The internet has the ability to spread or circulate information or communicate instantaneously. This has caused upheaval in many facets of our life. The use of internet in our day to day lives has many disadvantages as now it is used by many people for doing unlawful activities which has further given rise to criminal activities. Latest technologies have enhanced the possibility of invading into the privacy of the individual as the internet is used by many individuals to amass huge amount of private data of an individual, which can be further used for criminal activities.

The Information Technology Act, 2000 on the recommendation of General Assembly Resolution. This act unfolds the various aspects of information technology to promote efficiency in the delivery of government services by means of reliable electronic records.

1.1. Social Networking sites

Social Networking Site is a term used to describe websites which acts as a platform for interaction among people across the globe. It can be in various forms such as forums, blogs etc. through which people can communicate, exchange ideas and other multimedia.

When a user creates a profile on a particular social networking website, it allows him to share and discuss information and media with either the people on his friend list or with public at large. Social Networking relies upon users building up their own network of contacts on the sites, which in turn introduces them to new contacts. As the user network has increased, the risk related to the privacy of information and media which the user has uploaded has augmented. The crime rate on these networks is accelerating with addition of each user.

1.2. Cyber Crime

Cyber Crime can be explained as any criminal violation or unlawful act taking place on the computer. According to the Information Technology Act, 2000, cyber maybe said to include a computer, computer system or a computer network. Hence, any illegal act which involves a computer, computer system or a computer network s cyber crime. Information Technology Act, 2000 does not explicitly define the term cyber crime. When crime takes place on the Internet
there is exchange of information between computers connected to a network where some computers provide information, some seek for information and there are some which provide for smooth exchanges and route the flow of information.

Computer Crimes can be classified into following categories:

- Conventional Crimes through computer which includes cyber defamation, digital forgery, cyber pornography, cyber pornography, cyber stalking/harassment, internet fraud, financial crimes, online gambling, and sale of illegal articles.
- Crimes committed on computer networks include hacking/unauthorized access, denial of service.
- Crime relating to data alteration/destruction being virus/worms/Torjan horses/logic bomb, theft of internet hours, data diddling, salami attacks, stenography.
- Crimes relating to electronic mail such as spamming/bombing, spoofing.

Cyber crimes familiar to social networking websites are cyber defamation, cyber obscenity pornography, cyber stalking, hacking, privacy infringement, internet fraud, unauthorized disruption of computer system through virus and using any person’s copyright.

1.3. Cyber Defamation

According to Black Law defamation is an international false communication, either published or publicly spoken, that injures another’s reputation or good name. On internet, defamation imputation is published in electronic form. The issues related to defamation on internet include as to time of occurrence, the mode of publication, where the publication took place, i.e. the jurisdiction, who will be liable for the publication of the alleged defamatory statements. Cyber Defamation is covered under section 499 of IPC read with section 4 of IT Act, 2000. Section 499 lays down when the actual defamation takes place while section 4 of the IT Act provides for the legal recognition of electronic records. Therefore if any defamatory information is posted on the internet either through e-mails or chat rooms or chat boards, such posting would be covered under section 499 requirement of publication and would amount to defamation.

1.4. Cyber Obscenity and Pornography

Internet has brought with it vast knowledge and information for the individual and cyber obscenity and pornography is not distant to it. Easy accessibility and wide reach and availability of obscene material on the Internet have made it more convenient for individuals. Cyber pornography refers to stimulating sexual or other erotic behavior over the Internet which includes pornographic websites, pornographic magazines produced using computers to publish
and print the material and the Internet to download and transmit pornographic pictures, writings, etc. The geographical restrictions no longer exist and therefore, foreign publications can easily enter the local territories in a matter of seconds.

Child pornography on the Internet has been a matter of great concern as they are amongst the biggest users and beneficiaries of the Internet and constitute the most vulnerable group and are the worst sufferers of cyber pornography. Article 9 of the ‘Convention on Cybercrime’ merely imposes a duty upon the parties to offences of producing, offering or making available, distributing or transmitting, procuring or possessing child pornography intentionally and making the offenders criminally liable. Section 67B of the IT Act, 2000 criminalizes all kinds of online child pornography.

1.5. Cyber Stalking

Cyber stalking involves the act to pursue, harass or contact another in an unsolicited fashion using the electronic medium such as the Internet, e-mail, or other electronic communications devices to stalk another person.

Earlier there was no legislation against cyber stalking, but with The Criminal Law (Amendment) Act, 2013 section 354D was added which provided for criminalizing stalking and punishment for committing the offence of stalking.

Cyber stalking may involve electronic sabotage where a cyber-stalker may send hundreds of threatening or harassing e-mail messages by using sophisticated software that sends e-mail messages at regular or random intervals without perpetrator being physically present at the computer terminal.

1.6. Hacking

Hacking is when a computer system is accessed without the express or implied permission of the owner of that computer system. Hacking is usually a pre-planned process, where first a target computer system is identified; it’s security features are studied; tools are developed(passwords and programs) to gain unauthorized access and impair the normal(programmed functioning of a computer or a computer system or computer network. In this kind of crime the computer is a tool as well as the target. It is one of the most popular and fastest rising crimes and has accelerated with the help of Internet.
The meaning and scope of hacking under section 66 of the IT Act, 2000 is beyond than the mere ‘illegal or unauthorized access’ but that should have been done fraudulently and dishonestly.

1.7. Privacy Violation

The internet has many data collection mechanisms which collect a variety of information about surfers like the goods purchased, sites visited, and personal information and so on. It is possible to create profiles on the information collected from a range of sources, which can be paired with information about the user’s computer. The privacy of an individual can be infringed if there is unauthorized access to his account on a social networking website without his knowledge and the person obtains private information without the permission of the person.

There is no direct legislative provision with respect to privacy infringement on the internet but the IT Act, under sections 72 and 72A provides for penalty for breach of confidentiality and privacy and punishment for disclosure of information in breach of lawful contract respectively.

1.8. Internet Fraud

One or more components of the Internet such as chat rooms, e-mail, message boards, or websites are used to refer to any type of fraud scheme. Fraudulent activities can be conducted on social networking websites by persons impersonating to be somebody who they are not in order to commit an offence. Impersonating someone and then taking out information and other personal details also amounts to fraud. One can personally profit at other’s expense if personal information like bank account number, credit card number, telephone calling card number or any other valuable identifying data falls into wrong hands.

1.9. Virus Attacks

Virus attack the computer when programs transmitted are designed in a way to destroy, alter, damage, or even send across data residing in the computer. This transfer can be done by email, or sending messages on social networking websites asking the person to open the link and thereafter the virus attacks the computer system. Section 43 (c) of the IT Act, 2000 lays down the liability to pay compensation to the person who is affected by introduction of any computer contaminant or virus into any computer, computer system or computer network.
1.10. Copyright Infringement

Copyright is protecting original works of authorship that are fixed in any tangible medium of expression. Copyrighted material include the categories of literary works, musical works, dramatic works, pantomimes and choreographic works, pictorial, graphical and sculptural works, motion pictures and audio-visual works, sound recordings, architectural works and computer programmes. Any work copied on the Internet or from the Internet without acknowledging or giving credit to the original author will amount to copyright infringement and the person will be liable of the offence.

1.11. Conclusion

The Internet is a mammoth network of computers and that has made it a boon as well as a bane. On one hand everything has become so easy and convenient from shopping to cooking to playing games etc, on the other hand this has made cyber offenders to take advantage of the situation of this over dependency of people on the Internet. It can be concluded that more stringent laws should be made and implementation of these laws should be the main concern. There is lack of awareness among many individuals using the social networking websites and more often than not they are hesitant to take action against the offenders committing the offence.