INTRODUCTION-

There is no denying that we live in the age of technology. It is an essential part of everyday life and is constantly improving to do more and more impressive things. Along with the shift in technology, a shift in society and the way that we think and operate is also coming along as a consequence to the technological advances. There has been much debate on whether the effects of technology on society as a whole have been beneficial or not. One important debate in this is cyber stalking.

MEANING AND DEFINITION-

For a layman, Cyber stalking refers to the crime of using the Internet, email, or other types of electronic communications to stalk, harass, or threaten another person by sending harassing emails, instant or text messages, or social media posts, or creating websites for the sole purpose of tormenting the victim. In law, Cyber stalking is a criminal practice where an individual uses the Internet to systematically harass or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging clients and any other online medium. Cyber stalking can also occur in conjunction with the more traditional form of stalking, where the offender harasses the victim offline. There is no unified legal approach to cyber stalking, but many governments have moved toward making these practices punishable by law.

EVOLUTION & HISTORICAL BACKGROUND-

While there is little information available on the history of cyber stalking and cyber bulling, it is very evident that from the inception of the internet, that the possibility of stalking and bullying on the internet are very real.

With an increase in social media sites, committing a cyber crime such as cyberstalking is getting easier. Not to mention that if you upload media from your smart phone you could be
giving away your location without even knowing it. There are even apps for smart phones that allow you to track your friends.

Cyber stalking is sometimes referred to as Internet stalking, e-stalking or online stalking.

TECHNIQUES-

Cyber stalkers use a variety of techniques. They may initially use the Internet to identify and track their victims. They may then send unsolicited e-mail, including hate, obscene, or threatening mail. Live chat harassment abuses the victim directly or through electronic sabotage (for example, flooding the Internet chat channel to disrupt the victim’s conversation). With newsgroups, the cyber stalker can create postings about the victim or start rumors that spread through the bulletin board system.

Cyber stalkers may also set up a web page on the victim with personal or fictitious information or solicitations to readers. Another technique is to assume the victim’s persona on-line, such as in chat rooms, for the purpose of sullying the victim’s reputation, posting details about the victim, or soliciting unwanted contacts from others. More complex forms of harassment include mail bombs (mass messages that virtually shut down the victim’s e-mail system by clogging it), sending the victim computer virus, or sending electronic junk mail (spamming).

There is a clear difference between the annoyance of unsolicited e-mail and on-line harassment. Unsolicited e-mail is to be expected from time to time. However, cyber stalking is a course of conduct that takes place over a period of time and involves repeated, deliberate attempts to cause distress to the victim. People who do not have access to the Internet, or who choose not to go on-line, are not immune from cyber based crime. Databases of personal information available on the Internet can enable a stalker to trace a victim’s user name to their real name, address, telephone number, and other personal information, or can enable a stalker to impersonate the victim on-line.

The offender can then harass the victim on the computer via e-mail or at home through mail, telephone calls, or even by appearing at the victim’s home or workplace. Telecommunication technologies also make it much easier for a cyber stalker to encourage third parties to harass and/or threaten a victim.
Most of the cyber stalking cases that have been prosecuted did not involve technically complex forms of stalking, and e-mail was simply being used as an alternative form of communication.

However, this is not always the case.

The availability of anonymous software provides a high degree of protection for stalkers seeking to cover their tracks more effectively. Examples of these types of technologies are “anonymous re-mailers,” which automatically shield the sender’s identity with pseudonyms and send the e-mail through servers that instantly erase digital tracks to prevent later access by anyone, even law enforcement.

The more complex software and computer technologies become, the easier it is for cyber stalkers to operate anonymously, and the more difficult it is for law enforcement to investigate and collect enough evidence to support prosecutions. In order to address cyber stalking, it is critical to understand stalking in general.

In many cases, cyber stalking is simply another phase in an overall stalking pattern, or it is regular stalking behaviour using new technological tools. Therefore, strategies and interventions that have been developed to respond to off-line stalking can often be adapted to on-line stalking situations.

There are federal, state, and local criminal justice agencies which have begun to focus on stalking, and some have recently developed special task forces to deal with cyber stalking.

**INDIAN LAWS ON CYBER STALKING**

1) **THE INFORMATION TECHNOLOGY AMENDMENT ACT 2008**

S.66A Punishment for sending offensive messages through communication service, etc -Any person who sends, by means of a computer resource or a communication device,—

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,
(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.— For the purpose of this section, terms “electronic mail” and “electronic mail message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, images, audio, video and any other electronic record, which may be transmitted with the message.

2) S.72 Breach of confidentiality and privacy- 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

3) S.72A Punishment for disclosure of information in breach of lawful contract-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 fine which may extend to five lakh rupees, or with both.

These sections are read with section 441 Indian Penal Code -Criminal trespass.— 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 intent to commit an offence, is said to commit “criminal trespass”.

SECTION 354D IPC
(1) Any man who—

follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or

monitors the use by a woman of the internet, email or any other form of electronic communication,

commits the offence of stalking;

Provided that such conduct shall not amount to stalking if the man who pursued it proves that—

i. it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or

ii. it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

iii. in the particular circumstances such conduct was reasonable and justified.

Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.
CYBER STALKING INTERNATIONAL PERSPECTIVE-

In the United States the government quickly recognized the possible multi-jurisdictional nature of stalking and the problems that came along with it. Next to the difficulties that may derive from international cyber stalking the American police and prosecution service have to deal with the complexity of a federal system as well. Given the fact that stalking is regulated on a state level, this means that there is a concern to harmonize state laws and procedures within the United States.

The United States opted for a two-track approach to harmonize state legislation and to counter interstate (cyber)stalking: first, the creation of a Model Anti Stalking Code and second, the adoption of a federal anti-stalking law. In 1993, before the majority of the states had drafted anti-stalking legislation, the National Institute of Justice developed a model anti-stalking code to encourage states to adopt anti-stalking measures themselves and to provide them with a template that was expected to withstand the anticipated constitutional challenges.

As a result many states incorporated provisions of the code in their states statutes. Still there are differences between the various anti-stalking laws.

States differ for example in their anti-stalking legislation as to the type of repeated behaviour that is prohibited, whether a threat is required, the reaction of the victim to the stalking and the intent or mens rea of the perpetrator. Although most (cyber)stalking cases will fall within the jurisdiction of state authorities there are instances where state law is inadequate, where questions of jurisdiction arise or where state agencies do not have the expertise or resources to investigate and prosecute a case. In 1996, a federal interstate stalking law was enacted that prohibits individuals from travelling across a state line with the intent to injure or harass another person. State law therefore needed to be supplemented by federal law for cases that did not stay within the domain of one single state.

In 2000, the Violence Against Women Act amended the interstate stalking law so that it would include travelling across national borders. It also expanded the statute to cover conduct with the intent to kill or intimidate another person. In drafting the federal statute, the federal legislator could have chosen to bridge the variations that exist among state stalking laws.
One could think of using the strictest definition so that the prohibited behaviour was already criminalized in every state. What is remarkable is that the federal regulation is in fact not in line with many of the state anti-stalking laws or the Model Anti-Stalking Code.

In state law stalking is generally defined as ‘the wilful or intentional commission of a series of acts that would cause a reasonable person to fear death or serious bodily injury and that, in fact, does place the victim in fear of death or serious bodily injury’. In contrast to the majority of state laws, the federal law does not require an actual reaction from the victim to classify conduct as cyber stalking. So the stalking does not have to cause the victim to actually fear for death or bodily injury. Furthermore, the federal law is a ‘specific intent’ crime, meaning that it requires proof that the stalker intended to cause the victim to fear death or personal injury.

Many states, on the other hand, handle a ‘general intent’ requirement, implying that the stalker simply intentionally committed prohibited acts without necessarily intending the consequences of those actions. On top of that, cyber stalking with an inter-jurisdictional component is criminalized even in states where cyber stalking as such has not been criminalized at all.

In Illinois, Maryland, Hawaii, Connecticut and Wisconsin, the anti-stalking statutes all use narrow definitions of stalking that involve following, approaching or otherwise maintaining a physical proximity to a person. The power to impose federal legislation that is not in conformity with state law is inherent in the American federal system, but things become more complicated in an international context when states are autonomous and have the right to withhold from ratification if they do not consent with certain provisions.

Before assessing what legislation would be most suitable to deal with international stalking in the European – or even in a global – context and how this legislation needs to be worded in order for it to succeed, it is necessary to first have a look at the way stalking is criminalized in most European member states.

If there is sufficient common ground, drafting anti-stalking legislation that is widely accepted will not be that complicated. Cyber stalking that is not supplemented with behaviour that has a connexion with the offline world is not subjected to penalty in those states.
UAE Legal Framework—There is no specific data protection law in the UAE, however there is a data protection law in certain free zones. For the rest of the UAE, restrictions and or penalties relating to data privacy can be found in a number of legislative sources including:

- The UAE Constitution of 1971, which enshrines the right to privacy of personal information and guarantees "Freedom of communication by post, telegraph or other means of communication and the secrecy thereof."

- The UAE Penal Code of 1987 (as amended), which in particular prohibits:
  
  o (a) the publication, through any means, of news, pictures or comments pertaining to the secrets of people’s private or familial lives;
  
  o (b) any person who by reason of profession, craft, circumstance or art, is entrusted with a secret from disclosing or using (to his or another’s advantage) that secret without the consent of the individual concerned or where not otherwise permitted by law; and
  
  o (c) the interception and/or disclosure of correspondence or a telephone conversation without the consent of the relevant individuals. For those who fail to adhere to the law, the Penal Code sets severe penalties, which include fines and imprisonment.

- The UAE Civil Transactions Law, Federal Law No. 5 of 1985 (as amended), provides that a person is liable for all acts causing harm. This could include harm caused by un-authorised use or publication of the personal or private information of another.

Some other UAE laws that contain privacy protection and or requirements relating to data collection, storage and use (other than the Penal Code; Civil Transactional Law and the Constitution) include:

- Labour Law (Law No. 8 of 1980 as amended).
- Electronic Transactions and E-Commerce Law (Dubai Law No. 2 of 2002)
- Combating Cyber Crimes Law (Federal Law 2 of 2006)
- E-transactions and E-commerce (Federal Law No. 1 of 2006)

Free Zones

Certain Free Zone areas of Dubai International Financial Centre (DIFC) and Dubai Healthcare City (DHCC) have enacted comprehensive data protection framework based upon
the European model, which place a number of obligations on businesses established in those zones. These include restrictions on transferring personal data or patient health information to recipients located in jurisdictions outside the DIFC or DHCC respectively, without the individual's consent.

**Transferring Data Overseas**

In addition, UAE companies performing cross-border data transfers may also be subject to data protection rules of the jurisdiction from which the data is exported. This is a particularly important consideration for intra-group transfers where, for example, under the EU Data Protection Directive, such transfers may take place only if there is an adequate level of protection for the data or information in the importing jurisdiction and the exporting company retains primary liability for any data breach.

**LANDMARK JUDGEMENTS**

**CYBER PORNOGRAPHY CASE ODISHA** - In what is being touted as the first conviction in a ‘cyber pornography’ case in Odisha, RTI Activist Jayanta Das has been awarded 6-year jail term and asked to pay Rs 9,000 fine by Puri SDJM Court for defaming a lady on internet in 2012.

The accused has been convicted for sending obscene messages to a lady, defaming and causing mental harassment by putting up her personal details and information on a pornographic website.

The crime branch had earlier arrested Das on September 18, 2012 basing on the complaint filed by the victim same year in July.

The accused Jayanta Das had uploaded all the personal information of the victim in a bid to take revenge from her husband based in Puri.

Crime branch officials said that Das had posted the mobile number, address and private information of the victim on [deshunt.com](http://deshunt.com) website.

Being a pornographic and wife swapping website, the victim received calls from various persons asking more details about her.
Initially, the victim’s husband had lodged a case with Puri police who had failed to make any headway. Later, the crime branch took the case in August 2012 and the accused was arrested following a detailed investigation.

The accused was arrested under section 292, 465, 469, 500 of the Indian Penal Code and 66(C) and 67 (a) of the Information Technology Act.

Senior Crime Branch officials informed that Jayanta Das was involved in a six criminal cases including attempt to murder and illegal use of fire arms.

“During the course of trial the prosecution produced 13 witnesses including scientists of the Central Forensic Science Laboratory, Kolkata; while 55 documents were also exhibited,” said Special Director General of Police (Crime Branch) BK Sharma

**STATE V. YOGESH PRABHU**

Mumbai Cyber Cell secured first ever conviction in Maharashtra under the IT act on Friday. The case was investigated by the cell for online stalking in 2009.

Metropolitan Magistrate court convicted Yogesh Prabhu for stalking and sending obscene images to his colleague. The court sentenced him to three-years imprisonment and a fine of Rs 10,000 under relevant sections of the IT Act and Rs 5,000 fine under the Indian Penal Code. The conviction was procured on evidence, including crucial witness statement stating that the crime was committed using a laptop sponsored by office.

According to the prosecution’s case, the complainant communicated with Prabhu through online networking site Orkut. However, on one occasion Prabhu sent the complainant obscene messages, following which she removed him from her friend list. A few days later, she received an email from an unknown person with “foul and objectionable language”. The complainant continued to receive the emails and she eventually sent a complaint to Joint Commissioner of Police (Crime).

Following the complaint, the cyber cell traced the IP address and found that it was sent from the same office where she worked and it was the same person the complainant chatted with, Prabhu.
EFFECTS-

As with all stalking, the greatest trauma is the faceless terror that it brings into a victim’s life—24 hours a day, seven days a week. The Internet becomes an electronic curtain behind which the stalker hides while terrorizing the victim at home and work, with friends and neighbours, and with countless people that the victim does not even know.

Cyber stalkers may be located on the other side of the world, across the country, across the street, or in the next cubicle at work. They could be a former friend or lover, a total stranger met in a chat room, or simply a teenager playing a practical joke. The inability to identify the source of the harassment or threats is one of the most ominous aspects of this crime for a cyber stalking victim.

The fact that cyber stalking does not involve physical contact may create the misperception that it is less threatening or dangerous than physical stalking. Cyber stalking is just as frightening and potentially dangerous as a stalker at the victim’s front door.

The psychological torment is very real, even in the absence of a distinct physical threat. It totally disrupts a victim’s life and peace of mind. Cyber stalking presents a range of physical, emotional, and psychological trauma for the victim, who may begin to develop or experience: ‘Sleep disturbances; ‘Recurring nightmares; ‘Eating pattern disturbances; ‘Hypervigilance; ‘High levels of stress; ‘A feeling of being out of control; and/or ‘A pervasive sense of the loss of personal safety

HOW TO AVOID IT-

1. Avoid Posting Personal Data on Your Social Media Accounts

Apps such as Facebook, Twitter, Instagram, and Snapchat have made sharing information easy but more dangerous. Most people wouldn’t think twice about posting their personal email address, mobile number, or even their real home address. This makes it easier for stalkers to get a hold of your information and use it to harass, or worse, hack into your other accounts. Your personal information can sometimes be used to get past your credit card security and other financial accounts. To avoid being the target of a stalker, consider using a separate email account every time you register for social media apps. As much as possible, never post your home phone number, birthday or real home address, especially if you have public accounts.
2. Conduct an Internet Search of Your Name Regularly

You may not be posting things about yourself, but you can’t prevent all your friends from posting your photos and other information about you. Keep your name and identity protected by doing a regular search on the Internet. By doing this, you can prevent a cyberstalker from spreading false things about you through a blog, Craigslist account, or webpage. Once you find false information about yourself online, you can contact the website or the server administrator to request that the content be immediately removed.

3. Be Mindful of Your Passwords

Never underestimate the power of a unique password. Stalkers have a number of methods of trying to hack into their victims’ account, and passwords are your first line of defense. This is why they have to be unique and strong. Don’t use personal information such as your birthday, your anniversary or the place where you were born. Experts also recommend changing all your passwords every year. Answers to your secret questions should also be hard to guess, in order to give hackers and cyberstalkers an even harder time breaking into your accounts. More importantly, do not write your passwords on paper or share them to strangers.

4. Be Wary of Emails, Texts, Phone Calls that Asks for your Personal Information

A popular means of online marketing today is doing a survey. A representative of the company can call, email, or text a survey form to you. These survey forms usually ask you to verify your identification and provide personal information. If you feel suspicious about the activity, you can always opt to decline whatever it is they’re offering. If you want to know more about the product, try giving away secondary information like a work address or phone number and an alternate email address. Under any circumstance, never reveal your credit card identity pin and your social security number.

5. Change all Account Security If You Are Leaving a Relationship

In most incidents, the victims’ former partners are usually the ones who are behind cyberstalking. Especially in cases where there has been abuse, the dominant partner will still want to control his ex-partner even after the relationship has ended. Cyberstalking is the perfect tool for them to exert their power. If you are leaving a relationship, especially an abusive one, consider changing all your passwords or creating new accounts online. You also need to remind your bank that you are no longer in a relationship with this person and that he
can no longer access your account – this is especially true for those who have a joint bank account.

6. Seek Professional Help If You Are Being Cyberstalked

If the harassment and stalking escalate and make you feel unsafe or threatened, it is important that you enlist the help of trained professionals. Aside from reporting the incident to law enforcement, you can also seek the help of private investigators, especially if the stalker’s identity is still unknown. Reliable PIs conduct thorough surveillance and research to help find your online abuser and collect data against him. The faster you take action, the less chances the stalker can inflict permanent damage in your life.

Online stalkers get off on the rush of being able to render their victims helpless. They find ways to permeate important aspects of their victim’s life and, in turn, control them with just a click of a button. Thankfully, you can avoid becoming the target of online harassment by being cautious about your online information, protecting your passwords, and asking for professional help. Only by staying vigilant about your online information can you ward off unnecessary attention from possible stalkers.