**CHAPTER 1: INTRODUCTION**

This report is divided into five chapters, first chapter deals with objectives and research methodology of this report. Second chapter deals with Indian cyber stalking laws and its comparison with the laws of US, China and Russia. Third chapter consists of case studies and the fourth chapter tells about the data analysis and findings in which we have conducted a survey among 120 women to know about the current scenario of cyber stalking. Lastly, the final chapter consists of conclusion and recommendations of this report.

In India the use of internet has been growing at a faster rate. It is prevalent in every field like entertainment, business, sports, education and many more. Besides increasing opportunities in various fields it has also given rise to certain crimes which are dealt by the IT ACT 2000.However under Indian law, the term ‘cyber crime’ has not been defined under any Act enacted by the Indian Parliament. IT Act 2000 deals with offences related to cyber crimes. But the definition of cyber crime does not find any place either in IT Act, 2000 or in its amended version in the form of IT (amendment) act, 2008.

With the advent of digital technology the former descriptions such as “computer crime”, “crime by computer” has been replaced by the new term “cyber crime”. Other forms of such crime include “digital”, “electronic”, “virtual”, and “high-tech” crime.

Thus computer crime or cyber crime refers to any crime that involves a computer or a network. It is an unlawful act where the computer is used either as a tool or a target.

**Computer as a tool**: crime such as cyber stalking where individual is the main target of the crime the computer can be considered as a tool rather than the target.

**Computer as a target**: crime such as web defacement where the crimes are committed by a selected group of people with technical knowledge.

According to Pawan Duggal (cyber law expert) as more and more people take to the internet, cyber crimes and mobile crimes will continue to increase at an alarming rate. However, the fact remains that Indian cyber law is still ineffective in terms of delivering appropriate cyber crimes convictions. Further cyber fraud continues to increase with dramatic force in India. As per one Norton report, more than Rs50, 400 crores was lost by Indians during 2012 on cyber fraud itself and that trend showed no sign of lessening.

India is ranked 5th in worldwide in ranking of countries affected by cyber crime , claims a report by Security and Defence Agenda (SDA) and MacAfee reports of Sheetal Sukhija of ibnlive.com

Cyber stalking is a relatively new phenomenon and many countries are only now beginning to register the problem. India has also witnessed cases of cyber stalking, cyber harassment and cyber defamation. However, as there is no specific law or provision under the IT Act, a number of these cases are either not registered or are registered under the existing provisions of Indian Penal Code—which are ineffective and do not cover the said cyber crimes.

Since its promulgation, the IT Act 2000 has undergone some changes. One big change is the recognition of electronic documents as evidence in a court of law. Market players believe this will go a long way in giving encouragement to electronic fund transfers and promoting electronic commerce in the country.

However, all hope is not lost as the cyber crime cell is conducting training programmes for its forces. It also has plans to organize special courses for corporate to combat cyber crime and use them effectively.

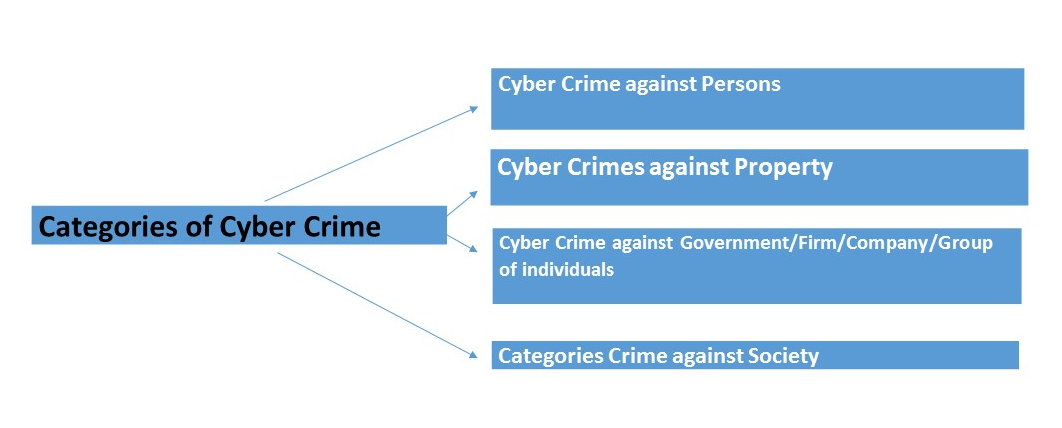
**CATEGORIES OF CYBER CRIMES**

**Cyber crime against person**. These crime includes harassment via e-mails, hacking, assault by threat, defamation etc.

**Cyber crimes against property**. These crimes include intellectual property crimes, cyber vandalism, transmitting virus, etc.

**Cyber crimes against government/firm/company/group of individuals**. These crimes include cyber terrorism, possession of unauthorised information, distribution of pirated software etc.

**Cyber crime against society**. These crimes include pornography, online gambling, forgery, sale of illegal articles etc.



**TYPES OF CYBER CRIMES**

**1. Unauthorized access and Hacking**

It means any kind of access without the permission of either the rightful owner the person in charge of the computer, computer system or computer network.

While hacking is a crime which entails cracking systems and gaining unauthorized access to the data stored in them.

**2. Virus, worms and Trojan attacks**

Virus is a programme that has the capability to infect other programmes and make copies of itself and spread into other programmes

Worms are programmes that multiply like virus but spread from computer to computer.

Trojan attack is an unauthorized programme which functions from inside seeming to be authorized programme and concealing what it is actually doing.

**3. Denial of service attack**

It involves sending of disproportionate data to the victim server beyond the limit that the server is capable to handle and hence, causes the server to crash

**4. Sale of illegal articles**

It includes sale of illegal articles and in these cases consideration is illegal and therefore, the agreement is void.

**5. E-mail related crime**

It includes e mail spoofing, e mail spamming and e mail bombing.

**6. Online gambling**

It includes website which are hosted on servers abroad that offer online gambling.

**7. Phishing**

It refers to acquiring information such as username, password, credit card details etc by disguising as a trustworthy entity.

**8. Intellectual property crimes**

Include distribution of pirated software, copyright infringement, trademarks violations etc. It is also known as cyber squatting.

**9. Web defacement**

Refers to substitution of original homepage of a website with another page by a hacker.

**10. Cyber terrorism**

Sec 66F Inserted vide ITAA, 2008. This section says that a person commits cyber terrorism if he uses cyberspace with intention to threaten the unity, integrity and security of a nation.

**11. Forgery and fraud**

Forgery refers to making of any false electronic record with intent to cause damage to the public or a person. Fraud refers to wilful commission of an act with intent to deceive the other.

**12. Identity theft**

Refers to all types of cyber crimes where someone wrongfully obtains and uses another person’s identity for his personal gain.

Of the above mentioned crime in this report we have discussed thoroughly about cyber stalking, and how adversely it has affected the society in India. Cyber stalking refers to the use of internet ,email or other electronic communication devices to stalk (harass) another person by mailing harassing phone calls, leaving written messages or objects etc. It is also known as online harassment or online abuse.

Recent statistics on cyber victim show that women victims generally outnumber male victims when it comes to cyber stalking. Working to Halt Online Abuse (WHOA), an organisation which deals with cyber stalking released a cumulative statistics which showed that out of 4,043 victims from the period of 2000-2013, 70% were women.

Almost all the researches done shows that cyber stalking is more of an interpersonal crime and the impact may be graver on women.

Almost every country has different laws relating to cyber stalking but in India we do not have any legislation related to this. Even the IT ACT 2000, which is India’s first cyber crime law, does not contain any provision relating to cyber stalking. With the help of this project we are discussing the loopholes in Indian law and the necessary steps to be taken in order to cater with this situation.

**OBJECTIVES**

To analyse the effectiveness of the existing laws in preventing cyber stalking.

To examine cyber stalking and victimisation of women.

To compare laws in India with other countries and suggest corrective steps to be taken.

**RESEARCH METHODOLOGY**

We conducted a survey among 120 people to know the trends of cyber stalking in an area. This is our primary source of data to know about the current status of cyber stalking prevailing in India.

Our secondary source of data includes various number of cases mentioning instances of cyber stalking and victimisation of women across India

This will help us to examine what is the current scenario of cyber stalking in India and what we can do about it.

**CHAPTER 2: LEGAL FRAMEWORK OF CYBER STALKING**

The Indian Information technology Act 2008 (amended) does not directly address stalking. But the problem is dealt more as an "intrusion on to the privacy of individual" than as regular cyber offences which are discussed in the IT Act 2008. Hence the most used provision for regulating cyber stalking in India is section 72 of the Indian information technology act (Amended) , 2008 which runs as follows;

Section 72: Breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

And also section 72A of the Information Technology Act, 2000(amended in 2008), which runs as follows:

Section 72A:Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008): Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

In practice, these provisions can be read with section 441 of the Indian Penal Code, which deals with offences related to Criminal trespass and runs as follows: Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property , or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate , insult or annoy any such person, or with an intent to commit an offence, is said to commit criminal trespass.

If the cyber stalking is done only to annoy the victim and is not resulted to serious offences like severe defamation, sexual crimes, identity theft or even grave crimes like terrorism, it is treated as a bail able offence.

However, after the December, 2012 Delhi gang rape incident, the Indian government had taken several initiatives to review the existing criminal laws. A special committee under Justice Verma was formed for this purpose and basing upon the report of the committee, several new laws were introduced. In this course, anti-stalking law was also introduced. The Criminal Law Amendment Ordinance, 2013 added S.354D to the Indian Penal Code to define and punish the act of stalking. This law is as follows:

S.354D of the IPC (as has been added by the Criminal Law Amendment Ordinance, 2013):

1. Whoever follows a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person or whoever monitors the use by a person of the internet, email or any other form of electronic communication or watches or spies a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person or interferes with the mental peace of such person, commits the offence of stalking.

Provided that the course of conduct will not amount to stalking if the person who pursued it shows

* 1. that it was pursued for the purpose of preventing or detecting crime and the person accused of stalking had been entrusted with the responsibility of prevention or detention of crime by the State , or
  2. that it was pursued under any enactment or rule of law, or to comply with any condition or requirement imposed by any person under any enactment, or,
  3. That in the particular circumstances, the pursuit of the course of conduct was reasonable.

1. Whoever commits the offence described in S.354D (1) shall be punished with imprisonment of either description for a term which shall not be less than one year but shall extend to three years and shall also be liable to fine.

**Punishment:**

Whoever commits the offence shall be punished for an imprisonment up to three years on first conviction and on a second or subsequent conviction the imprisonment could extend up to five years. In each case, the offender shall also be liable to pay the fine.

**How to Report Cyber-Stalking in India**

1. One must register a written complaint to her immediate cyber-cell in the city. In case of non-availability of cyber-cells in the city, one can file a F.I.R. in the local police station.
2. In case of non-acceptance of your complaint, one can always refer your complaint to the commissioner or judicial magistrate of the city.
3. Legal Assistance: If a woman approaches to the police station with an allegation of cyber-stalking she is entitled to legal counsel to help her file a case.
4. Privacy: The victim’s statement would be taken down in private. Often the cyber police station has women police officers/constables who can help the complainant to file a complaint.

**COMPARISON OF CYBER STALKING LAWS WITH THAT OF US, INDIA AND RUSSIA**

The challenges faced by cyber laws are vast due to geographical hurdles, cultural patterns and land laws governing one’s particular land. Easy access to cyberspace is one of the main reasons for the growth of cyber crime thereby threat to the National security of the country. There exists a dearth of adequate laws.

**India**

According to NASSCOM, there is extremely low rate of conviction of cyber crime in India. It saddens to say that India as a country in its 10 years old history of cyber crime investigation has so far witnessed only four convictions.

The statistics show that 1600 have been arrested against 3682, where the conviction is shocking 7 of which 3 are significant. To look into more detail the number of crime has gone up by 10 fold. I would like to bring to the notice that such a rise in the crime is due to low rate of conviction rate. In the year 2007, the arrests made were 154 while in the following year there was 178. In the years 2009 and 2010, the numbers of persons arrested were 288 and 799 and in 2011, it was 1,184. This shows clearly a huge rise in the number of arrests but yet a single digit conviction rate. A further study also show that 217,288, 420,966 and 1,791 cyber crime cases were registered under IT Act, 2000 during the years 2007, 2008, 2009, 2010 and 2011.

The Information Technology (Amendment) Act 2008 is the only Legislation that governs cyber crime in India. Till date it has brought various sweeping changes. The various sections that have been amended are Section 66 A - An offence to send offensive messages, Section 66B – An offence to receive stolen computer resource. Section 66C, 66D, 66E & 67F are inserted to declare identity theft, cheating and percolation, violation of piracy, video voyeurism and cyber terrorism and such which are punishable under the IT Act. The section 67A, 67B & 67C which provides punishment of imprisonment of three years and fine for acts such as, child pornography.

**1. Civil Wrong**

Section from 43 to 47 tackles the civil liability of individuals. The liability is to the extent of damages. The quantum of compensation is decided by the adjudicating officer as he has jurisdiction to adjudicate such claims which does not exceed Rupees five Crore. Section 64 provides for recovery of penalty as arrears of land revenue for the suspension of license or Digital Signature Certificate till penalty is paid.

**2. Criminal Wrong**

Section 65 –Tampering with computer Source Documents, imprisonment up to 3 years or fine which may extend to two lakh rupees or both.

Sec 66E – Punishment for violation of privacy, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees or both.

Sec 66 – Computer Related Offences with reference to section 43, punishable with imprisonment for a term which may extend to 3 years or with fine which may extend to five lakh rupees or both. This section has reference to IPC for some definitions.

Sec 66F – Punishment for cyber terrorism, shall be punishable with imprisonment which may extend to imprisonment for life.

Sec 66A – Punishment for sending offensive messages through communication service, punishable with imprisonment for a term which may extend to 3 years and with fine.

Sec 67 – Punishment for publishing or transmitting obscene material in electronic form.

Sec 66B – Punishment for dishonestly receiving stolen computer resource or communication device.

Sec 67A – Punishment for publishing or transmitting of material containing sexually explicit Act shall be punished on first conviction with imprisonment for a term which may extend to five years and with fine which may extend to ten lakh rupees and further punishment on subsequent conviction.

Sec 66C – Punishment for identity theft, punishment with imprisonment which may extend to 3 years and liable to fine which may extend to one lakh rupees.

Sec 67B – Punishment for publishing material depicting children in sexually explicit act in electronic form shall be punishable on first for a term to five years and with a fine which may extend to ten lakh rupees and for subsequent offence, punishment for term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Sec 66D – Punishment for cheating by personating by using computer resource, punished with imprisonment which may extend to three years and shall be liable to fine which may extend to one lakh rupees.

9. There are Other Offenses Covered under IPC and Special Laws

Sec 503 – Sending threatening messages by email

Sec 464- False document

Sec 499 – Defamation

Sec 468 – Forgery for cheating

Sec 463- Forgery

Sec 469 – Forgery for purpose of harming reputation

**USA**

1. The Wire Fraud Statute: being the first law used to prosecute computer criminals in the USA. It was seen that the communication wires were used in international commerce to commit fraud. To overcome such US passed the Law so as to prohibit the use of communication wires. This was an effective statute as it was to overcome defrauders trying to obtain money, property by false representation or promise; modus operandi being radio or television communication, signs or signals. This statute was successfully used in 1970’s and 1980’s to convict government officials of defrauding the public of its intangible right [8]. In a paradigmatic case Governor Marvin Mandel of Maryland was convicted of mail fraud for promoting certain legislation beneficial to the owners of a race in violation of his obligation to render the citizen of the state fair and impartial service free from bribery.

2. EEA Economic Espionage Act passed in 1996: To stop trade secret misappropriation. There being other Statute namely National Stolen Property Act and Virginia Internet Policy Act comprising of 7 bills. The proposed Computer Crime Legislation namely,

3. FOISA – Fraudulent Online Identity Sanction Act, registering online domain under false identification, increase jail time to provide false information.

4. CSPCA – Computer Software Privacy and Control Act, to deal with eighth problems of spyware. When passed it would prohibit transmission of software that collects and transmits personal information about the owner or operator of the computer.

The US legal system is and always more tech savvy and specialized to tackle various issues. In case of credit Card Fraud in USA there is a separate Federal Credit Card Law that stipulates the consumer. The Fair Credit Billing Act (FCBA) will apply to billing errors on credit card, unauthorized charges, charges for goods and services. This Act is an attempt to minimize Credit Card Fraud in India.

**China and Russia**

Recent reports by UK and US-based private information security companies and government intelligence agencies suggest that China and Russia invest their resources in industrial espionage, and that the risks of cyber-attacks from these two countries are very high. Law firms have been identified as high-risk targets…101 Indeed, the international fear about the threat of cyber attacks from People’s Republic of China is growing rapidly; meanwhile, however, China also has its own internal concerns about protecting their cyberspace and fighting cyber crimes within the country.

The Chinese government appears to pay more attention to cyber-crimes that involve damaging the political stability and state unity rather than other cyber-criminal behaviours, such as online fraud. We have not uncovered public documents that discuss cyber-warfare or cyber-attacks by foreign interests.

The Law and the need for Warrants Several Ministries regulate cyber-crime and cyber-security in China. Among them are the Ministry of Internal security, and the Ministry of State Security, which handles external security.

In 1999 China created the National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNCERT/CC.) CNCERT/CC operates under the administration of the Ministry of Information Industry and its main responsibilities include a national cyber security monitoring centre, operation centre, assessment centre, and media centre, and support for the government so it can meet relevant social and public responsibilities regarding cyber security.

China’s Criminal Law was amended in 1997, 2000, 2009 and 2011 to refer to cyber-crimes.106 the main provisions are as follows:

Article 285a – Accessing [hacking] of computer systems in the areas of State affairs, national defence or sophisticated science and technology

Article 285b – Obtaining of computer data and controlling of computer systems

Article 285c – Provision of programs or tools used to access or control computer systems

Article 286 – Sabotaging computer systems or data, that results in systems failure.

Chinese regulations stipulate that ISPs must record data and provide them to the authorities upon request. There are no clear provisions on real-time surveillance in the regulations. China has not joined any of the international treaties for cyber security, although it considers itself as having standards equal or superior to the Budapest Convention standards. China has long viewed to Council of Europe Treaty as “regional”, and has called, with Russia, for the UN to play a leading role in the creation of an international governance framework for the internet and its security.

**CHAPTER 3: CASE STUDY ANALYSIS**

**Findings from secondary data** -

**CASE 1**

Delhi university law student charged with cyber stalking.

In the case of (chauhan, 2011) it was found that the accused used to stalk her and created fake profiles of her on social networking sites to defame her.

A case under section 66-A of Information Technology Act 2000 was lodged and in the complaint, the victim said that she was a victim of cyber stalking and identity theft which has created grave problems for her and her family.

**CASE 2**

First conviction in cyber stalking case in Maharashtra.

In this case (shah, 2015), a 35 year old man was convicted in a cyber stalking case in Maharashtra. This was the first conviction in a cyber stalking case in Maharashtra. The man use to send obscene material and photos to a women he met online. A case was registered under section 509[outraging the modesty of a woman] of Indian Penal Code and section 66[E] [punishment for violation of privacy] of the Information Technology Act 2008.

**CASE 3**

Women employee cyber stalked by hacking.

In this case (TOI, 2003), a woman received a series of e mails telling her to pose nude for the stalker or give him Rs 1,00,000.He threatened to put her photos on adult websites, he even mailed her photographs to her e-mail address and it was found that the stalker hacked her e-mail which contained her photographs. A case was registered under section 509 of Indian Penal Code and under Information Technology Act, 2000.

**CASE 4**

Cyber stalked by own relative.

In the case, (HI, 2017), police arrested a cyber stalker who had posted indecent videos of a girl on porn websites and sent the links to all of her relatives as she refused to appease his requests. The victim was identified and he was a relative of the victim. The complaint was lodged and the case was registered.

**CASE 5**

First conviction in cyber stalking case in Kanpur.

In this case (Correspondent, 2016), a man was convicted for stalking a teenage girl on internet, creating a fake face book account in her name and posting obscene morphed pictures. This was the first conviction in a cyber stalking case in Kanpur. The case was registered under provisions of IT Act, 2000 and under protection of children from Sexual Offences Act, 2000.

**CHAPTER 4: DATA ANALYSIS AND FINDINGS**

The survey conducted clearly shows that out of 120 women, more than half of them [55%] belonged to the age group of 19 or under, followed by the age group 20-30 with 35.8% , then age group 31-40 with 6.7%,41-50 with 1.7% and finally age group 71 and above with 0.8%.

The survey shows that a large number of women are currently residing in Delhi. After Delhi, Gurugram comes second, followed by Faridabad, Noida and UP. Lastly Patna, Bangalore, Karnataka and Mumbai have least an equal number of women.

It was found that everybody uses the internet on a daily basis.

Out of 120 women, everyone [i.e.100%] uses internet on a daily basis and 98.3% of them uses social media.

Out of the various social media sites, 66.4% use WhatsApp messenger, 33.6% use Facebook, 22.7% use Instagram, 5% of people use other social media sites and 25.2% uses all of the social media sites listed except Twitter.

72.5% of women consider themselves as an intermediate in terms of their computer knowledge, 18.3% think themselves as a beginner and 9.2% see themselves as expert/professional.

In the past one year, 61.7% of the women felt that they are safe on the internet while 38.3% felt unsafe while surfing the internet.

33.3% of women experienced that somebody has tried to access their personal information like messages or e-mail, 13.3% have received threats or abusive messages in chat rooms while 17.8% of them have received via social networking sites, 8.9% have received threats through e-mail and messages. Rest 29.2% have experienced behaviours of cyber stalking in another ways.

Out of 120 women, 65.8% of women have been harassed online by unknown people, 2.5% by ex-partner, 3.3% by a friend, 0.8% by work colleague and rest 29.2% by others.

80.8% of the women did not inform anybody about themselves being harassed while 19.2% reported someone.

**CHAPTER 5:** **CONCLUSION AND RECOMMENDATIONS**

At the beginning of the new millennium, the internet has the potential to empower women by allowing them access to information and social support regarding their physical and mental health concerns and by facilitating online advocacy for changes in public and organizational policy. There are risks and potential hazards, however that need to be confronted. Inaccurate information, loss of privacy, error in communication, online harassment and cyberstalking can all lead to online victimization. Users, both individuals and human service agencies, must understand and protect against these dangers if the potential of the Internet to provide services is to be realized.

There is little known about the extent to which cyberstalking is taking place, but the number of case reports related to online harassment is increasing. Many anecdotes and stories of cyberstalking have been reported, 48 Colleges across the country are increasingly dealing with cases of cyberstalking.

Cyberstalking can be a terrifying experience for women, placing them at risk for psychological and possible physical harm. Prevention and education about online safety issues are necessary but not sufficient. Laws are reflective of societal values and principles in rules of social conduct. The Internet has evolved faster than laws that govern it. Legal mechanisms that both inhibit online abusive behaviour and punish it must be developed nationally

1. Modernization of police force of India is need of hour. We need modern police force that can easily deal with the latest technology of electronic and social networking, where the possibilities of related crimes and its misuse is to be aware well in advance. They should take lead in awareness program.

2. Human service organizations should institute measures to protect the confidentiality and security of online messages through using password protection of their computer and maintaining storage of back-up files in a secure place.

3. Stringent norms and strict regulations is required in our country.

4. Cyber security should be increased for example strong passwords should be used, confidential information should be protected etc.

**REFERENCES**

# Bibliography

chauhan, N. (2011, june 20). *TNN.* Retrieved from times of india: imesofindia.indiatimes.com/city/delhi/DU-law-student-charged-with-cyber-stalking/articleshow/8917937.cms?from=mdr

Correspondent, H. (2016, october 23). *HT.* Retrieved from Hindustan Times: http://www.hindustantimes.com/india-news/man-gets-two-year-jail-term-for-cyber-stalking-posting-obscene-pictures/story-Fgbd4KHeMQw9fxh0tPytYK.html

HI. (2017, MARCH 23). *THE HANS INDIA.* Retrieved from HANS INDIA: http://www.thehansindia.com/posts/index/Crime/2017-03-05/Youth-arrested-for-cyber-stalking-girl/284769

shah, V. k. (2015, july 4). *HT.* Retrieved from Hindustan times: http://www.hindustantimes.com/mumbai/35-yr-old-first-convict-in-a-cyber-stalking-case-in-state/story-sjIiVKJOGxwwUdr4UYyz6O.html

TOI. (2003, december 26). *TOI.* Retrieved from India Forensic: http://indiaforensic.com/cyberstalking.html

Correspondent, H. (2016, october 23). *HT.* Retrieved from Hindustan Times: http://www.hindustantimes.com/india-news/man-gets-two-year-jail-term-for-cyber-stalking-posting-obscene-pictures/story-Fgbd4KHeMQw9fxh0tPytYK.html

labh, M. (2015, may).

shah, V. k. (2015, july 4). *HT.* Retrieved from Hindustan times: http://www.hindustantimes.com/mumbai/35-yr-old-first-convict-in-a-cyber-stalking-case-in-state/story-sjIiVKJOGxwwUdr4UYyz6O.html

TOI. (2003, december 26). *TOI.* Retrieved from India Forensic: http://indiaforensic.com/cyberstalking.htm

**ANNEXURE**

SURVEY ON CYBER STALKING

A SHORT SURVEY ON CYBER STALKING

\* Required

Please tick the appropriate age group \*

19 OR UNDER

20-30

31-40

41-50

51-60

61-70

71 OR OVER

Please state which city you currently live in? \*



Your answer

How often do you use the internet? \*

EVERYDAY

EVERY WEEK

EVERY TWO WEEKS

EVERY MONTH

Do you use social media? \*

YES

NO

If yes, which social media you use frequently?

FACEBOOK

TWITTER

WHATSAPP

INSTAGRAM

ALL OF THE ABOVE

Other:



How would you rate yourself from the table below regarding computer knowledge? \*

BEGINNER

INTERMEDIATE

EXPERT/PROFESSIONAL

In the past 12 months, have you ever felt unsafe on the internet? \*

YES

NO

Have you ever experienced any behaviour associated with cyber stalking from the list below? If yes, please tick the appropriate one[s]

YOU HAVE BEEN SENT THREATENING OR ABUSIVE E-MAIL MESSAGES

HAVE RECEIVED THREATS OR ABUSIVE COMMENTS VIA SOCIAL NETWORKING SITES

HAVE RECEIVED THREATS OR ABUSIVE COMMENTS IN CHAT ROOMS

SOMEBODY HAS TRIED TO ACCESS CONFIDENTIAL INFORMATION ON YOUR COMPUTER SUCH AS E-MAIL MESSAGES

Other:



If you have been harassed, who was the person who harassed you? \*

DON"T KNOW

EX-PARTNER

FRIEND

WORK COLLEAGUE

Other:



Did you report the harassment to anybody? \*

YES

NO

SUBM