Charge/Penalties Against Hacking in INDIA

CYBER CRIME AND ITS TYPE

Computer crime, or cybercrime, refers to any crime that involves a computer and a network The computer may have been used in the commission of a crime, or it may be the target. Net crime refers to criminal exploitation of the Internet. Such crimes may threaten a nation's security and financial health. Issues surrounding this type of crime have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation-state is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

Topology

Computer crime encompasses a broad range of activities. Generally, however, it may be divided into two categories: (1) crimes that target computers and directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device. Crimes that primarily target computer networks or devices include:

Computer • viruses
• Denial-of-service attacks
Malware • (malicious code)

Crimes that use computer networks or devices to advance other ends include:

Cyber • stalking
Fraud • and identity theft
• Information warfare
Phishing • scams

Spam, or the unsolicited sending of bulk email for commercial purposes, is unlawful in some jurisdictions. While anti-spam laws are relatively new, limits on unsolicited electronic communications have existed for some time. 33 *Fraud* 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 • computer input in an unauthorized way. This requires little technical expertise and is not an uncommon 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;
Altering • or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes.

Other forms of fraud may be facilitated using computer systems, including bank fraud, identity theft, extortion, and theft of classified information. A variety of Internet scams target consumers direct. *Obscene or Offensive Content* The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal. Over 25 jurisdictions place limits on certain speech and ban racist, blasphemous, politically subversive, libelous or slanderous, seditious, or inflammatory material that tends to incite hate crimes. The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs. One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography. *Harassment* Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested. Any comment that may be found derogatory or offensive is considered harassment. *Drug Trafficking* Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away. *Cyber Terrorism* Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyber terrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them. Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered 34 cyber terrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc. Cyber extortion is a form of cyber terrorism in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks. According to the

Federal Bureau of Investigation, cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the domain. Perpetrators typically use a distributed denial-of-service attack. *Cyber Warfare*

The U.S. Department of Defense (DoD) notes that cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included the attack on Estonia's

infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of

Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.

IT ACT OF INDIA 2000

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. Some highlights of the Act are listed below: Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber. Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that 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 rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference. The said chapter also details the legal recognition of Digital Signatures. Chapter-IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the

need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates. Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act. Chapter-IX of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court. Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred. 35 Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking. The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend

the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records. In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature. From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law. Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act. Digital signatures have been given legal validity and sanction in the Act. The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates. The Act now allows Government

to issue notification on the web thus heralding e-governance. The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government. The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date. Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

SECTIONS UNDER CYBERLAWS AND PENALTIES UNDER THEM

Information Technology (Amendment) Act 2008

Information Technology (Amendment) Act 2008 has been notified and enforced on 27th Oct, 2009. This Act punishes various cyber crimes including Cyber Terrorism. Important Sections Related to Cyber Crimes

65. Tampering with Computer Source Documents Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programmed, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. ***Explanation:*** For the purposes of this section, "Computer Source Code" means the listing of programmer, Computer Commands, Design and layout and programmed analysis of computer resource in any form. **Sec 66. Computer Related Offences** 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. ***Explanation:*** For the purpose of this section,-

(a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;
(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

66 A Punishment for Sending Offensive Messages through Communication Service, etc Any person who sends, by means of a computer resource or a communication device,- any information that is grossly offensive or has menacing character; or 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, 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 purposes 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, image, audio, video and any other electronic record, which may be transmitted with the message. **66 B. Punishment for dishonestly receiving stolen computer resource or communication device** Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both. **66C Punishment for identity theft** Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh. **66D Punishment for cheating by personation by using computer resource** Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. **66E Punishment for violation of privacy** 37 Whoever, 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 ***Explanation:*** For the purposes of this section--

(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) “publishes” means reproduction in the printed or electronic form and making it available for public;

(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that--

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

66F. Punishment for cyber terrorism

1. Whoever,-

A. with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-
(i) denying or cause the denial of access to any person authorized to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or
(iii) introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or
B. knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.
(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'. **67. Punishment for publishing or transmitting obscene material in electronic form** Whoever publishes or transmits or causes to be published 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.
67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form 38 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. ***Exception:*** This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science,literature,art,or learning or other objects of general concern; or
(ii) which is kept or used bona fide for religious purposes.

67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form Whoever,- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or (d) facilitates abusing children online or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description 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: Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-
(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
(ii) which is kept or used for bonafide heritage or religious purposes Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

67 C. 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 prescribe. (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. **68. Power of Controller to give directions** 39 (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under. (2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both. **Sec 69. Powers to issue directions for interception or monitoring or decryption of any information through any computer resource** (1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it

is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense 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 or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource. (2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed (3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical

assistance to – (a) provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or (b) intercept or monitor or decrypt the information, as the case may be; or (c) provide information stored in computer resource. (4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine. **Sec 69 A Power to issue directions for blocking for public access of any information through any computer resource** (1) Where the Central Government or any of its officer specially authorized 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, defense 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-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource. (2) 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. (3) The intermediary who fails to comply with the direction issued under subsection (4) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine. **Sec 69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security** (1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. (2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating , transmitting, receiving or storing such traffic data or information. 40 (3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed. (4) Any intermediary who intentionally or knowingly contravenes the provisions of

sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine. ***Explanation:*** For the purposes of this section,
(i) "Computer Contaminant" shall have the meaning assigned to it in section 43
(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Sec 70 Protected system (1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. ***Explanation:*** For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety. (2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1) (3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this

section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine. (4) The Central Government shall prescribe the information security practices and procedures for such protected system. **Sec 71 Penalty for misrepresentation** Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, 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 72 Breach of confidentiality and privacy** Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. **Sec 72 A. Punishment for Disclosure of information in breach of lawful contract** Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. **Sec 73. Penalty for publishing electronic Signature Certificate false in certain**

particulars (1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that 41 (a) the Certifying Authority listed in the certificate has not issued it; or (b) the subscriber listed in the certificate has not accepted it; or (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation. (2) Any person who contravenes the provisions of sub-section (1) 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.