Law Journals

National Journal of Cyber Security Law

Volume 3, Issue 2
www.stmjournals.com

A Grey Area in the Bright Future of Cyber Law: Cyber Pornography and Cyber Crime

Priya Jha[1,*], *Purvai Kaprate*[2]
[1,2]Student, New Law College, Bharati Vidyapeeth, Pune, Maharashtra, India

Abstract

The most common debate today is the ever-increasing influence of technology and the advantages and disadvantages it carries with itself. The prolonged and continuous use of technology has drastically affected the way people communicate. As Frank Abagnale has thoughtfully cited how technology breeds crime, the radical increase in cybercrimes, evidently proves the misuse of technology. This misuse is the main reason for the implementation and enactment of the cyber laws. This paper focuses on the emerging cybercrimes with an emphasis on cyber pornography along with issues relating to the implementation of respective law. The internet connects people from all parts of the world easy, fast and relatively. They have been developed to reduce the effort of people and provide countless visible advantages for human beings. Alongside the growing need of cyber space, it can also pose certain threats which have critical impact on the civilisation. It becomes a more dangerous place to be in, where the offenders roam freely to execute their malicious intentions encouraged by the anonymity that internet provides. The central idea behind this piece of research is to deal with the negative use of Information technology including 'cyber pornography' and possible changes needed in the system to combat with the problems relating to cyber-crime having safe and trustworthy transactions.

Keywords: *internet, cyber crime, transactions, malicious, threats, civilization*

***Author for Correspondence** E-mail: pjha2400@gmail.com

INTRODUCTION

Much like the industrial revolution, the Internet revolution has changed the way people exist. Over the last few decades, technology has become a particularly important source of knowledge and has provided numerous opportunities to individuals. Internet was initially available in the country through ERNET and was made available for commercial use in August 1995. The technology and innovation have changed our lives in all aspects; it can be stated as the driving force behind all the cultural and historical changes. Today with the propagation of the more and more advance technologies we are able to overcome various obstacles of time and space. Technology has provided number of tools and machines which can be used to gain an understanding of many unknown entities, meeting people over the world, maintain and strengthening effective communication and also help us to speed up the socialization process.

But, if the impact of technology is to be examined from other point of view, technological advancement has caused people distracted, exceedingly stressed and progressively more isolated. Technological burden has challenged the real meaning of well-being and has its impact on all the spheres of human existence. Apart from technology leading to an increased rate of frustration and stress, there is a remarkable increase in crimes including cyber space.

An unlawful act which uses cyberspace as a target or tool, or both is termed as cyberspace. Having a low risk and high rate of return investment, cybercrimes are increasing all over the world. It provides easy access of information and data, but it becomes very difficult to entrap the offender. The current scenario, where most of the information processing depends on the use of information technology, the development of adequate legislation has become an essential part of

cyber security. It can be observed that now there is a highly complex cybercriminal network, bringing together a community at a global level in real time to commit crime.

TYPES OF CYBER CRIMES

A Cybercrime includes a wide range of attacks on individuals as well as organisations. It contains all the computer mediate activities that are either extrajudicial or considered illicit by bound parties and which may be conducted through international electronic networks" [1]. It includes fraud, forgery and unauthorized access [2]. Bifurcating cybercrimes are dependent on the commission of crime and the targets that are affected.

Various Cybercrimes Arising out of the Commission of Crime Includes

Hacking

It is a crime basically done to access the personal or sensitive information of a person wherein the person's computer is accessed by the intruder without the person's permission with a motive of greed, fame, power, etc.

Virus Dissemination

Computers are infected with viruses that destruct the computer operation and affect the data stored and have a tendency to circulate them to other computers on network. Viruses are of two categories, one that only disseminate and cause no damage, and others those programmed to cause damages.

Logic Bombs

A logic bomb is a piece of code (not a virus but behaves somewhat in a similar manner) which is intentionally inserted into software to execute a malicious task. It is also known as slag code. It stays dormant until specific conditions are met.

Denial of Service Attack

It is an attempt to make services unavailable to the intended users usually carried on websites to stop them from functioning. It involves flooding a computer resource with more requests than it can handle resulting in server overload.

Phishing

It is a technique by which confidential information like credit card numbers, username and passwords is extracted out by mail spoofing.

Email Bombing and Spamming

It involves sending huge volumes of mail containing long and meaningless messages or infected files as attachment to the target address resulting in victim's email account crashing.

Web Jacking

Its name is derived from 'hijacking'. The hacker fraudulently takes control of the website and the owner no longer has any control over the website and the hacker can use it for his own selfish means. He may change the content of the original website or redirect the user to the similar looking fake page.

Cyber Stalking

It refers to a crime when a person is followed or pursued online. A cyber stalker does not follow the victim physically but virtually by following the online activity of the victim to harvest information. Cyber stalkers harass their victims via mail, chat rooms, discussion forums, blogs, etc. Social networking sites are a platform for socialization although it also increases the risk of internet violations.

Data Diddling

It is an unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done.

Identity Theft and Credit Card Fraud

It occurs when someone steals the identity of another person and pretends to be that person to access resources such as credit cards, bank accounts and other benefits. Credit card fraud involves the criminal use of the credit card of a person to fund the transactions.

Salami Slicing Attack

It is a technique where cyber criminals steal money for financial gains bit by bit so that there's no noticeable difference.

Software Piracy

Internet piracy is an integral part of our lives and everyone is capable of contributing to it, knowingly or unknowingly. Software piracy is

the unauthorized use and distribution of computer software. Pirated material may contain viruses, Trojans, worms and other malwares.

There are Certain Cybercrimes that Affect the Society at Large and Have a Critical Impact on the Civilization

Cyber Pornography

It involves the use of computer networks to create, distribute, or access materials that sexually exploit any individuals and also includes activities concerning indecent exposure and obscenity.

Cyber Trafficking

It includes trafficking in drugs, human beings, arms weapons etc. by the use of computer affecting large number of persons.

Financial Crimes

This type of offence is common as there is rapid growth in the users of networking sites and phone networking where the offender will try to attack by sending bogus mails or messages through internet.

Forgery

It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's lifestyle.

CAUSES OF CYBER CRIMES

Ease of Access

To fool biometric systems and bypass firewalls to get past many a security system is that there is every possibility of violating the technology by stealing access codes, recorders, pins, retina imagers etc.

Cyber Hoaxes

Cybercrime is committed to cause threats or damage one's reputation. Cyber Hoaxes is the most dangerous of all the causes. They believe in fighting their cause and want their goal to be achieved. They are called cyber terrorists.

Negligence

Negligence provides the criminals management to wreck the computer. There square measures prospects of not listening in protective the system.

Revenge or Motivation

It includes youngsters or those who are driven by lust to make quick money and they tamper with data like e-commerce, fraud in transactions and e-banking.

Poor Law Enforcing Bodies

Many criminals get away without being punished due to lack in cyber laws of many countries.

Cyber Crimes Committed for Publicity or Recognition

Generally, cybercrimes committed by youngsters where they just want to be noticed without hurting someone's sentiments.

Economically Motivated Cyber Crime

Money is the major motivator for many cyber criminals as is the case with many crimes committed outside the Internet. For example, pull in nearly 700 million bucks each year globally [3]. Business week estimates that cybercrimes targeting on-line banking accounts alone.

Personally Motivated Cyber Crime

Cyber criminals are still citizenry and what they are doing—as well as their crimes—is commonly the explanation for personal emotions and vendettas. From the dissatisfied worker putting in a scourge on workplace computers to a jealous boyfriend hacking into a girlfriend's social media accounts or a youngster taking down a college website simply to prove that he might make out, several cybercrimes are basically crimes of passion committed over the Internet. Several crimes, however, will still have serious impacts and cause hefty property harm [4].

Ideologically Motivated Cyber Crime

After financial Companies like DEBIT CARD, VISA, MASTERCARD, and PAYPAL refused to let account and card holders make contributions to the non-profit WikiLeaks, the "hacktivist" group Anonymous coordinated a series of larva attacks on the companies'

servers, rendering them unreachable to internet users.

REASONS BEHIND THE CYBER CRIME

There are many reasons behind the cybercrime; some of them are mentioned below:

a. For the sake of recognition
b. For the sake of money.
c. Lack of reporting and standards
d. Limited media coverage
e. Difficulty in identification
f. To fight a cause, one thinks he believes in
g. New opportunity to do legal acts using technical architecture
h. Official investigation and criminal procedure are rare.
i. Corporate cybercrimes are done collectively and not by individual persons.

CHALLENGES OF FIGHTING CYBER CRIME

Challenges of fighting Cybercrime is categorised into two types:

1. General Challenges
2. Legal Challenges

General Challenges

There is an endless discussion regarding the pros and cons of cybercrime. There are so many General challenges in front of us to fight against cybercrime. Some of them are discussed below:

a. For the defense forces, police and the security agency personnel there is no E-mail account policy.
b. Cyber-attacks have come from neighboring countries contrary to our national interest and also from terrorists.
c. Promotion of Research and Development in ICTs in today's era is not up to the mark [5].
d. Law enforcement Personnel and Security forces are not equipped to address high-tech cybercrimes.
e. At individual as well as organization level there is a lack of awareness and the culture of cyber security.
f. To implement the counter measure there is a lack of trained and qualified manpower.
g. The police are almost illiterate to cyber-crime because the minimum necessary eligibility to join the police doesn't include any knowledge of computer sector.
h. For training of the law enforcement, security personnel's and investigators in ICT are less budgets for security purposes as compared to other crimes.
i. It identifies the investigative responsibility for crimes that stretch internationally for which the present protocols are not self-sufficient.

Legal Challenges

Challenges in Drafting National Criminal Laws [6]

Proper legislation and precedent are the foundation for the prosecution and investigation of cybercrime. However, law makers must continuously monitor the effectiveness of existing provisions and respond to the internet developments, especially in the speed of developments in network technology. It takes a lot of time to update national criminal law to prosecute new forms of online cybercrime. Some countries have not finished this adjustment process. Offences that are criminalized under national criminal law need to be updated and reviewed. For example, digital information must have equivalent status as printouts and traditional signature. The delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law is the main challenge for the national criminal legal system.

Adjustments to National Law Must Start with the Recognition of an Abuse of New Technology

There are specific departments which is needed within national law-enforcement agencies, which are qualified to investigate potential cybercrimes. The development of computer security incident response teams (CSIRTs), computer incident response teams (CIRTs), computer emergency response teams (CERTs), and other research facilities have improved the situation [7].

Identification of Gaps in the Penal Code

It is necessary to compare the status of criminal legal provisions in the national law

with the requirements arising from the new kinds of criminal offences to ensure effective legislative foundations. The need for the legislative amendments is limited to those offences that are insufficiently covered by the national law.

For e.g. Laws addressing forgery may easily be applied to electronic documents.

Drafting of New Legislations

It is difficult for national authorities to execute the drafting process for cybercrime, without international as well as national cooperation due to the rapid development of complex structure and network technologies. National law can benefit from the experience of international expert legal advice and experience from the other countries.

New Offences

Law makers must analyze new and developing type of cybercrime to ensure their effective criminalization. The most important example of cybercrime which has not yet been criminalized in all countries is fraud and theft in computer and online games [8].

Developing Procedures for Digital Evidence

The number of digital documents is increasing as compared to the storage of physical documents due to the low costs [9]. In cybercrime investigations digital evidence plays an important role in various phases. It is possible to separate in four phases. The first phase deals with the identification of the relevant evidence. The second phase deals with preservation and collection of the evidence. The third phase deals with the analysis of digital evidence and computer technology. And lastly, the evidence needs to be presented in the court.

Increasing Use of ICTs and the Need for New Investigative Instruments

The introduction of increasing use of ICT'S and the need for new investigative instruments is always a result of a trade-off between the advantages for interference with the rights of innocent internet users and for law-enforcement agencies. Offenders use ICTs in various ways in the preparation and execution of their offences [10].

FUTURE TRENDS OF CYBER CRIME

One of the biggest concerns is what if there is a hack into the critical systems in companies, governments, financial institutions etc. This could cause malware in essential systems resulting in knowledge loss, misuse or maybe killing the essential systems. Since the communication flow is straight forward via the internet, the crime organizations would possibly merge and collaborate even more than they are presently. It is feared that due to increased quality, funds and other people may transfer easily. The Internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through that a lot of and a lot of international trade takes place, the opportunities for washing cash through over-invoicing and under-invoicing are likely to grow. Online auctions supply similar opportunities to move money through apparently legitimate purchases, however paying much more than goods are worth. Online gambling conjointly makes it attainable to move cash especially to offshore financial centers [11].

There are following points which we can focussed on future trends:

1. *Internet of things (IOS) Hacking*: The Internet of things has grown rapidly with the popularity of home devices like Google Home Hub and Amazon Echo.
2. *Social Engineering:* Murray Goldschmidt, COO of Information security firm sense of security, called Social Engineering "the new norm in hacking" in a recent post for CSO. These schemes are designed to trick users into giving up passwords or financial details or even to manipulate the outcome of current events.
3. *Maintain current security updates*
4. *Restrict access to your network*
5. *Change passwords frequently*

CYBER CRIME CASES

SMC Pneumatics (India) Private Limited Vs. Jogesh Kwatra [12] the defendant, a worker of the plaintiff's company started sending

defamatory emails to his workers different subsidiaries of the company all over the world. The plaintiff thereafter filed a suit for permanent injunction restraining the defendant from posting such defamatory messages. The counsel of the plaintiff contended that the emails sent by defendant were distinctly vulgar, obscene, abusive and humiliating in nature. Further these emails have harmed the reputation of the company all over the India and across the world. The Hon'ble Delhi High Court in this case allowed an ex-parte ad interim injunction observing that a prima facie case was made out by the plaintiff and restrained the defendant from posting such remarks.

In the Parliament Attack Case [12] the Bureau of Police Research and Development, Hyderabad had recovered a laptop from the terrorist who attacked the Parliament in 2001. The laptop, which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that confirmed the terrorist's motives and contained proof of the making of a forged sticker of the ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem. The emblems were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir. However vigilant findings by the court proved that it was all forged and made on the laptop.

In the Andhra Pradesh Tax Case, the owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 crore was recovered from his house by the Vigilance Department. The officials wanted evidence from him regarding the unaccounted cash. The alleged person submitted a total of 6,000 vouchers to prove the legitimacy of his trade, however on careful scrutiny of the vouchers and contents of his computer, it was evident that every one of them were made after the raids were conducted. The fact that the suspect was running 5 businesses beneath the presence of 1 company and used fake and computerized vouchers to show sales records and save tax was concealed. So, the questioning techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.

CYBER PORNOGRAPHY IN INDIA

Cyber pornography has increased over the past decade. The effects can be both negative including interpersonal distress and positive hereby increasing sexual knowledge and attitudes towards sex. The legal status of pornography adopted by various countries varies widely. Most of the countries allow least some form of pornography. The distribution and production of pornography are both extrajudicial except accessing pornography in private. According to Chapter XI, section 67 of the Information Technology Act, 2000 (IT Act), the Government of India clearly considers online pornography as punishable offence stating that:

Section 67 of the Information Technology Act, 2000 makes the following acts punishable with imprisonment up to 3 years and fine up to 5 lakhs:

1. Publication—which would include uploading on a website or on any other digital portal where third parties can have access to such content.
2. Transmission—this includes sending obscene photos or images to any person via email, messaging, WhatsApp or any other form of digital media.
3. Causing to be published or transmitted—this terminology is used where the intermediary portal is held liable; using which the offenders publish and transmit such obscene content. The Intermediary Guidelines under the Information Technology Act puts the burden on the Intermediary Service Provider to exercise due diligence.

Section 67A of the Information Technology Act makes publication, transmission and causing to be transmitted any material in electronic form containing sexually explicit act

or conduct, punishable with imprisonment up to 5 years and a fine up to 10 lakhs.

SOCIAL EFFECTS OF CYBER PORNOGRAPHY

With the growth and easy access of personal computer networks, cyber pornography has found a convenient venue for sexually abusing individuals. The executive and judiciary have found that detecting and prosecuting cyber pornographers has become a taxing task, leading to high failure rate of placing the offenders behind bars. The methods currently employed by law enforcement officers to combat cyber pornography are considered to be primitive and inefficient by many.

Pornography may happen to pose a great risk of sexually aggressive behaviour and may lead to subsequent increase in sexual violence. It may also increase aggression against females. The individuals affected by cyber pornography showed more global disturbances of personality. Pornography is noted to be progressive, besides being addictive.

CYBER PORNOGRAPHY CASES

In the case of State v. Jayant Kumar Das [13], an RTI campaigner Jayant Kumar Das was arrested in 2012 and convicted for cyber pornography. The complainant Biswajit Patnaik, working as a journalist in the vernacular daily stated that the accused had made severe attempts to defame the complainant's wife to take revenge on him. The accused had created a forged e-mail account and a fake profile in the complainant's wife name and had linked the fake profile to an America-based porn website with vulgar remarks and the complainant's phone number on the porn portal.

Disturbed with the said act the complainant filed a complaint against the accused in 2012 and the accused was arrested by the cyber cell of crime branch in August of the same year. A charge sheet was filed against him under Sections 292 (obscenity), 465 (forgery), 469 (forgery for the purpose of harming reputation) and 500 (punishment for defamation) of the IPC and 66C/67/67A of the Information Technology Act.

The case was dealt by Puri Sub-Divisional Judicial Magistrate Shibasis Giri who sentenced the convict six years of imprisonment and also slapped the convict with a fine of Rs-9,000.

In, *Avnish Bajaj v. State [14]* this case was about the child pornographic material where the girl was filmed by her boyfriend in very sexually explicit conditions. The case is commonly known as DPS MMS case or *Baazee* Case. In this case the MMS of the girl was listed on the website for sale and the website was baazee.com where a student of fourth year from IIT Kharagpur listed the MMS for selling on the website hence making it easily accessible on the internet. The CEO Avnish Bajaj was arrested for an advertisement of the sex scandal video. The video was not uploaded on the portal, despite that Avnish was arrested under Section 67 of the Information Technology Act. It was after this case that the Intermediary guidelines were passed in 2011 whereby an Intermediary's liability would be discharged if they exercised due diligence to ensure obscene content is not displayed on their website.

IMPLEMENTATION OF CYBER LAW

Since the beginning of civilization, there has been tremendous need for the progress of existing technologies. As a result, various developments and progress took place. One of the most significant advances is the development of internet.

The rapid evolution of internet facilitated e-commerce, e-banking, e-governance, promoted electronic commerce, etc. But it also led to cybercrime and cyber terrorism. The countries throughout the world are adopting different approaches towards regulating and facilitating electronic communication and commerce.

The Parliament of India passed its first ever cyber law, the Information Technology Act, 2000 with a primary motive to deal with cybercrime and e-commerce. It is based on the *United Nations Model Law on Electronic Commerce 1996* (UNCITRAL Model) which

was recommended by the General Assembly of United Nations by a resolution on 30 January 1997 [15].

The object of the Information Technology Act, 2000 is to provide legal recognition for digital transactions carried out by means of electronic communication also referred to as "electronic commerce", which involve the use of alternative methods to paper-based methods of communication and storage of information and to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith.

Jurisdiction

Section 1(2) of the Information Technology Act, 2000 provides:

"It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person."

Section 75 of the IT Act, 2000 states:

1. "Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
2. For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India."

The legislative function of the Government is to enact laws and administrative function to enact those laws. The principles of jurisdiction followed by a State must not exceed the limits which international law places upon its jurisdiction.

- Chapter I of the Act stipulates the application and jurisdiction. It also defines various terms which are used in the act repetitively.
- Chapter II of the Act specifically provides that any subscriber may authenticate an electronic record by affixing his digital signature. It further mentions that any person by the use of a public key of the subscriber can verify the electronic record.
- Chapter III of the Act stipulates electronic governance. It gives legal recognition to electronic records and digital signatures.

Section 4 of the IT Act, 2000 states:

"Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

a. Rendered or made available in an electronic form; and
b. Accessible so as to be usable for an ulterior reference."

The said chapter also details the use of electronic records and digital signatures in Government and its agencies. It also provides for the power of the Central Government to makes rules in respect of digital signature.

- Chapter IV manages attribution, acknowledgment and dispatch of electronic records. An electronic record is credited to the originator if it was sent by the originator himself, or, by a person on behalf of the originator, or, by an information system programmed by or on behalf of the originator. Its further details about the acknowledgment of receipt and time and place of dispatch and receipt of electronic record.
- Chapter V stipulates secure electronic records and secure digital signature. Its further states that the Central Government shall prescribe the security procedure having regard to commercial circumstances.
- Chapter VI specifically stipulates the regulation of certifying authorities. It details out the appointment of controller and other officers and functions of controller. It states that the Controller shall be the repository of all Digital Signature Certificates issued under this Act. Any individual can make an application, to the Controller, for a license to issue Digital Signature Certificates. It also provides for

application for license, renewal of license, procedure for grant or rejection of license and suspension of license. The controller shall also have the power to delegate and investigate.

- Chapter VII of the Act details about the scheme of things relating to Digital Signature Certificates such as power of Certifying Authority to issue Digital Signature Certificate, suspension and revocation of digital signature certificate.
- Chapter VIII enshrines the duties of subscribers.
- Chapter IX talks about penalties and adjudication for various offences including the penalty for damage to computer systems have been fixed as damages by way of compensation not exceeding one crore rupees to the person so affected. The penalty for failure to furnish information shall be liable for a penalty not exceeding one lakh and fifty thousand rupees for each such failure and for a successive offence, not exceeding five thousand rupees for every day during which such failure continues.
- Chapter X of the Act states that the Cyber Regulations Appellate Tribunal frames an appellate body where appeals against the orders passed by the Adjudicating Officers shall be preferred. The said Tribunal should not be bound by the principles of the Code of Civil Procedure but shall follow the principles of natural justice and shall have the same powers as that of the Civil Court. An appeal shall lie in the High Court against a decision of the Cyber Appellate Tribunal.
- Chapter XI deals with various offences such as tampering with computer source documents, hacking with computer system and publishing of information which is obscene in electronic form. The said offences should be investigated only by an officer not below the rank of the Deputy Superintendent of Police.

LOOPHOLES IN THE INFORMATION TECHNOLOGY ACT

Hurried Legislation

Experts have opined that the hurry in which act was brought in, without any public debate, has not only frustrated the ultimate purpose of bringing in the act but has also adversely affected the adequacy of the legislation. The Government has tried to amend a lot of problems by the way of amended act of 2008 [16].

Uniform Law

It has always been the common opinion that a uniform law is required to curb the menace of cyber crime which is itself a global issue. It is advisable that the wrong and it's the cure must come from same level [17].

Lack of Awareness

The Act of 2000 failed because of the lack of awareness among of people about the cyber space and its set back. Since most of the cases went on being unreported the law failed to act in its full capacity.

Raising a Cyber Army

Like every agency needs proper framework and mechanism to function so it is required by the cyber law. The cyber law lacks just not a proper framework task force to deal with the new trends of technical crime but also the teeth to punish the offender. The government has taken few positive steps in this direction and the establishment of the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI) to deal with cyber offences and punish the offender.

Cyber Savvy Bench

Judiciary had always played a prominent role in filing the gaps between the law and its enactment and so Cyber savvy judges are the most needed for dealing these types of cases.

Hesitation to Report Offences

The thing that has most fatally affected the successful application of the act is the unreported cases. One obvious reason is the non-cooperative police force. The police are becoming a powerful force today which plays an important role in preventing cybercrime. Simultaneously, it can also end up in harassing innocents and preventing them from going about their normal cyber business. A cooperative police force is the most important factor for proper application of the provisions of this Act [18].

Apart from these loopholes and problem, the inadequacy and lack of knowledge among the policemen to deal with cybercrime has always been a point of debate and it is always realized that they need adequate training to be familiar with the "Modus operandi" of cybercrimes. The existing relevant act is though the comprehensive legislation in itself, but it lacks the practicality to some extent. It is the need of the hour that the efficiency of police system at all ranks should be upgraded in terms of cybercrimes because the inefficient police system allows the immoral, lethal mind criminals to take advantage of this.

Both bench and Bar should realize the gravity of the nature of cyber offences. They should familiarize themselves with the intricacies of cyber law, else it would be very difficult for them to serve justice in the cases related to cyber.

MEASURES

These measures can be thought about as suggestions also:

- No credit card details should be shared by an individual to any unsecured site, to protect against frauds.
- One should avoid revealing any personal data to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers online as misuse of photograph incidents has been increasing day by day.
- It is always recommended that the parents must keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site for preventing cybercrimes as number of internet users are growing day by day.
- Strict statutory laws should to be passed by the Legislatures keeping in mind the interest of netizens (cybercitizen or an entity or person actively involved in online communities or a user of the Internet).
- Web servers running public sites must be physically separately protected against internal corporate network.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and they should also keep additional duplicate back up volumes so that one may not suffer data loss in case of any virus contamination.
- It is best to use a security program by the body corporate to regulate data on sites.
- The information Technology department should pass certain guidelines for the protection of computer network system and should additionally bring out some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is one of the biggest threats to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime. This means a uniform law should be created to deal with the cybercrimes world-wide.
- Special police task force which is expert in technical field should be constituted.
- Justice should be provided to the victims of cybercrimes by way of compensatory remedy and offenders must be punished with highest sort of punishment in order that it will anticipate the criminals of cybercrime [19].

CONCLUSION

Technological advancement has become the predecessor of such change in the 21st Century where the information sector is taking the leading step towards the comfort, luxury and communication. In the current era of internet, maximum of the critical information's details is processed online which prone to cyber threats. With the numerous advancement of the internet the crime owing to internet has also widened its route in all directions. Cyber space offers excess of opportunity for Cyber offenders to cause harm to the innocent people. Crimes are as old as men himself and computer crimes are as old as computer themselves. The women find themselves particularly vulnerable in the increasing Cyber Crime become prey of Cyber bullying and cyber pornography. All the hate materials that a culprit puts online disgrace and enrage a victim's family. Operative and dynamic law enforcement can help deter Internet pornography and diminish the supply of inappropriate sexually explicit material

available to children. For concrete and practical reasons, it is most feasible to seek regulation of commercial sources of such material. Internet safety education can be compared parallel to the safety education in the physical world. The solution to make children less inclined to spend their time searching for inappropriate material or engaging in unsafe activities is the promotion of more compelling, safe, and educational Internet content that is developmentally appropriate.

REFERENCES

1. Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18
2. The United Nations Manual on the Prevention and Control of Computer Related Crime
3. https://itstillworks.com/causes-cyber-crime-1846.html
4. IBID
5. https://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-12-08-96.pdf
6. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
7. Computer Emergency Response Team. The CERT Coordination Centre was founded in 1988 after the Morris worm incident, which brought 10 per cent of Internet systems to a halt in November 1988. For more information on the history of the CERT CC, see: www.cert.org/meet_cert/; Goodman, Why the Police don't Care about Computer Crime, Harvard Journal of Law and Technology, Vol. 10, Issue 3, page 475.
8. Regarding the offences recognized in relation to online games, see above: § 2.6.5.
9. Giordano, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; Willinger/Wilson, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.
10. Regarding the use of ICTs by terrorist groups, see: Conway, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16; Hutchinson, "Information terrorism: networked influence", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf; Gercke, Cyberterrorism, Computer Law Review International 2007, page 64.
11. https://www.ijera.com/papers/Vol2_issue2/AG22202209.pdf
12. CS(OS) No. 1279/2001, Delhi High Court
13. MANU/SC/0465/2005
14. Case No.1739/2012 T.R.No.21/2013
15. CRL.M.C. 3066 of 2006
16. B.M. Gandhi, Indian Penal Code, India: Eastern Book Company, p. 41. ISBN9788170128922.
17. Parthasarati Pati, 'Cyber Crime' http://www.naavi.org/pati/pati_cybercrimes_dec03.htm accessed on 6 December 2017
18. Kumar Vinod, 'Winning the Battle against cyber Crimes' http://www.cyberriskinsuranceforum.com/content/are-we-losing-battle-against-cyber-crime accessed on 30 November 2017
19. Dewang Mehta, 'Role of Police in Tackling Cyber Crimes' http://www.naavi.org/pati/pati_cybercrimes_dec03.htm accessed on 30 November 2017

Cite this Article

Priya Jha, Purvai Kaprate. A Grey Area in the Bright Future of Cyber Law: Cyber Pornography and Cyber Crime. *National Journal of Cyber Security Law*. 2020; 3(2): 1–11p.