CYBER-CRIME AND VULNERABILITY OF WOMEN

DR. SOMA GHOSH
PRINCIPAL
Hiralal Mazumdar Memorial College for Women
Dakshineswar, Kolkata - 700035

Prelude

There is a phenomenal growth in the Cyber-crimes (as per Information Technology Act, 2000) in India. 'There were 4192 cyber-crimes in 2013 which were 2761 in 2012. If one considers such crimes as per Indian Penal Code also, the number of crimes was 5500. Police has arrested 3301 criminals in this regard. Under Information Technology Act, 2000, there were 681 and 635 crimes in Maharashtra and Andhra Pradesh respectively. In these two states there is 50 per cent rise in cyber-crimes. As per National Crimes Records Bureau (NCRB), in 2013 there was 122 percent increase in cyber-crimes in India. Such crimes in other states were: Karnatak (513), Kerala (349), Madhya Pradesh (282) and Rajasthan (239). In the state of Gujarat, such crimes were 68in 2012 and 61 in 2013'[1]. This updated research paper is the partial outcome of a MinorResearch Project undertaken by the author as the Principal Investigator under the aegis of the University Grants Commission.

Cyber-crime – an introductory note

Cyber-crime and the Victimization of Women is a new and very much relevant contribution to the literature on cyber-crime. It focuses on gendered dimensions of cyber-crimes like adult bullying, cyber stalking, hacking, defamation, morphed pornographic images, and electronic blackmailing. These and other tactics designed to inflict intimidation, control, and other harms are frequently been committed by persons who are hardly been punished. In such a situation socially women suffer from exclusion syndrome and psychologically they also feel exclusion.

[1] Gujarat Samachar, Ahmedabad, 3 July, 2014

Cyber-crime, also called computer crime, is to be defined in terms of the use of a computer as an instrument for illegal ends, such as committing fraud, trafficking in women andchild pornography and intellectual property, stealing identities, or violating privacy. Identity theft and credit card account thefts are considered to be cyber-crimes when the illegal activities are committed through the use of a computer and the Internet. Cyber-crime encompasses any criminal act dealing with computers and networks, popularly known as hacking. Cyber-crime, especially through the use of internet, has grown in importance as the computer has become central to education, commerce, entertainment, and government.

Norton Report 2012[2] defines cyber-crime in following terms:

Social cybercrime is defined as any of the following activities on social networking platforms:

• Being harassed or bullied or had inappropriate content posted about someone,

• Responding to a forged or fake message or website trying to get one's personal details, such as passwords, bank Account information (i.e., phishing),

• Clicking on a link or a 'like' that takes to a blank page, or reposts itself automatically into one's account or onto his/her profile.

There are lots of other term, of which a very few has been mentioned.

The earliest victims and villains of cybercrime were the Americans, because of the early and widespread adoption of computers and the Internet in the United States. The advancement of technology has made man dependent on Internet for all his needs all over the world; simultaneously it has made people vulnerable to all sorts of criminal attacks through computer and internet network. Internet has given man easy access to social networking, online shopping, storing data, gaming, online studying, online jobs et. It has simultaneously opened a space for criminal activities. Cyber-crimes are committed in different forms. A few years back, there was lack of awareness about the crimes that could be committed through internet. In the matters of cyber-crimes, India is also not far behind the other countries where the rate of incidence of cyber-crimes is also increasing day by day. However, it is to be noted that such criminal activities affect both men and

[2] Norton Report 2012 - now-static.**norton**.com/.../**2012**

women, but when it affects dignity or reputation of a lady, it becomes a concern of social scientists. It needs special attention because women are also frequent users of internet. Thus with the advent of technology, the rights of women in cyber space are to be recognized as important as rights of women in physical space. Women should give equal emphasis on their rights in cyber space and their related duties.

Even though the International Covenant on Civil and Political Rights in Article 17 (1) states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation;" and Council of Europe convention for cyber-crimes (2001) does protect human rights to a certain extent, we observe that there are no universal codes for specifically protecting women's rights in the cyber space. Most of the cyber-crimes against women happen due to lack of recognition of women's rights and zero or less lawsto protect women's interest in the cyber space. In this context, a mention must be made of"Convention on the Elimination of All Forms of Discrimination against Women"[3], 1979. The primary aim of this convention was to eradicate discriminations against women and establish equality for women in the society.

Article 1 of the convention. The convention opens with firm notes on defining what 'discrimination against women' shall mean in Article 1. To quote Article 1;

For the purposes of the present Convention, the term "discrimination against women" shall mean any distinction, exclusion or restriction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment or exercise by women, irrespective of their marital status, on a basis of equality of men and women, of human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field.

Article 2 of the Convention mentions that:

[3] *Ensuring Accountability to UNSCR 1325 and 1820 using CEDAW reporting mechanisms". Gnwp.org. Global Network of Women Peace builders. November 2010. Retrieved June 5, 2014.*

States Parties condemn discrimination against women. States Parties condemn discrimination against women in all its forms, agree to pursue by all appropriate means and without delay a policy of eliminating discrimination against women and, to this end, undertake:

(a) To embody the principle of the equality of men and women in their national constitutions or other appropriate legislation if not yet incorporated therein and to ensure, through law and other appropriate means, the practical realization of this principle;

(b) To adopt appropriate legislative and other measures, including sanctions whereappropriate, prohibiting all discrimination against women;

(c) To establish legal protection of the rights of women on an equal basis with men and to ensure through competent national tribunals and other public institutions the effective protection of women against any act of discrimination;

(d) To refrain from engaging in any act or practice of discrimination against women and to ensure that public authorities and institutions shall act in conformity with this obligation;

(e) To take all appropriate measures to eliminate discrimination against women by any person, organization or enterprise;

(f) To take all appropriate measures, including legislation, to modify or abolish existing

laws regulations, customs and practices which constitute discrimination against women;

(g) To repeal all national penal provisions which constitute discrimination against women.

Types of cyber-crime that are committed against women:

Amongst the various cyber-crimes committed against individuals and society at large the crimes which can be mentioned as specially targeting women are as follows: –

1. Harassment via e-mails.

2. Cyber-stalking.

3. Cyber pornography.

4. Defamation.

5. Morphing.

6. Email spoofing.

Unfortunately even though Chapter XI of the IT Act deals with the offences such as Tampering with computer source documents (s.65), Hacking with computer system (s66), publishing of information which is obscene in electronic form (s.67) Access to protected system (s70), Breach of confidentiality and privacy (s. 72), Publication for fraudulent purpose (s.74) IT Act 2000 still needs to be modified. It does not mention any crime specifically as against women and children.

Herein lays the Significance of the study:

While women benefit from using new digital and Internet technologies for self-expression, social networking, and professional activities, cyber victimization may keep them suppressed. Women may suffer more as cyber victims, which may affect their social and political life and even can make them nonassertive. Failure to stop cyber victimization of women will definitely have an adverse effect on equal participation of women in all squares of life, including their political life.

Scope of the rules of law and of conventions, related to the rights of women in cyber space, social taboos related to women's access to different social networking sites in cyberspace,require detailed analysis, combining it with the views of women in this respect. The importance of CEDAW and its execution in cyber space needs serious introspection. Laws and constitutions of countries like USA, Canada and India are also analyzed.

Various duties of women in cyber space are to be examined in-depth with a view to generate a sense of social awareness against violations of rights of women in cyber space as well as against probable misuse of these rights by tech-savvy women themselves.

As cyber space has no physical boundaries and as such, no strict rule or regulation originating in any particular geographic region can regulate cyber space as a whole, the role of the international organizations like UNO should also come under microscope.

Basic fundamental rights of human beings, such as freedom of speech and expression, right to privacy, right to live a safe life etc, prevail universally both in the physical space as well as in the cyber space in all democratic countries. But the big difference between the rights prevailing in the physical space and those prevailing in the virtual space lies in the modes of legal sanctity and justifiability of these rights. The issues of women's rights in the cyber space demand special attention of the scholars, researchers, law makers, and ordinary women largely due to theallegation that national governments, as well as of the international ones still lag far behind because of their sluggish attitudes in executing the gender equality and gender justice promises.

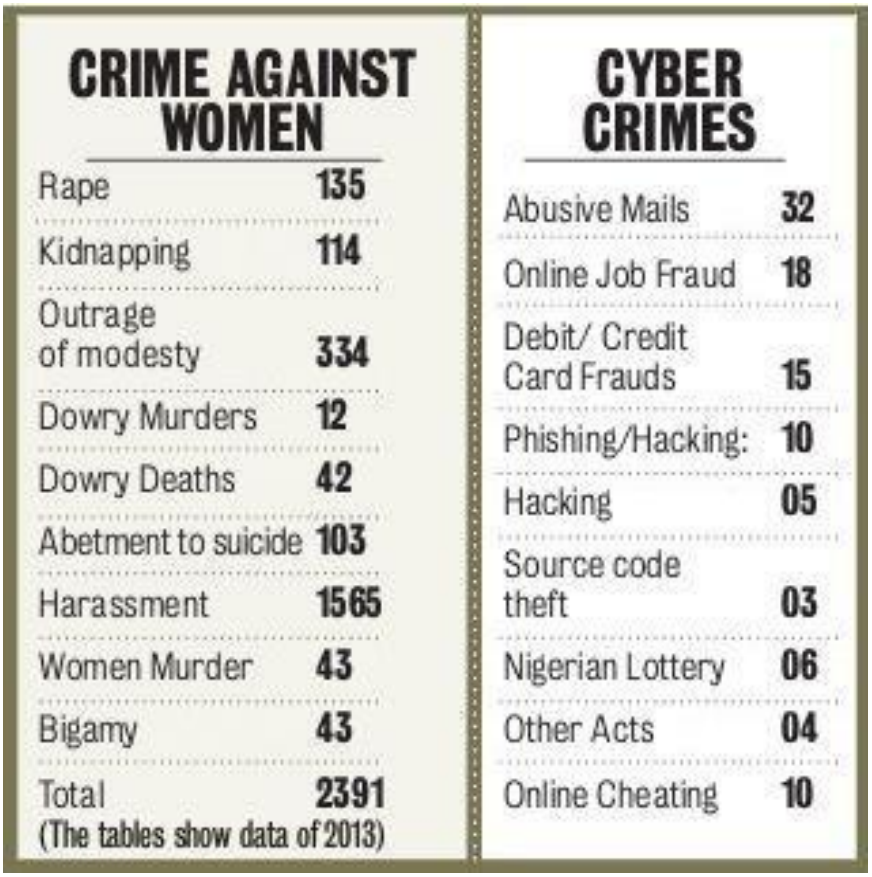
As more and more people take to the internet, cyber-crimes and mobile crimes will only continue to increase at an alarming rate. However, the fact remains that Indian cyber law is still ineffective in terms of delivering appropriate cyber-crime convictions. Further, cyber fraud continues to increase with dramatic force in India. As per one Norton report, more than Rs 50,400 crore was lost by Indians during 2012 on cyber fraud itself and that trend showed no signs of lessening.

Section 66A of the Information Technology Act, 2000 continues with its casual run. Various cases under Section 66A were registered in the country. In February 2013, a Palghar court closed the case against two girls who were arrested for posting a comment on Facebook on the bandh after the death of Shiv Sena supremo Bal Thackeray on November 17 last year. It was only after the Palghar case that an Advisory was issued by the Government to take the prior permission beforethe registration of cases under Section 66A of the Information Technology Act, 2000.

Social media as a phenomenon has grown by leaps and bounds in 2013. However, with the passage of time, 2013 has exhibited that the Information Technology Act, 2000 is not capable of effectively

addressing the legal, policy and regulatory concerns generated by the use of social media in India.

The report presented below upholds an alarming scenario for us: [4]



CRIME AGAINST WOMEN

Rape	135
Kidnapping	114
Outrage of modesty	334
Dowry Murders	12
Dowry Deaths	42
Abetment to suicide	103
Harassment	1565
Women Murder	43
Bigamy	43
Total	2391

(The tables show data of 2013)

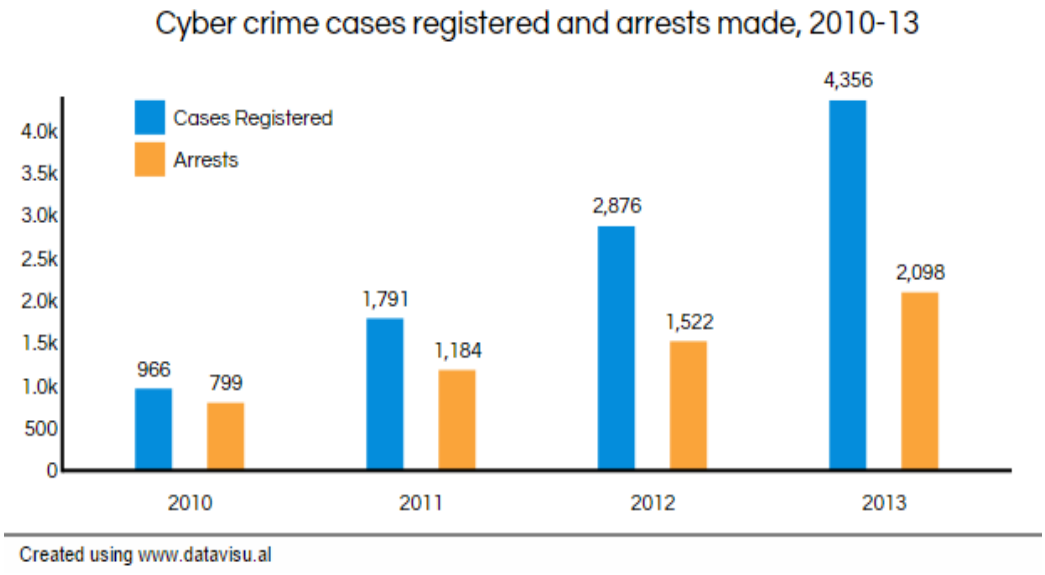
CYBER CRIMES

Abusive Mails	32
Online Job Fraud	18
Debit/ Credit Card Frauds	15
Phishing/Hacking:	10
Hacking	05
Source code theft	03
Nigerian Lottery	06
Other Acts	04
Online Cheating	10

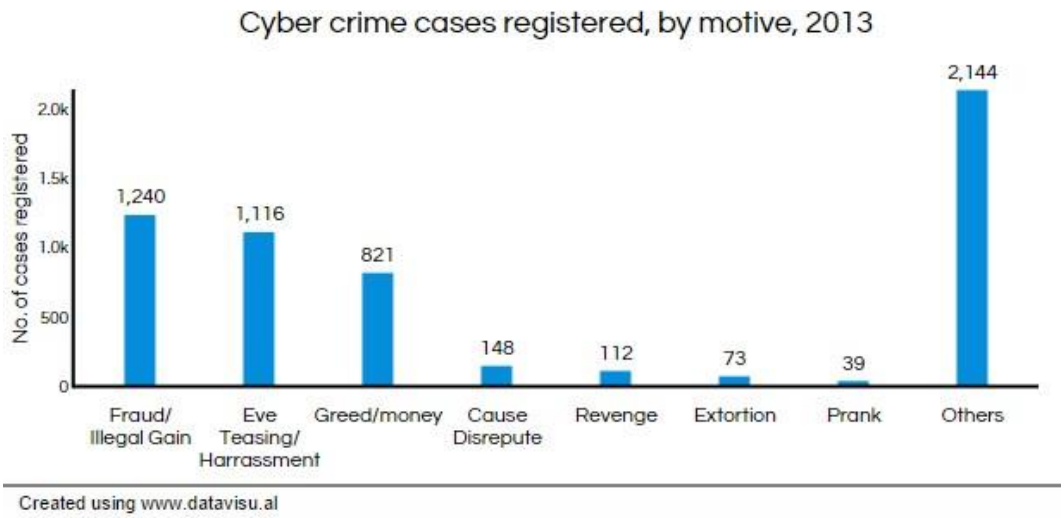
Perpetrators of such crimes can be booked under sections 66C (which prescribes punishment for identity theft), 66A (which prescribes punishment for sending offensive messages through communication services), 66D (which prescribes punishment for cheating by impersonation) and 67 of the I.T. Act, 2000 (which prescribes punishment for publishing or transmitting obscene material in electronic form).

[4] The Hindu, Bangalore, October 31, 2013, Updated: October 31, 2013 00:42 IST

They can also be booked under 499 (which defines defamation) /120B (which prescribes punishment for criminal conspiracy) of the Indian Penal Code and Section 6 of the Indecent Representation of Women (Prohibition) Act. But these are insufficient measures or inadequate tools to fight against growing menace of cyber-crime in India.West Bengal - Kolkata in particular - has shown the biggest jump nationwide in cyber-crime cases,according to the National Crime Records Data for 2012. From six cases in 2011, Kolkata Policehas registered 68 cases in 2012 and 84 in 2013. The case details depict that most cases relate to damage or loss to a computer or device (section 66 (1) of IT Act, 2000) and hacking (section 66 (2) of IT Act, 2000). In the three years up to 2013, registered cases of cyber-crime were up 350%, from 966 to 4,356.[5] Business Standard report is presented below.

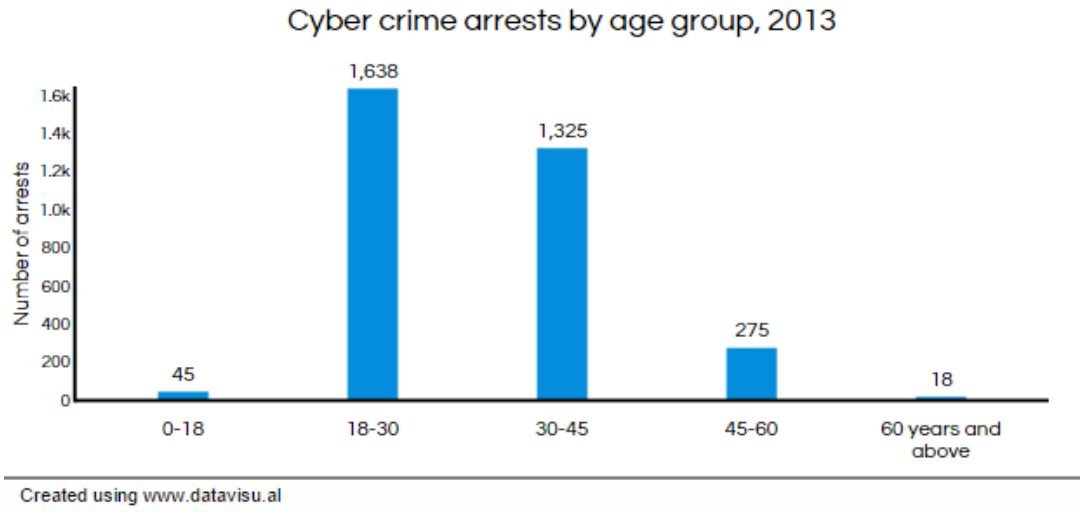


[5] Business Standard, January, 19, 2015; last updated at 13.33IST.



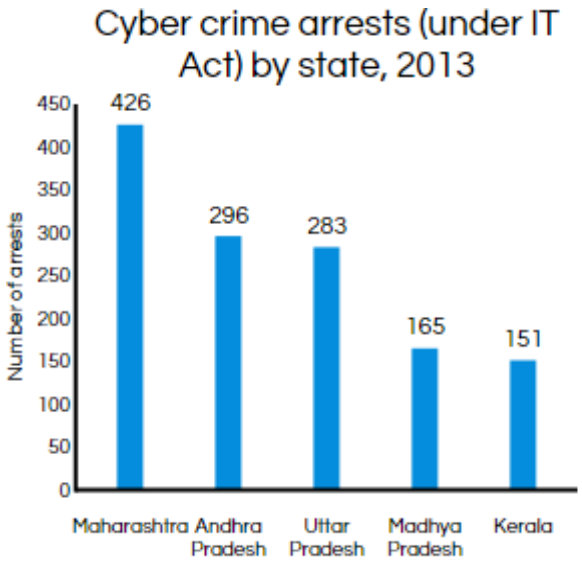
Source: NCRB

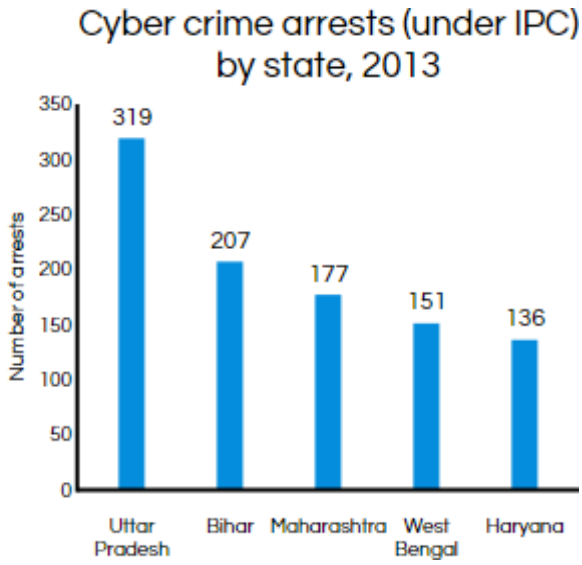
NCRB reports that incidence of cyber-crime cases during 2014 in India is about 9,622.



Source: NCRB

Those who are arrested under these laws are overwhelmingly young. Data show that the age group of 18-30 accounts for the highest percentage of cyber-crime with 1,638 persons arrested in the age bracket out of a total arrests of 3,301 in 2013.



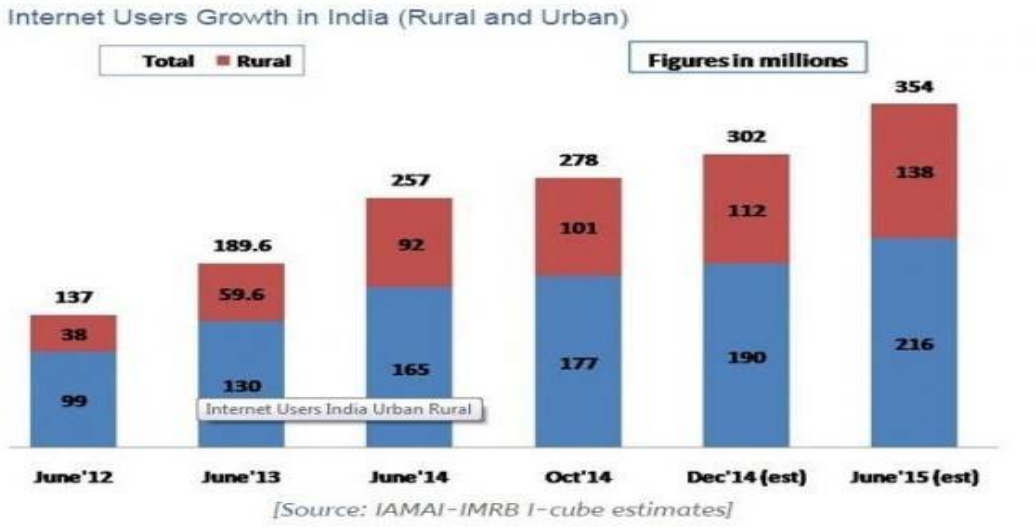


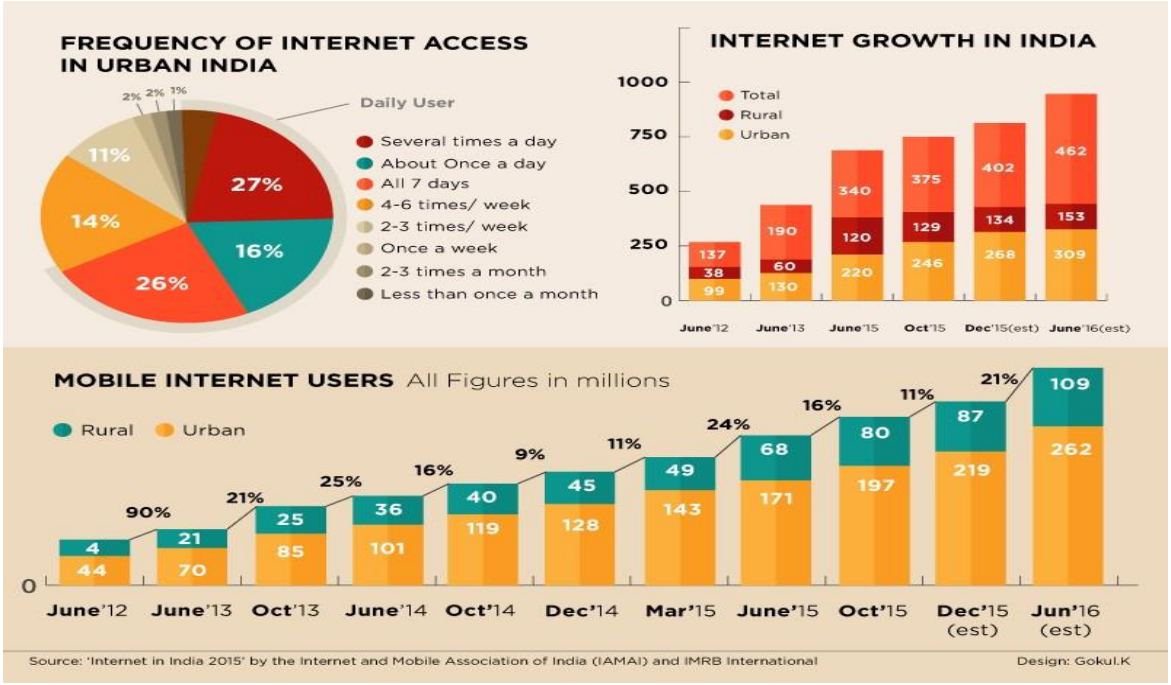
Cyber-crime appears to be concentrated in states with major cities, indicating that urbanization and so internet penetration–is a factor. Maharashtra accounts for the most persons arrested under the IT Act, 2000, and Uttar Pradesh reported the most arrests under the older Indian Penal Code (IPC). The figures are also indicative of a rising trend among cops in states like West Bengal to register cyber-crime cases under the traditional IPC sections giving the IT Act, 2000, a pass. The Kolkata figures are even scarier - a 1033.3 % jump between 2011 and 2015[6]. Among those arrested last year for cyber-crimes were four students and six minors, who were treated as "sexual freaks". In such cases also police cops are increasingly filing cases under IPC sections, giving the Cyber-crime Act a miss.

There has been a wide penetration of internet in urban and rural India today, which was being centered in the purely urban areas even few years back. The penetration of active internet users in India has grown rapidly. These are some of the findings from the latest I-Cube Report on

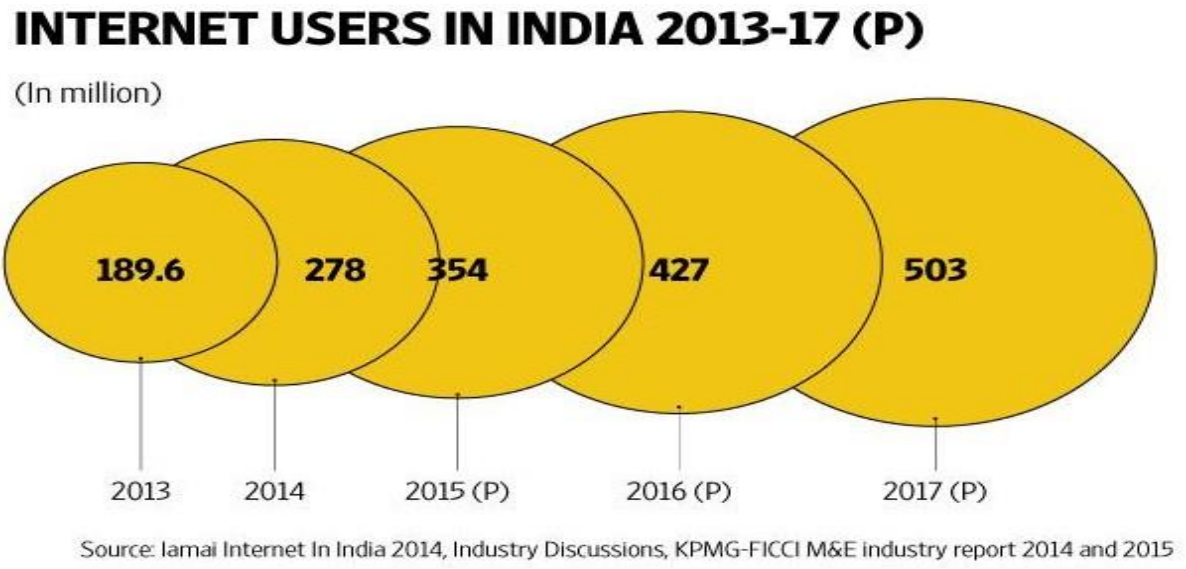
[6] Ghosh Dwaipayan, 'Kolkata tops cyber-crime table' | TNN | Oct 29, 2015, 01.10 AM IST

'Internet in Rural India' which was released by the Internet and Mobile Association of India (IAMAI) and IMRB.





According to the report, the number of claimed internet users even in rural India is expected to rise more rapidly. The report further states that mobile phones are fast emerging as an important point of internet access in rural India. This is just the tip of the iceberg, in the next few years, a combination of affordable smart phones and local language content is likely to lead to higher internet usage in India, empowering India with a level playing field of knowledge and information.



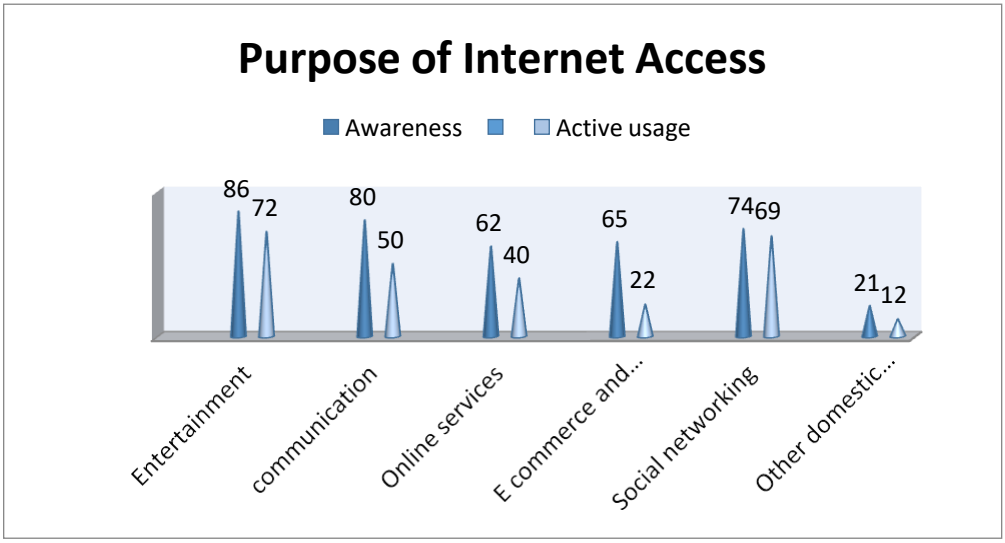
Purpose of Internet Access:

A study in some selected areas of 24 Parganas North, i.e., Barasat, Barrackpur, Baranagore, Durganagar, Madhyamgram, Dankuni, Habra, North and South Dumdum and some places in central Kolkata, like Baghbazar has detected that entertainment is the primary driver of internet use. However, there is still a difference between rural and urban areas in the nature of using internet. As per the survey report, prepared on the basis of the interview taken by the field surveyors, for 70% of the urban internet users, online communication or other services happens to be the top reason for accessing the internet on their devices. Entertainment was top priority for only 30% of these users. Among rural users, on the other hand, 62% said that their primary reason for accessing the internet was entertainment. Communication and social networking stood at 37%

and 39% respectively. After surveying the areas under Kamarhati Assembly constituency and some areas under Barrackpur Subdivision, it has come out that communication could be lower down the rankings due to a preference for offline use of services. Irrespective of rural- urban divide the survey explores following scenario.

Purpose of Internet Access:

Level of usage	Entertainment	Communication	Online services	E-commerce and online finance	Social networking	Other domestic needs
Awareness	86	80	62	65	74	21
Active usage	72	50	40	22	69	12

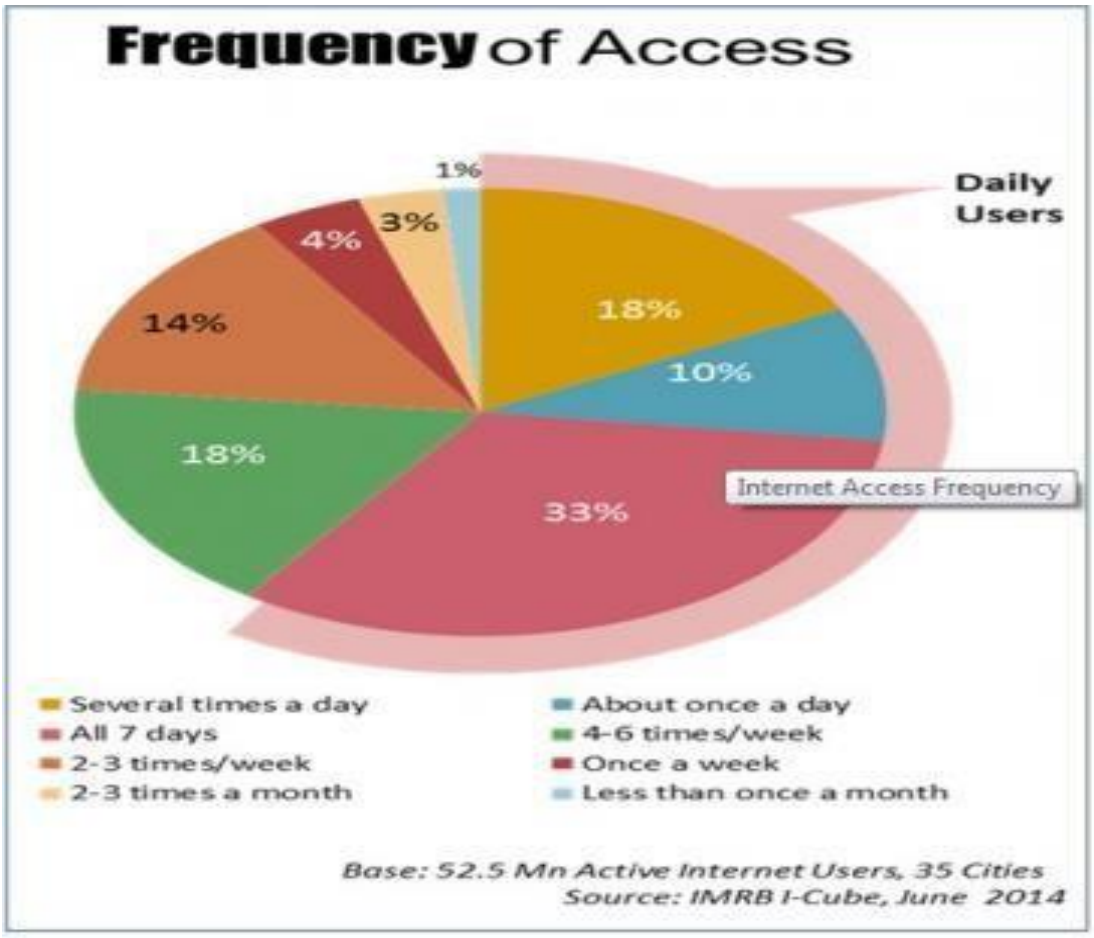


72% of users use internet for entertainment, like accessing Music, Videos and Photos for entertainment, while 50% uses it for communications; there have been 40% and 22% users respectively who avail of online access for online access for online services and online finance

etc. There is a growing interest amongst the rural constituents seeking information on education. 81% of claimed internet users seek information pertaining to school / university and examination centers.

It is also evident that large part of internet users consider internet as a tool for male counterpart. Only 12% women use internet. According to the survey report covering above mentioned areas internet user base is growing fast. But so far as the gender distribution of internet users in these areas as of March 2, 2015 to March, 2016 is concerned, only about 29% of women have been found as consistent internet users[7]. The majority of internet users were male. Primary reasons to access the internet for women are communication, social networking and entertainment. Majority of the women urban users use the internet most for communication, whereas most of the women rural users still access the net for entertainment.

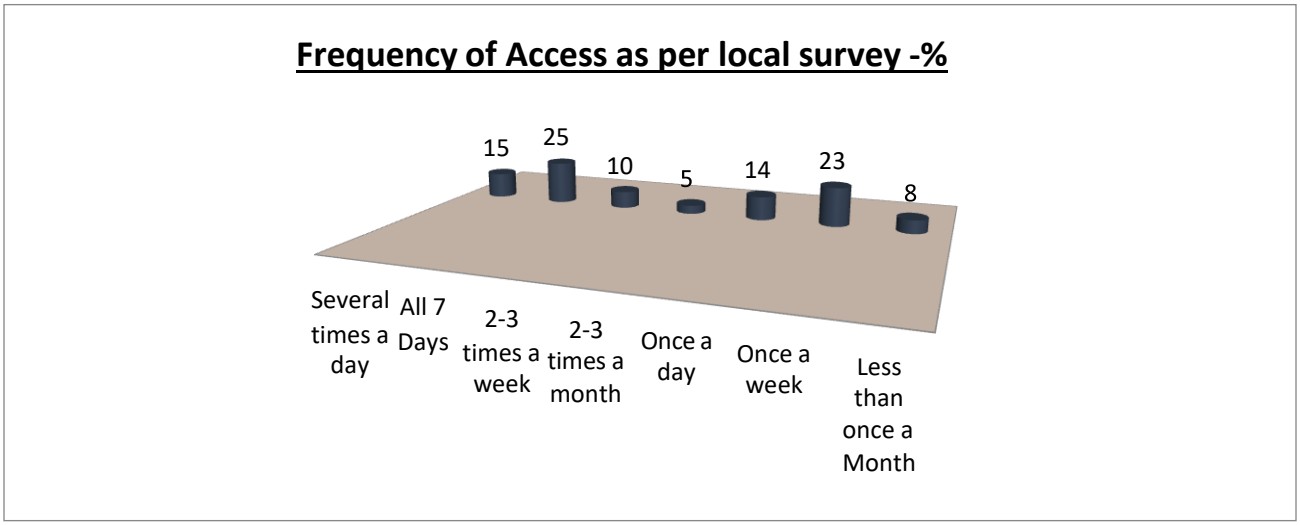
On the basis of survey it has been found that frequency in accessing internet resembles mostly the IMRB report presented below:



[7] Data source: Survey reports in N 24 Parganas and Kolkata Cyber cafes

Frequency of Access as per local survey

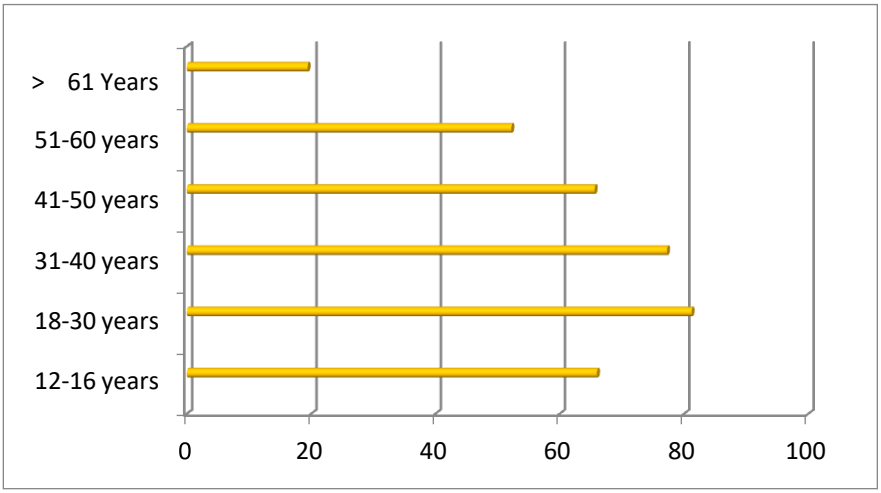
Frequency	Several times a day	All 7 Days	2-3 times a week	2-3 times a month	Once a day	Once a week	Less than once a month
%	15	25	10	5	14	23	8



Use of Internet According to Age Group

Following statistic prepared on the basis of survey, presents information on the age distribution of internet users in India in the project years. During this period of time, 79.25 percent of internet users are between 18 and 40 years old.

Years	12-16 years	18-30 years	31-40 years	41-50 years	51-60 years	≥ 61 Years
%	66	81.23	77.27	65.63	52.23	19.45



Principal Investigator, her project assistants and surveyors have found that police are concerned by the mushrooming of internet cafes and there is little control on what people access in these places. In the suburbs, cyber cafe owners are not much bothered about restricting entry of minors too. During survey it has been observed that usually the internet is assessed through computer or laptop. However, the use of internet through smart phones is increasing at faster rate especially in semi urban and rural areas. A sub inspector under Belghoria Police station warned that they often receive cyber-crime cases, though under IPC, where internet is accessed by using open/free Wi-Fi zones in malls, markets, offices, hotels, and other places. These free net zones are accessed by hackers and terrorists more frequently. This is because, many times it may be difficult to trace the users since it is openly used by anyone. By and large, such Wi-Fi zones are unsafe and it requires proper security.

What's alarming is that the trend of harassing women has flooded the CID's cyber cell and cyber-crime police station in Lalbazar, said sources, while probed by the surveyors. But the problem actually lies in whether the complaints are lodged under IPC or the IT Act, a senior officer told to the PI.

The tendency to lodge cyber-crime cases under IPC sections is justifiable only relating to evidence. Say for example, an SMS or an image send through a cell phone device is coveredonly under the IT Act and not IPC. Hacking, for example, is covered only under the IT Act and not IPC. Now gauge the fate of the case in courts if these were to be lodged under IPC," pointed out a retired OC of the cyber-crime police station.

There are lots of such evidences which are admissible in a court of law under the IT Act only, said an Inspector in the cyber cell. It has been found that cases under the IT Act can only be investigated by police inspectors and above. Thus, one would need at least 113 inspectors alone for this purpose, which is highly inadequate considering the volume and number of the cases registered. The matter is to be addressed with utmost care as it is worth noting that even the number of Cyber-crime cases filed under the IPC has increased year on year, as is evident from the statistics[8] presented below , the number of cases filed under the IT Act has increased at a much greater rate.

This isn't all. These numbers have completely overshadowed the biggest cyber-crime scourge - like harassing women on social networking sites and mobile devices, sending them sexually explicit content or morphing their faces etc. In West Bengal, However, targeting women through Internet and mobile phone devices have shown a higher prevalence than hacking, though Bengal is quite a long way from being the country's cyber-crime capital. While visiting cyber cells under Barrackpur and Bidhannagar Police Commisionarates, it has been found that cyber Stalking is being hardly reported due to public ignorance and no laws to govern such crimes, though Section 503 of the Indian Penal Code can be used to deal with a section of this Internet crime. Also IPC Section 509 is sometimes cited to punish the offenders of stalking. The gravity is yet to be comprehended.

Cyber security is very important when the use of computers, e-mails and mobile phones is increasing. IT infrastructure is secure with corporates, since it is programmed internally by them. The infrastructure of use of mobile / smart phones is vulnerable to more cyber threats and needs more security. A more serious mode of threat is for women, as in our social process women still are very sensitive regarding their dignity and social reputation. Harassment via e-mails, cyber-stalking, cyber pornography, defamation, morphing, emails spoofing etc. are some of the dirty mechanisms which affect the women to the extent of taking away their right to life and personal liberty.

[8] NCRB REPORT, 2014

Incomplete computer knowledge makes women more vulnerable. Browsing the internet through Google or the use of social networking websites like Facebook, Twitter, or Orkut without proper knowledge of privacy protection, protection from spy ware, internet viruses like Trojans, tracking cookies etc. jeopardizes women's safety and same applies to children also.

This study revealed that gender differences were strongest with regard to complex computer task. However, no significant differences were reported in terms of simple computer task. Males had significantly higher self-efficacy expectation than females. Male respondents reported less computer anxiety and higher computer confidence than the females. A close analysis of these results of the studies shows that males have a better edge in computer literacy domain than females. Victimization of women through social networking websites is mainly because of their insufficient knowledge. Women are less aware of the privacy policies and safety tips of using networking sites. Indian women netizens still hesitate to report the cyber abuse or cyber-crime. The biggest problem of cyber-crime lies in the detection of modus operandi and determining the motive of the cyber offender.

Cyber-crimes against women are on the raise and women have been drastically victimized in the cyberspace. Some perpetrators try to defame women by sending obscene e-mails, stalking women by using chat rooms, websites etc., developing pornographic videos where women are depicted in compromising positions mostly created without their consent, spoofing e-mails, morphing of images for pornographic content etc. The sex-offenders look for their victims on social network websites, and also on job or marriage websites where people post their personal information for better prospect. The revealing of personal information has made women more a casualty of cyber-crime.

Amongst the various Cyber-crimes committed against women and girl child, the following need our attention immediately to address the issues:

a) Harassment through Emails: This is not a new concept. It is very similar to harassing through letters. Harassment includes blackmailing, threatening, bullying, and even cheating via emails. E-harassments are similar to the letter harassment but create a problem quite often when posted from fake IDs.

b) Cyber Stalking: This is one of the most talked about net crimes in the modern world. There are three primary ways in which Cyber Stalking is conducted: E-mail Stalking; Internet Stalking; Computer Stalking. The Oxford dictionary defines stalking as 'pursuing stealthily'.

Cyber stalking involves following a person's movement across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms visited by the victim, constantly bombarding the victim with emails, etc.

c) Cyber Pornography: This is yet another threat to the female netizens. This would include pornographic websites, pornographic magazines produced using computers, (to publish and print the material) and the Internet to download and transmit pornographic pictures, photos, writings, etc.

Pornography - Time Statistics[9]:

Every second - $ 5,075.64 is being spent on pornography
Every second - 48,258 Internet users are viewing pornography
Every second -572 Internet users are typing adult search turn into search engines
Every 39 minutes - a new pornography video is being created in the United States

In India, Hicklin's test has been adopted by the Supreme Court in a leading case of Pornography of Ranjeet. D. Udeshi vs State of Maharashtra. (AIR1965 SC 881) This case has decided many issues pertaining to Cyber Obscenity. In another case in India Samaresh Bose vs Amal Mitra (AIR 1986 SC 967) held a new definition of Cyber Pornography. Section 67 of IT Act deals with obscene and pornographic material on Internet.

d) Cyber Defaming: Cyber trot including libel and defamation is another common crime against women in the net. This occurs when defamation takes place with the help of computers and/or the Internet. For e.g.: someone publishes defamatory matter about someone on a website or sends emails containing defamatory information to all of the person's friends.

[9] *(Source: Funell, Setven; 'Cyber-crime; Vandalizing the Information Society", London, AddisonWesley, 2010)*

e) Morphing: This is editing the original picture by unauthorized user or fake identity. It was identified that, fake users and again re-posted/uploaded on different websites download female pictures by creating fake profiles after editing it.

f) E-Mail spoofing: A spoofed email may be said to be one, which misrepresents its origin. It shows its origin to be different from which it actually originates. A review in the CyberLawtimes.com shows that India has crossed the danger mark in Cyber-crime targeting women and children.

g) Crimes related to mobile phones: This technology is the 'new playground for Cyber criminals'.

- **SMS Spoofing:**

It is like e-mail spoofing, which looks to originate from one acquainted number but in reality it is spoofed, and sent from some evil minded individual. We can take this by an example. Suppose if a woman receives a Short Messaging Service (SMS) in her cellphone in the middle of the night from the mobile of her spouse asking her to bring cash as he has met with an accident. The chances are that she would check the mobile number and if she confirms the cell is her husband'sthen she would rush out with the cash. If this could be the response then the chances are that she is not aware of 'Mobile Spoofing'. Using a web-based software, a Cyber-criminal could send anyone a message from any person's cell without even touching his mobile. And no cellular service provider can say that it was a spoofed or faked one. Women have been countless timesthe victims of such Cyber-criminal activity. Unless there is cooperation between website owners and the administrators of message servers it is very difficult to detect the perpetrators of such crime.

- **MMS (Multimedia Messaging Service).**

This involves the option of sending photographs, sound clips, or even movie clips along with the message. The MMS service was basically meant for use to interact more lively with friends, family and relatives, but it was used by a large number of people to send porno clips from one mobile to another. Service providers use this facility along with 'Voice Chat', a 'Find a Friend' service that allows one to look for like-minded companions. Women and adolescent girls arevery easily prone to become victims of this crime. The famous scam of reputed Public School of Delhi

that was in news recently involves the use of MMS. The clip, which was made, was distributed by the accused to his friends via MMS, which soon reached the market.

Talk, text, music, photos, Internet, print, are just the beginning of the newer killer applications that are being added onto a mobile handset. Convergence has truly become the new mantra for the mobile industry. The mobile subscribers in India has a huge base of 236 million users andthis also is a very fertile space for cyber related unwanted forays and victimization of unguarded users.

- **Social Networking/Online Friendship Websites:**

A social networking site is an online location where a user can create a profile and build a personal network that connects him or her to other users. In the past 5 years, such sites have rocketed from a niche activity into a phenomenon that engages tens of millions of Internet users, a major section of which consists women folk, particularly homemakers (MRP survey report). A great debate has ensued about the potential risks posed when personal information is made available on such a public setting.

Netiquette is a set of rules (mainly unwritten) to follow while you are on-line. These rules have sort of evolved and exist to make the Internet a safe and secure place. While these are not carved in stone – you may become unwelcomed if you deviate too far from them. This term 'Netiquette' is coined for either 'network etiquette' or 'Internet etiquette'. 'The more power you have, the more important it is that you use it well'. (Rule 9- Don't abuse your power)[10].

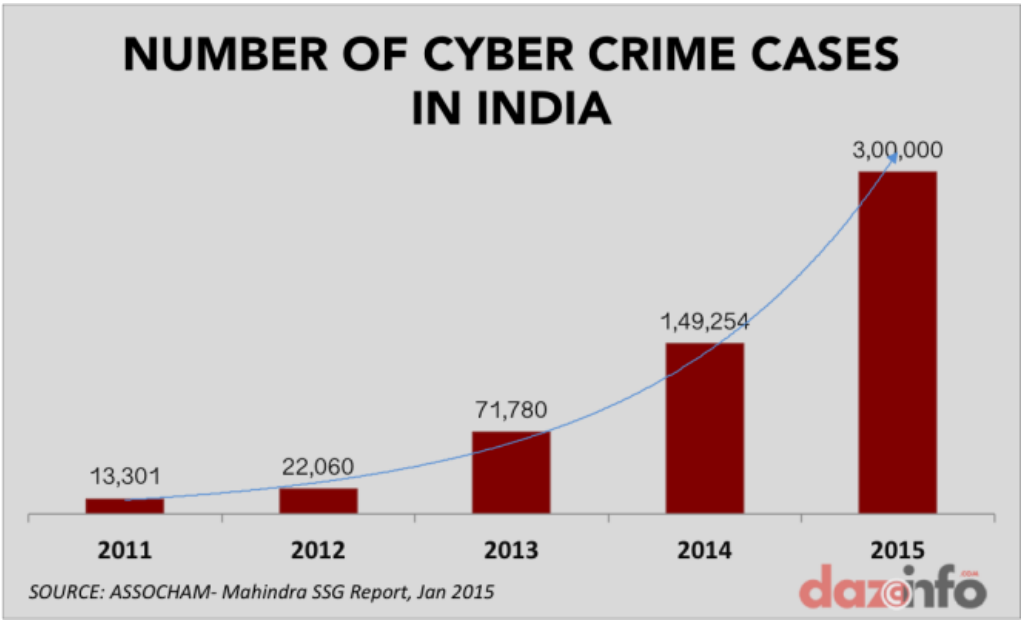
The Government of India has ordered the telecom operators and internet service providers to block 857 porn sites. The order is issued under the provisions of Information Technology Act, 2000 and Article 19 (2) of The Constitution of India. There is a view that this can be assessed in privacy. The government is of the opinion that such things should not be viewed in public places like cyber cafes.

[10] *Virginia, Shea: 'Netiquette': San Francisco, lbion Books, 2010, ISBN 0-9637025-1-3*

The Central Government is thinking to set up a Cyber-crime Coordination Centre, to which complaints relating to cybercrimes against individuals across the country will be directed for technical analysis and identification of redressal mechanism, before they are forwarded to the competent law enforcement agency for investigation.

The center will be modelled on the lines of Intelligent Crime Complaint Centre (IC 3) of US. The technical experts will look at the technical aspects of the cybercrime, including identifying the internet sites/content to be blocked before trigging a blocking request to the I T ministry. The Cybercrime coordination center will also study the laws to be invoked on the basis of the crime reported and pass on the case to the state police or CBI, as per the relevant jurisdiction, for investigation and prosecution[11].

If immediate steps are not being taken, rising at alarming rate, the number of cyber-crimes in India may touch a humungous figure very soon, causing havoc in the financial space, security establishment and social fabric.



[11] (Times of India, Ahmedabad: 10 July, 2015)

Select Bibliography

1. Moore, R. (2005) "Cyber-crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
2. Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
3. David Mann and Mike Sutton (2011-11-06). "Netcrime". Bjc.oxfordjournals.org. Retrieved2011-11-10.
4. Halder, D., & Jaishankar, K. (2011) Cyber-crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
5. Spinello, Richard, Cyberethics(2009), Morality and Law in Cyberspace, Jones & Bartlett Publishers,
6. Cavazos, Edward and Morin, Gavino,(1994) Cyberspace and the Law Your Rights and Duties in the On-Line World, MIT Press eBooks, ISBN: 9780262303545
7. VIswanathan , Aparna, (2012)Cyber Law, Lexis Nexis, ISBN: 9788180387395
8. Jain, Atul,(2005), Cyber-crime: Issues Threats and Management (2 Vols), New Delhi, Isha Books, ISBN 13: 9788182051065
9. Dr. Dasgupta M., (Reprint 2014), Cyber-crime in India - A Comparative Study , New Delhi, Eastern Law House,ISBN : 9788171772773
10. Vikas, Pareek, Cyber-crime in Indian Context,(2013), LAP Lambert Academic Publishing Cyber-crime in Indian Context, ISBN-13 9783659502583
11. Halder, Debarati, Cyber-crime and the Victimization of Women: Laws, Rights and Regulations, (2011), IGI Global, ISBN-13: 978-1609608309
12. Naveed, Shazib, (2013), Internet Usage & Task Preferences Part 1 A perspective with gender differences LAP Lambert Academic Publishing, ISBN: 978-3-659-40587-7

13. Criminal Manual: Cr.P.C., I.P.C. & Evidence (with Free Guide to Criminal Pleadings - Model Forms) Hardcover – 2015 Publisher: UNIVERSAL LAW PUB CO.P.LTD.-DELHI by Universal's Legal Manual (Author)
14. Virginia, Shea(2010) 'Netiquette': San Francisco, lbion Books, ISBN 0-9637025-1-3
15. Cooper , Jonathan, (1998), Liberating Cyberspace: Civil Liberties, Human Rights & the Internet: Turtleback Books
16. Chander, Harish(2012),Cyber Laws and IT Protection, PHI Learning ISBN-13: 978-8120345706
17. Belapure, Sunit & Godbole, Nina(2011),Cyber Security: Understanding Cyber-crimes, Computer Forensics And Legal Perspectives, New Delhi, Wiley India, ISBN: 978-81- 265-2179-1
18. Chaubey, Manish Kumar, (2013), Cyber-crimes & Legal Measures, New Delhi, Regal Publications, ISBN: 978-81-8484-228-9