal of Asian Social Science* 4.5 (2014): 632-41. Print.

Aveek Sarkar & Anr. Vs. State Of West Bengal And Anr 4 SCC 257 (2014)

*Blane, J. V. (2001). Cyberwarfare: Terror at a click. Huntington, NY: Novinka Books.*

*Eu National Cyber Security Strategy and Programs Handbook: Strategic Information and Developments*. Place of Publication Not Identified: Intl Business Pubns Usa, 2013. Print.

Essof, S. (2009). South Africa: violence against women and information communication technologies. *Association for Progressive Communications (APC).*

Faqir, R. S. (2013). Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010.*International Journal of Cyber Criminology*, *7*(1), 81

File, T., & Ryan, C. (2014). Computer and Internet use in the United States: 2013. *American Community Survey Reports*.

Henry, Balfold. "Cybercrimes Act to Be Repealed." *Jamaica Observer*. 21 May 2015. Web. 5 Dec. 2015.

"Jamaica to Debate New Cyber Crime Legislation." *Antigua Observer*. 14 Oct. 2015. Web. 10 Dec. 2015. <http://antiguaobserver.com/jamaica-to-debate-new-cyber-crime-legislation>.

"Joint Monitoring Committee On The Improvement Of The Quality Of Life And Status Of Women." Proc. of National Policy Framework for Women's Empowerment and Gender Equality : Parliament's Gender Conference. 2001. Print.

K, Vijaykumaran Nair, and Vinod Chandra S.S. *Informatics*. 2014. Electronic.

Kashmiria, S., Dr. (2014). Mapping Cyber Crimes Against Women In India. *International Research Journal Of Commerce And Law, 1*(5), 22-38. Retrieved December 7, 2015, from http://ijmr.net.in/download.php?filename=766t9kt3Iqv1Osa.pdf&new=IRJCLPAPER2DECEMBER2014.pdf

Malik, K. P. (2010). *Computer & Information Technology Law*. Jain Book Agency.

Miller v. California, 413 U.S. 15 (1973)

Munyua, Alice, Muriuki Mureithi, and Grace Githaiga. *Women and Cybercrime in Kenya: The Dark Side of ICTS*. Working paper. Print

Paranjape, V. (2010). *Legal Dimensions of Cyber Crimes and Preventive Laws*. Allahabad: Central Law Agency.

Regulation of Cyber Space. (2008). Indira Gandhi National Open University School of Law, 12(3).

Viswanathan, A., Ms. (n.d.). *Cyber Law* (1st ed.). LexisNexis.