HOW TO REPORT CYBER CRIMES IN INDIAN TERRITORY

Ompal[1], Tarun Pandey[1], Bashir Alam[2]

[1]Ministry of Electronics & Information Technology, Government of India (India)

[2]DepartmenofComputer Engineering, Faculty of Engineering & Technology,
Jamia Millia Islami New Delhi (India)

ABSTRACT

Initially Internet was the tool for sharing the information related to the research and development. In the present day world, communication over the Internet, interaction through social media over Internet, online purchasing, online banking, online bill payment etc. are becoming the necessities for among of us. Now, physical crime world has been shifted towards to cyber crime world. As with use of the Internet, cyber crimes are increasing day by day, hence there is a strong need to make the appropriate cyber laws to deal with these cyber crimes. In this paper, types of cyber crimes, Cyber Crime Preventive Measures, Mechanism to Report Cyber Crimes and Right Path for Sending the Blocking, Removal Request for Objectionable Content which is available over cyber space are discussed under the IT Act 2000 of Indian Government.

Keywords: Cyber Crime, Cyber Law, Online Fraud, Phishing, Hacking, IT Act, Copy Right Infringement

I. INTRODUCTION

Due to exponential growth of Internet and thereby online/mobile banking and such other related technologies, present world is being benefited by the use of these technologies. In each segment like banking, airport, space, railway, telecommunication and social media today's world is fully dependent on the technology and all these technologies are interlinked with one another through Internet. Each innovation or new technology facilitates a lot of advantages but same time it may produces the side effects. In the present day world is fully dependent on Internet via social media, banking transaction, mobile transactions etc.

As we know Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. Despite technological measures being adopted by corporate organizations and individuals, we have witnessed that due to the advancement of knowledge of individuals in field of cyber space, the frequency of cyber crimes has increased over the last decade.

The term cyber crime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction [4]. Other words represents the cyber crime as ―Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data[25].

Cyber crime is a fast-growing area of crime. More and more criminals are exploiting the speed convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

Cyber crime could include any monetary offences as financial frauds as well as non-monetary offences, such as cyber bullying, creating and distributing small or large programs written by programmers called viruses on other computers or posting confidential business information on the Internet [1, 2, 3, 5, 6 and 7].

Disclaimer: "All content presented in this paper is personnel view of authors. This content cannot be treated as an official view of the authors."

For our civilised society, there is a strong need to take the necessary steps to prevent such cyber crimes. There are many bodies are working all over the world. In India, CERT-IN (Indian Computer Emergency Response Team), Department of Electronics and Information Technology, Ministry of Communication & Information Technology issues advisories for preventing the cyber crimes on regular basis.

If anyone fails to comply with the issued advisories and after the victimisation of cyber crimes, he/she has to report the cyber crime to the right agency, so that timely action against the cyber criminals may be taken. To report the social abuse and cyber crimes, there are definite guidelines and paths for reporting the cyber crime or cyber abuse in India. In this paper, types of cyber crimes, Cyber Crime Preventive Measures, Mechanism to Report Cyber Crimes and Right Path for Sending the Blocking, Removal Request for Objectionable Content are discussed.

The paper is organised as follows- in section 2 the details of different kind of cyber crimes is given. In section 3, the detail some sections of Information Technology Act 2000 is given. In section 4 preventive measures of cyber crimes, in section 5 post steps of cyber crimes, in section 6 detail of section 69A and roles and responsibilities under 79 of IT Act 2000 are given. Conclusion of the paper is given in section 7 and in last references is given.

II. TYPES OF CYBER CRIMES

2.1 Cyber-Stalking

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to Web site or a discussion group. A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected.

2.2 Cyber Defamation

Cyber defamation is not a specific criminal offence, misdemeanour or tort, but rather defamation or slander conducted via digital media, usually through the Internet.Penalties for 'Cyber defamation' vary from country to country, but the fundamental rights covered in the UN Declaration of Human Rights and European Union Fundamental Human Rights.

2.3 Hacking

Hacking is the gaining of access (wanted or unwanted) to a computer and viewing, copying, or creating data (leaving a trace) without the intention of destroying data or maliciously harming the computer.   Hacker - Person who gains authorized/unauthorized access to a computer without the intention of causing damage

2.4 Cracking

Cracking is the method by which a person who gains unauthorized access to a computer with the intention of causing damage. Cracker - Person who gains unauthorized access to a computer with the intention of causing damage.

2.5 E-Mail Spoofing

Email spoofing is the creation of email messages with a forged sender address. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations.

2.6 SMS Spoofing

SMS spoofing is a relatively new technology which uses the short message service (SMS), available on most mobile phones and personal digital assistants, to set who the message appears to come from by replacing the originating mobile number (Sender ID) with alphanumeric text. Spoofing has both legitimate uses (setting the company name from which the message is being sent, setting your own mobile number, or a product name) and illegitimate uses (such as impersonating another person, company, and product).

2.7 Carding

A form of credit card fraud in which a stolen credit card is used to charge pre-paid cards. Carding typically involves the holder of the stolen card purchasing store-branded gift cards, which can then be sold to others or used to purchase other goods that can be sold for cash. Credit card thieves who are involved in this type of fraud are called carders.

2.8 Bot Networks

A botnet is a collection of compromised computers often referred to as “zombies” infected with malware that allows an attacker to control them.

2.9 Intellectual Property Crimes

Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc.   A copyright is the legal right of an author, publisher, composer, or other person who creates a work.

2.10 Cyber Squatting

Cyber squatting (also known as domain squatting), according to the United States federal law known as the anti-cyber squatting Consumer Protection Act, is registering, trafficking in, or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. The cyber squatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price [16].

2.11 Cyber Vandalism

Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.

2.12 Cyber Trespass

The word “trespass” in general means to enter into the other’s property without seeking consent. It is considered a civil wrong ordinarily. If the trespass is committed with criminal intention it is called criminal trespass. The concept of trespass is applicable in cases of the cyber world and may be termed as Cyber Trespass [17].

2.13 Internet Time Thefts

Internet time theft comes under the heading of hacking. It is the use by an unauthorized person of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.

2.14 Online Gambling

Internet gambling business means “the business of placing, receiving or otherwise knowingly transmitting a bet or wager by any means which involves the use, at least in part, of the Internet, but does not include the performance of the customary activities of a financial transaction provider, or any interactive computer service or telecommunications service [18].

2.15 Fraud and financial crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes.
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect.
- Altering or deleting stored data.

2.16 Cyber extortion

Cyber extortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cyber extortionists are increasingly attacking corporate websites and networks, crippling their -bility to operate and demanding payments to restore their service. [19]

2.17 Transmitting Virus

Computer viruses usually spread in one of three ways: from removable media; from downloads off the Internet; and from e-mail attachments.

2.18 Phishing

Phishing schemes are one of the chief ways in which people end up with their identity stolen and a computer fill of viruses. A phishing scheme starts when you receive an email from a website claiming to be your bank or Credit Card Company. Many times, when you visit these sites, spyware, adware and viruses are automatically installed on your. [20]

2.19 Cross-site Scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

2.20 Credit/Debit Card Fraud

Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

2.21 Identity Theft

Identity theft happens when fraudsters access enough information about someone’s identity (such as their name, date of birth, current or previous addresses) to commit identity fraud. Identity theft can take place whether the fraud victim is alive or deceased [15, 21].

2.22 Cyber Bullying

The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature [1].

2.23 Unwanted exposure to sexually explicit material etc.

More research concerning the potential impact of Internet pornography on youth is warranted, given the high rate of exposure, the fact that much exposure is unwanted and the fact that youth with certain vulnerabilities, such as depression, interpersonal victimization, and delinquent tendencies, have more exposure.

2.24 Spam

Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.

2.25 Cyber terrorism

Cyber terrorism is the act of Internet terrorism in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses [22].

2.26 Harassment via E-Mails

Email harassment is usually understood to be a form of stalking in which one or more people send consistent, unwanted, and often threatening electronic messages to someone else. There isn’t always an exact definition of what a message has to look or sound like in order to be harassing. It’s usually a matter of circumstance, since what one person finds offensive or harmful may not actually come off that way to someone else[23].

2.27 Distribution of pirated software

Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries [24].

2.28 Child Pornography

Child Pornography is a criminal offence and is defined as any visual depiction involving the use of a minor, or one appearing to be a minor, engaging in sexually explicit conduct.Since technology moves much faster than legislation, crimes committed via social media are often prosecuted by applying existing statutes. Child pornography is any visual depiction of sexually explicit conduct involving a minor.

III. INFORMATION TECHNOLOGY ACT 2000

IT Act 2000 is an Act of the Indian Parliament (No 21 of 2000) notified on October 17, 2000 to have its exhaustive law to deal with the technology in the field of information technology including e-commerce, e-governance, e-banking etc as well as penalties and punishments in the field of cyber crimes[8].

3.1 Penalties, Compensation and Adjudication

Sec.43 If any person without permission of the owner damages to computer, computer system, etc. he/she shall be liable to pay compensation to the person so affected.

Sec.43A Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, in negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Sec.45 Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Sec.66 If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Sec.66B Punishment for dishonestly receiving stolen computer resource or communication device is Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Sec.66C Punishment for identity theft— Whoever, fraudulently make use of electronic signature or password, shall be liable for imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Sec.66E Punishment for violation of privacy- Whosoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Sec.66F Cyber terrorism Imprisonment which may extend to imprisonment for life.

Sec.67 Punishment for publishing or transmitting obscene material in electronic form.—Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Sec.67A Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.—Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Sec.67B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form- Abusing children online, imprisonment for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Sec.67C Preservation and retention of information by intermediaries.—(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribed. (2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Sec.72 Penalty for 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 thereunder, 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.

Sec. 75 Act to apply for offences or contravention committed outside India.—(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.

IV. PREVENTIVE MEASURES TO DEAL WITH CYBER CRIME

CERT-IN (Indian Computer Emergency Response Team), Department of Electronics and Information Technology, Ministry of Communication & Information Technology issues advisories on regular basis for common users on Desktop Security, Mobile Phone Security, Broadband Internet Security, USB Devices Security, Secure uses of Debit/Credit Card and preventing phishing attacks which are disseminated through portals like “secureyourepc.in”, www.secureyoureelectronics.in and www.cert-in.org.in. To create awareness about such frauds by using emails and SMS, advisories are being issued by banks and telecom service providers which may be referred to [12, 13, 14].

V. POST STEPS OF CYBER CRIMES

5.1 Reporting of the Various Kind of Cyber Crimes

After victimization of any cyber crime, first step is to report the crime to the Law enforcement agency (Cyber crime branch or any police station of your state.). Matters of cyber crimes are investigated by law enforcement agency (LEA) on registration of FIR. Further LEA approaches to Indian Computer Emergency Response Team (CERT-In) for getting the information related to technical analysis like details of emails, sms, Facebook, Twitter, IP address, URLs details etc. In addition of getting information related to technical analysis from CERT-In (Definition and functions of CERT-In are given in section 5.3 of this research paper).

Assam CID HQ,Dy.SP (Assam Police) Ph: +91-361-252-618 / +91-9435045242 **E-mail id**: ssp_cod@assampolice.com	**Bangalore (for whole of the Karnataka)** Cyber Crime Police Station C.O.D Headquarters, Carlton House, # 1, Palace Road, Bangalore - 560 001 Ph.+91-80-2220 1026 +91-80-2294 3050 +91-80-2238 7611 (FAX) **Website**: http://www.cyberpolicebangalore.nic.in/ **Email-id:** ccps@blr.vsnl.net.in, ccps@kar.nic.in
Pune Deputy Commissioner of Police(Crime) Office of the Commissioner Office, 2, Sadhu Vaswani Road, Camp, Pune 411001 Ph. +91-20-26123346 / +91-20-26127277 +91-20-2616 5396 +91-20-2612 8105 (Fax) **Website:** www.punepolice.gov.in **E-mail id:** crimecomp.pune@nic.in, punepolice@vsnl.com	**Delhi** CBI Cyber Crime Cell: Superintendent of Police, Cyber Crime Investigation Cell Central Bureau of Investigation, 5th Floor, Block No.3, CGO Complex, Lodhi Road, New Delhi – 3 Ph. +91-11-4362203, 011-26851998 011-26515229, +91-11-4392424 **Website**: http://cbi.nic.in/ Asst. Commissioner of Police, Cyber Crime Cell,EOW, Crime Branch, 2nd Floor, Police Training School, Malaviya Nagar, New Delhi-110017 **Email-id:** cbiccic@bol.net.in,dcp-eow-dl@nic.in
Punjab Cyber Crime Police Station DSP Cyber Crime, S.A.S Nagar,Patiala,Punjab Ph: +91 172 2748 100	**Kerala** Hitech Cell Police Head Quarters Thiruvananthapuram Ph: +91-471 272 1547 / +91-471 272 2768 **E-mail id:** hitechcell@keralapolice.gov.in
Himachal Pradesh	**West Bengal**

CID Office , Dy.SP Himachal Pradesh Ph: +91-94180 39449 **E-mail id:** soodbrijesh9@gmail.com	CID, Cyber Crime West Bengal Ph: +9133 24506163 **E-mail id:** occyber@cidwestbengal.gov.in
Jharkhand IG-CID,Organized Crime Rajarani Building, Doranda Ranchi,834002 Ph: +91-651-2400 737/ 738 **E-mailid:**a.gupta@jharkhandpolice.gov.in	**Haryana** Cyber Crime and Technical Investigation Cell, Joint Commisioner of Police Old S.P.Office complex,Civil Lines, Gurgaon **E-mail id**: jtcp.ggn@hry.nic.in
Meghalaya SCRB,Superintendent of Police Meghalaya Ph: +91 98630 64997 **E-mail id:** scrb-meg@nic.in	**Jammu** SSP,Crime CPO Complex,Panjtirthi, Jammu-180004 Ph: +91-191-257-8901 **E-mail id:** sspcrmjmu-jk@nic.in
Bihar Cyber Crime Investigation Unit Dy.S.P.Kotwali Police Station, Patna Ph: +91 94318 18398 **E-mail id**: cciu-bih@nic.in	**Uttar Pradesh** Cyber Complaints Redressal Cell, Nodal Officer Cyber cell Agra, Agra Range 7,Kutchery Road, Baluganj,Agra-232001 Uttar Pradesh Ph: +919410837559 **E-mail id:** info@cybercellagra.com
UttaraKhand Special Task Force Office Sub Inspector of Police, Dehradoon Ph: +91 135 2640982/ +91 94123 70272 **E-mail id**: dgc-police-us@nic.in	**Hyderabad** Cyber Crime Police Station Crime Investigation Department, 3rd Floor, D.G.P. office Lakdikapool, Hyderabad – 500004 +91-40-2324 0663 / +91-40-2785 2274 /+91-40-2785 2040 +91-40-2329 7474 (Fax)

	Website: http://www.cidap.gov.in/cybercrimes.aspx **E-mail id:** cidap@cidap.gov.in, info@cidap.gov.in cybercell_hyd@hyd.appolice.gov.in
Chennai Asst. Commr. of Police, Cyber Crimes Cell, Vepery, Chennai 7 Ph: 04423452348/04423452350 **E-mail id:** cybercrimechn@yahoo.com **For Rest of Tamil Nadu,** A-Wing, III rd Floor, Rajaji Bhawan, Besant Nagar, Chennai-600090 Ph: 044-24461959/24468889/24463888 **E-mail id:** hobeochn@cbi.gov.in	**Thane** 3rd Floor, Police Commissioner Office Near Court Naka,Thane West, Thane 400601. Ph: +91-22-25424444 **Website:** www.thanepolice.org **E-mail id:** police@thanepolice.org
Orissa Cyber Crime Police Station, CID, CB, Odisha, Cuttack-753001 Ph. 0671-2305485 **E-mail id**: sp1cidcb.orpol@nic.in	**Gujarat** DIG, CID, Crime and Railways Fifth Floor Police Bhavan Sector 18, Gandhinagar 382 018 +91-79-2325 4384 / +91-79-2325 0798 +91-79-2325 3917 (Fax)

VI. INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-IN)

CERT In is the national nodal agency for responding to computer security incidents as and when they occur. As per the Information Technology Amendment Act 2008 and Section 70B of IT Act 2000, CERTIn has been designated to serve as the national agency to perform the following functions in the area of cyber security: Collection, analysis and dissemination of information on cyber incidents, Forecast and alerts of cyber security incidents, Emergency measures for handling cyber security incidents, Coordination of cyber incident response activities.Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.Such other functions relating to cyber security as may be prescribed.

6.1 What can be reported to CERT-In?

6.1.1 Users and System Administrators can report computer security incidents and vulnerabilities to CERT-In. If you encounter any of the violations given below, you may contact CERT-In for technical assistance

- Attempts (either failed or successful) to gain unauthorised access to a system or data therein
- Disruption or denial of service

- Unauthorised use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without owner's knowledge, instruction, or consent
- Email related security issues, spamming, mail bombing etc.

6.2.2 Users of different systems working on various platforms and using different applications may report any vulnerability found in these systems, platforms, applications, services and devices to CERT-In.

6.2 How to report incidents to CERT-In?

You can report an incident to CERTIn by filling up the form on our website, electronic mail, telephone hotline or by Fax.

6.2.1 Through Website :

The incident can be reported by filling up incident reporting form CERTIn website. Fill in as many of the fields as possible to enable us to assess the severity and nature of the incident and assist in recovery, as needed.

6.2.2 Through Electronic Mail:

The CERT-In email address for reporting incidents is “incident@cert-in.org.in”. For all other inquiries and correspondence, write to “info @cert-in.org.in”.

6.2.3 Through Telephone and Fax:

Contact CERT-In on +91-11-24368572.

Incident report can be faxed to CERT-In at +91-11-24368546

6.2.4 Postal Address:

Indian Computer Emergency Response Team (CERTIn), Ministry of Electronics and Information Technology , Government of India, Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi 110003, India.

6.3 How to report a vulnerability to CERTIn?

Vulnerability can be reported to CERT-In by filling up the Vulnerability Reporting Form provided on its website. The information about a particular vulnerability can also be sent to CERT-In by Fax or by following email “vulnerability@cert-in.org.in”.

6.4 Appropriate Path for Reporting the Crime under Section 69A and Section 79(3) (b)

6.4.1 Section 69A Power to issue directions for blocking public access of any information through any computer resource.—

- Where the Central Government or any of its officer’s specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing by order, direct any agency of the Government or intermediary to block for access by the public any information generated, transmitted, received or stored in any computer resource.
- The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.
- The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

6.4.1.1 Appropriate Path for Sending Blocking Request under section 69A

Ministry of Electronics & Information Technology (MeitY), Government of India invokes Section 69A of Information Technology Act 2000 to block websites / URLs with objectionable contents, whenever such requests are received from any organization through their nodal officer in prescribed format (form 6(2) of (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 of IT act 2000) Court order. The rules for blocking of information for public access namely "Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009", were notified under section 69A of the Information Technology Act, 2000 on 27th Oct. 2009 [9,10].

6.4.2 Intermediary

Section 2(1) (w) of the amended Information Technology Act, 2000 states as follows:"Intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes."

Section 79 of the amended Information Technology Act, 2000: Once the Government becomes an "intermediary", its liability for third party data or information is specifically stipulated under Section 79 of the amended Information Technology Act, 2000. Section 79 of the amended Information Technology Act, 2000 states as follows:-

"Section -79 Exemption from liability of intermediary in certain cases.Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or hosted

(b) The intermediary doesn't- (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission

(c) The intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if-

(a) The intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act.

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner." Explanation- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary" [11].

6.4.3 Some useful links to report objectionable content to Social Media intermediaries like Facebook, Twitter etc.

Every intermediary has its own policy to judge the content. Any one may report the objectionable content to intermediary as per their policies and guidelines directly. Here some e-mail ids and link for reporting the objectionable contents are given below.

Facebook: https://www.facebook.com/policies/?ref=pf https://www.facebook.com/about/privacy Ms. Ankhi Das, Facebook India, Public Policy Director Building No. 14, Raheja Mindspace, Hi Tech City, Main Road, Vittal Rao Nagar, Hyderabad, Andhra Pradesh, India **E-mail id:** records@fb.com,ankhi@fb.com and jwu@fb.com	**Microsoft Corporation (I) Pvt. Ltd.** Ms. Madhu Khatri Associate General Counsel, Microsoft Corporation India Pvt. Ltd. 10th Floor, Tower B & C,DLF Building No.5 (Epitome), Cyber City, DLF Phase III, Gurgaon, 122002 Fax: 91-124-4158888 Dial toll-free: 1800 102 1100 or 1800 111 100 **E-mail id:** Meenu.Chandra@microsoft.com
Apple India Pvt Ltd. 19th floor, Concorde Tower C, UB City, No. 24, Vittal Mallya Road, Bangalore 0560001 India **E-mail id**: khanafer@apple.com, bangalore_admin@apple.com	**Yahoo India** Mr Robin Fernandes, Sr.Executive Compliance Building 12, 6th Floor, Solitaire Corporate Park, Guru Hargovindji Marg, Andheri (E), Mumbai 400 093 Tel: + 91 22 3308 9600 ,+ 912233089652 Mobile: +91 8452049536 Fax: +91 22 3308 9700 **E-mail id**: robinfe@yahoo-inc.com
Twitter https://support.twitter.com/articles/80586 E-mail id: grievance-officer-in@twitter.com ; support@twitter.com	**YouTube and Google India Pvt. Ltd.** https://www.youtube.com/t/contact_us https://support.google.com/youtube/topic/2803240?hl=en&rd=1 Ms. Gitanjli Duggal, Legal Director, DLF Cyber City, Tower 8C. 9th floor, Gurgaon – 122002. **E-mail id**:support-in@google.com; gitanjli@google.com

6.5 Suggestive Solution for Pornography Content:

Individual grievances related to pornography are not covered under 69A of IT Act 2000. For these types of crimes, any one may approach to LEA for registration of FIR and LEA may issue the appropriate directions for intermediary in this regards. Alternatively any one may also approach to a competent court in India (who can direct DoT/ISPs to block access of these URLs) for redress the matter.

6.6 Technical Challenges in Blocking of Objectionable Content with https header:

At ISP level, only URLs containing non-encrypted header (http) may be blocked. If any URL is encrypted (https) then it is technically infeasible for ISPs to determine the exact URL from incoming encrypted traffic. Since HTTPS mechanism is being used for accessing the web services, it may not be feasible to block the URL pages for specific region only, as encrypted communication is involved at the ISP level. In case of mobile apps, it may not be possible to block the communication from Apps, as mobile apps are available in Play Store which can be downloaded freely by the users for using the services. Since the Apps may be using encryption during communication with the websites, Intermediaries like Google, Apple etc to be approached for removing such apps from the respective play store

VII.CONCLUSION

It has been witnessed that due to the advancement of knowledge of individuals in field of cyber space, the frequency of cyber crimes has increased over the last decade and it is on continuation on rise. In this paper, different kind of cyber crimes like monetary offences as financial frauds as well as non-monetary offences, such as cyber bullying, creating are discussed and it is felt that for our civilised society, there is a strong need to take the necessary steps to prevent such cyber crimes. Various preventive measures have been discussed and right path to report the cyber crime to the right agency is also discussed. To report the social abuse and cyber crimes, there are definite guidelines and paths for reporting the cyber crime for each intermediary as per their policies. Anyone can report the cyber crimes to intermediary as per their policies. Proper mechanism to report the Cyber Crimes and Right Path for Sending the Blocking, Removal Request for Objectionable Content under section 69A and 79(3)(b) are also discussed. At last some general frequently ask questions with suitable answers are also discussed. As per various sections of this paper, government agencies as well as individuals may plan their strategies to prevent, report the cyber crimes and can take the necessary actions efficiently. As per the alarm of the cyber crimes, it is felt that there should be a proper registration of the cyber world participant and there is a strong need of the establishment of the proper regulatory body to monitor such cyber threat.

REFERENCES

[1] Richard Donegan, “Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis”, The Elon Journal of Undergraduate Research in Communications • Vol. 3, No. 1 • Spring 2012.

[2] http://www.rmlnlu.ac.in/webj/sedition.pdf

[3] Harpreet Singh Dalla, Ms. Geeta, “Cyber Crime – A Threat to Persons, Property,Government and Societies”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[4] Hemraj Saini, Yerra Shankar Rao, T.C.Panda, “Cyber-Crimes and their Impacts: A Review”, International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 2, Mar-Apr 2012.

[5] Vineet Kandpal and **R. K. Singh, "Latest Face of Cybercrime and Its Prevention In India", International Journal of Basic and Applied Sciences Vol. 2. No. 4. 2013.

[6] Anand Kumar Shrivastav, Dr. Ekata, " ICT Penetration and Cybercrime in India: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013

[7] Saroj Mehta & Vikram Singh, "STUDY OF AWARENESS ABOUT CYBERLAWS IN THE INDIAN SOCIETY", International Journal of Computing and Business Research (IJCBR) Volume 4 Issue 1 January 2013

[8] PARDEEP MITTAL, AMANDEEP SINGH, "A Study of Cyber Crimes & Cyber Laws In India", Scholarly Research Journal for Interdisciplinary Studies, ISSN- 2278-8808, JULY- AUGUST 2013, Vol. – I, Issue-I.

[9] http://www.deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/itbill2000.pdf

[10] http://www.deity.gov.in/content/view-it-act-2000

[11] http://cis-india.org/internet-governance/resources/information-technology-procedure-and-safeguards-for-blocking-for-access-of-information-by-public-rules-2009

[12] http://infosecawareness.in/cyber-crime-cells-in-india

[13] www.cert-in.org.in

[14] http://searchsecurity.techtarget.com

[15] https://en.wikipedia.org/

[16] http://www.bizandlegis.com/articles/cyber-trespass/

[17] http://definitions.uslegal.com/i/internet-gambling-business/

[18] https://en.wikipedia.org/wiki/Cybercrime

[19] http://noorhome.blogspot.in/2009/09/11-ways-computer-viruses-are-spread.html

[20] http://www.actionfraud.police.uk/fraud_protection/identity_fraud

[21] https://en.wikipedia.org/wiki/Cyberterrorism

[22] http://www.wisegeek.org/what-is-email-harassment.htm

[23] http://whatis.techtarget.com/definition/piracy

[24] Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.html