CHAPTER- IV

4.0 STATUTES DEALINGS WITH CYBER CRIMES

Every state has a statute deals specifically with computer crime. The first wave of computer crime legislation appeared in the late 1970s, as computers became more widely used in business, legislative activity in the mid 1980s was likely a part, a response to the report of the American Bar Associations Task Force on Computer Crime, which suggested that Computer Crime was likely to increase as technological advances simplified communications between computers and that many lacked appropriate penalties to deter those crimes when congress first enacted the federal Computer Fraud and Abuse Act in 1984, more than 20 states already had some version of a comprehensive computer crime statute. Another group of states adopted computer crime laws in the 1980s or early 1990s as the Internet and declining prices for personal computers made technology more widely available than ever before.

State computer crime laws generally follow one of three models. One model divides computer crime into three categories: Crimes against computer equipment and supplies; crimes against computer users and crimes against computer data. Another model uses "unauthorized access" to a computer as the touch stone for portioning criminal conduct into a variety of categories, such as simple unauthorized access without any resulting damage or loss to the victim; unauthorized access involving destruction, alteration, or theft of data; unauthorized access with intent to commit fraud or obtain money unlawfully, unauthorized access to obtain services; unauthorized access that denies use of the computer to authorized users; and the like. Typically simple unauthorized access is treated as a trivial misdemeanor with light penalties and the other types of unauthorized access are treated as serious misdemeanors or felonies, with the punishment escalating as the dollar amount of the damage or loss escalates. The third model simply lists a number of offenses under an umbrella heading such as "computer crime". Although these general models for computer crime statutes exist, most states have adapted the statutes in their own unique ways.

Most of the basic computer crime statutes that were enacted in the 1980s have been recently updated to reflect technological changes particularly the use of e-mail and the internet to communicate. As a result of the wave of much publicized denial-
of-service ("DOS") attacks on major web sites, computer viruses or worms, and the disruptions caused by "spam" (that is, unsolicited, bulk e-mail) many state statutes have added sections to address these problems. Some statutes have explicitly defined a "computer virus" and created sanctions for creating and deploying them.

A second major category of state computer statutes deals with unlawful interruption of electronic communications or unlawful access to stored computer data. The vast and ever increasing quantities of stored electronic data have made computer databases and communications the target of choice for those seeking to steal credit numbers, personal identifying information or confidential business information. The federal counterparts, which prohibit unlawful interception of electronic communications or access to stored computer data under the federal wire tap statute, those crimes are also often defined under state wiretap statutes.

Some individual states have adopted a wide variety of specific computer crime statutes. For example, several states have enacted criminal statutes prohibiting the unauthorized manipulation of digital signatures, while others have passed statutes criminalizing certain commercial uses of anonymous e-mail.

4.1 DIFFERENT NATIONAL LAWS RESPONSE TO CYBERCRIME

The criminal liability for committing cyber crimes have been established in different national legislations:

4.1.1 (A) The United States of America

The following statutes pertain to cyber-crime in the United States under 18 U.S.C.:

- Section 1029 : Fraud and Related Activity in connection with Access Devices
- Section 1030 : Fraud and Related Activity in connection with computers
- Section 1362 : Communication Lines, Stations, or Systems
- Section 2510 : Wire and Electronic Communications Interception and Interception of Oral Communications
- Section 2512 : Manufacture, Distribution, Possession And Advertising Of Wire, Oral Or Electronic Communication Intercepting Devices Prohibited
- Section 2517 : Authorization for Disclosure and use of Intercepted wire, oral, or Electronic Communications

Section 2520: Recovery of Civil Damages Authorized

Section 2701: Unlawful Access to Store Communications

Section 2702: Voluntary Disclosure of customer Communication or Records

Section 2703: Required Disclosure of Customer Communications or Records

Section 3121: Recording of Dialing Quoting, Addressing, and Signaling Information

Section 3125: Emergency Pen Register and Trap and Trace Device Installation

On October 26, 2001, the USA PATRIOT (Uniting and Strengthening America of Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act was enacted into law. Within the PATRIOT Act of 2001, several laws relating to computer crime and electronic evidence were amended, and the U.S. government is considering more changes under proposals known as PATRIOT Act II.

In 2002, the Homeland Security Act was passed containing Section 225 known as the Cyber Security Enforcement Act of 2002. The following titles, part of the act as a whole, were included (Homeland Security Act of 2002):  

- Title I deals with the Department of Homeland Security (DHS) and its mission and functions.
- Title II deals with information analysis and infrastructure protection
- Title III deals with chemical, biological, radiological, and nuclear countermeasures
- Title IV deals with border and transportation security
- Title V deals with emergency preparedness and response
- Title VI deals with the internal management of the DHS.
- Title VII deals with general provisions and coordinating with nonfederal entities, the Inspector-General, and the U.S. Secret Services
- Title VIII deals with transitional items
- Title IX deals with conforming and other technical amendments

U.S. legislation in 2003 included the Prosecutorial/Remedies and Tools against the Exploitation of Children Today Act (PROTECT Act) – legislation aimed at child pornographers. In February 2003, this piece of legislation was passed by the U.S. Senate by a vote of 84-0. Its intent was to assist law enforcement agents in their efforts to track and identify pedophiles using the Internet. It was also intended to
permit the use of relevant images and graphics in prosecuting such cases. It is seen as a response to the April 16, 2002, Supreme Court decision that overturned most of the Child Pornography Prevention Act of 1996 (Known as the CPPA). That case was Ashcroft v. Free Speech Coalition (00-795), 198F.3d 1083.

Also in 2003, the Can Spam Act was passed on the United States Senate on November 25 and was aimed at commercial e-mailers and spammers. The bill was signed by President Bush on December 16, 2003 and took effect on January 1, 2004. Its longer title was the controlling the Assault of Non-solicited Pornography and marketing Act of 2003 a title that accurately reflects its purpose.

As of 2003, the U.S. Congress found that unsolicited commercial e-mail was estimated to account for more than one-half of all electronic mail traffic up from an estimated 7 per cent in 2001. Worse, Congress has noted that the volume of Spam continuous to rise – and that most of these messages are fraudulent or deceptive in one or more ways. It was for these important reasons that the Can Spam Act of 2003 was passed. Under the Act, Chapter 47 of title 18, United States Code, was amended at the end of new Section 1037, Fraud and Related Activity in connection with Electronic Mail.

Offenders under the Can Spam Act are those being in or affecting interstate or foreign commerce who knowingly:

- Access a protected computer without authorization and intentionally initiate the transmission of multiple commercial e-mail messages from or through that computer.
- Use a protected computer to relay or retransmit multiple commercial e-mail messages to deceive or mislead recipients or any Internet access service as to the origin of such e-mail messages.
- Falsify header information in multiple commercial e-mail messages and intentionally initiate the transmission of such messages.
- Falsify header information in multiple commercial e-mail messages and intentionally initiate the transmission of such messages.
- Register using information that falsifies the identity of the actual registrant for five or more e-mail accounts or online user accounts or two or more domain names.
- Falsely represent oneself to be registrant or the legitimate successor in interest to the registrant of five or more Internet Protocol (IP) address and intentionally
initiate the transmission of multiple commercial e-mail messages from such addresses.

The punishment for an offence under the Can Spam Act is a fine, imprisonment for not more than 5 years, or both. The Can Spam Act is enforced by the Federal Trade Commission (FTC). Unique to this Act, within 6 months of the date of its enactment, the FTC transmitted to the Senate Committee on Commerce, Science and Transportation and to the House of Representatives Committee on Energy and Commerce a report that set forth a plan and a time table for establishing a nationwide marketing Do-Not-E-Mail registry (“The Can Spam Act”, 2004).

Other countries have enacted similar anti-intrusion legislation. For example, Section 342.1 of the Canadian Criminal Code is aimed at several potential harms, including theft of computer services, invasion of privacy and persons who trade in computer passwords or who crack encryption systems. Changes for violations are typically made pertaining to the sections of the Criminal Code dealing with theft, fraud, Computer abuse, data abuse, and the interception of communications².

4.1.2 (B) UNITED KINGDOM

The United Kingdom has passed various legislations to deal with cyber crimes and to regulate the transactions on cyber space. In the context of combating cyber-crimes, the most important are the following TNO Acts:

- The Computer Misuse Act, 1990

The Computer Misuse Act 1990 contains the substantive provisions with regard to cyber offences and prescribes punishments for offences. The Act list the following as offences:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate commission of further offences
- Unauthorised modification of computer materials³.

Section 1 of the Computer Misuse Act 1990 imposes Criminal Liability and the accused is punishable with imprisonment for six months or fine or both.

A person is guilty of committing offence (Sec.2).

---

U/s 3 of the Act provides that a person is held liable for causing modification of any computer material with intent

i) to impair the operation of any computer
ii) to prevent access to any program or data
iii) to impair the operation of any such programme

The accused person be punished with imprisonment of six months, fine or both for Summary conviction but for severe offence the imprisonment extends to five years or fine or both.

As for the jurisdiction, the Act does not require the accused to have been in the home country on the impugned act took place is therein. Existence of any significant link with domestic jurisdiction is enough to attract the jurisdiction of British Court (Sec. 5)\(^4\).

4.1.3 (C) Australia

The Cyber Crime Act 2001 as amended by Act of 2002 deals with different offences under division 477 – serious computer offences and prescribe punishment for the commission of such offences as under:

The unauthorized access, modification or impairment with intent to commit a serious offence – a person guilty of such offence is punishable for imprisonment for life or five or more years (u/s 477-1).

- A person is guilty of an offence for unauthorized modification of data to cause impairment held in a computer attracts absolute liability and punishment is for ten years imprisonment (u/s 477.2).
- A person is guilty of an offence for unauthorized impairment of electronic communication to or from a computer attract punishment for ten years imprisonment (us 477.3).

Division 478 describes following offence punishable:

- Prescribes 2 years imprisonment for unauthorized access to, or modification of restricted data.
- Imprisonment for 2 years for unauthorized impairment of data held on a computer disc.
- Imprisonment for 3 years for possession or control of data with intent to commit a computer offence.

\(^4\). Supra 1 – p. 119.
• Imprisonment for 3 years for producing supplying or obtaining data with intent to commit a computer offence.

4.1.4 (D) Germany

Section 2002a, 263a, 269, 270, 303a and 303b of the German Penal Code provides for certain provisions of cyber crimes.

i) For data espionage (Sec. 2002a).

ii) For computer fraud (Sec. 263a)

iii) Falsification of legally relevant data (Sec. 269)

iv) For deception in Legal relations through data processing (Sec. 270)

v) For alteration of data (Sec. 303a)

vi) Computer sabotage (Sec. 303b)

4.1.5 (E) Singapore

Singapore passed the Computer Misuse Act in 1998 for dealing exclusively with cyber crimes. The Act is said to be enacted on the basis of UK Computer Misuse Act, 1990. The Act criminalises following acts and prescribes stringent punishments for each of them:

• Unauthorised access to computer material

• Access with intent to commit or facilitate commission of an offence

• Unauthorised modification of computer material

• Unauthorised use or interception of computer service

• Unauthorised obstruction of use of computer

• Unauthorised disclosure of access code

Further, the Act prescribes enhanced punishment for access, access with intent to commit or facilitate offence, unauthorized modification of computer material and unauthorized use or interception of computer service involving a protected computer to the tune of fine not exceeding $ 1,00,000 or imprisonment for a term not exceeding 20 years or both. Abatement and attempts to commit any of the above offences are also liable to same punishment.

The Act is applicable to all offences where either the accused was in Singapore at the material time or the computer program or data was in Singapore at the material time. The Act prescribes wide range of powers to the police officers to
investigate cyber crimes, including the power to inspect the information contained in
any computer system suspected of being used for any offences. He can also order any
person in possession of encrypted information to provide him with decryption
information. These powers are only subject to the written order from Commissioner
of Police and consent of public prosecutor in certain powers.

4.1.6 (F) Malaysia

Malaysia has enacted the computer Crimes Act, 1997. The Act provides for
criminal liability for cyber crimes.

i) Section 3 of the Act provides for punishment for unauthorized access
with fine or imprisonment for three years or both.

ii) Sec. 4 provides for punishment for act of fraud etc. through the
computer with fine or imprisonment for ten years or both.

iii) Sec. 5 provides for punishment for modification of data with fine or
imprisonment of seven years or both

iv) Sec. 6 provides for the act of communicating access code program,
password with fine or imprisonment for three years or both

v) Sec. 7 provides for same punishment of the offence concerned for
abetment or attempt to commit any of the above mentioned offences.
But in case of any act of preparation or act in furtherance of the offence,
the penalty will be one half of the penalty provided for the offence in
question.\(^5\)

4.2 LEGISLATIVE RESPONSE DEALING WITH CYBER CRIME IN INDIA

The Information Technology Act, 2000:

The Indian parliament enacted in the Fifty-first year of the Republic of India,
an Act called the Information Technology Act 2000. This Act is based on the
Resolution A/RES/51/162 adopted by the General Assembly of the United Nations on
30\(^{th}\) January, 1997 regarding the Model Law on Electronic Commerce earlier adopted
of the United Nations Commission on International Trade Law (UNCITRAL) in its
twenty-ninth Session.

The aforesaid resolution of the General Assembly recommends that all states
give favourable consideration to the Model Law on Electronic Commerce when they

\(^5\) Supra 3 – p. 118 - 119.
enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper based methods of communication and storage of information.

The Act further amends the Indian Penal Code, 1860, the Indian Evidence Act, 1872 the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act 1934.

Objectives — The electronic transactions like other parts of the globe, are in vogue in India, however, they were without legal security before the enactment of I.T. Act, 2000.

New Communication Systems and digital technology has made dramatic changes in the way we live. A revolution is occurring in the way people transact business. Business and consumers are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form has many advantages. It is cheaper, easier to store, retrieve and speedier to communicate. Many legal provisions assume the existence of paper based records and documents and records which should bear signatures. The Law of Evidence is traditionally based upon paper based records and oral testimony. Since electronic commerce eliminates the need for paper based transactions, hence to facilitate e-commerce, the needs for legal changes have become an urgent necessity. International trade through the medium of e-commerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to e-commerce.

The focus of the Information Technology Act is limited to facilitating e-commerce and e-governance and does not include combating of cyber crimes.

4.2.1 OFFENCES AND PENALTIES

The Act defines certain offences and penalties that deal with certain acts and omissions falling under the term cyber crimes. Chapter V deals with offences and Chapter IX with penalties and adjudication.

4.2.2 (I) Penalty for damage to Computer, Computer System etc.

Section 43 of the Information Technology Act, 2000 states if any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network —

7. This fact was admitted by the Parliamentary Affairs Minister Shri Pramod Majahan in Parliament, see HT 16 May, 2000.
b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

c) introduce or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

d) damages or causes to be damaged any computer, computer system or computer network data, computer data base or any other programmes residing in such computer, computer system or computer network;

e) disrupts or causes disruption of any computer, computer system of computer network;

f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, or rules or regulations made thereunder;

h) charges the services availed of by a person to the account of another person tampering with or manipulating any computer, computer system or computer network.

4.2.3 (2) Penalty for failure to furnish information, return, etc.

Section 44 provides that if any person who is required under this Act or any rules or regulations made thereunder to –

- furnish any document return or report to the controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

- file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

- maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues;
4.2.4 (3) Residuary penalty

Section 45 provides that 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.

4.3 Establishment of Cyber Appellate Tribunal

Central Government establishes one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal having appellate jurisdiction. The tribunal is entitled to exercise its appellate jurisdiction both on fact as also in law over a decision or order passed by the Controller of Certifying Authorities or the adjudicating officer.

4.4 Civil Court not to have jurisdiction

Section 61 stipulates that no court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

4.5 THE CYBER OFFENCES

The cyber crime in a collective term encompassing both ‘cyber contraventions’ and ‘cyber offences’.

Tampering with Computer source documents

Section 65 of the Act provides that whoever knowingly or intentionally concedes, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, 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 costing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

The term “computer source code” as defined in the Act incorporates the entire gamut of programming process. It includes computer commands/programming codes/machine; assembly and high/level) design prototypes flow charts/diagrams, technical documentation, design and layout of the necessary hardware program-testing details etc. Furthermore, it is important to know that the Act makes no mention whether the source code exists in tangible (a paper) or intangible (electrical pulses) form. The Act accepts the computer source code in both tangible and intangible form. The Act accepts the computer source code in both tangible and intangible form. Importantly by virtue of the Explanation, the term “Computer source code” also includes the software programm’s “object code” as well.

The idea behind the aforesaid section is to protect the ‘intellectual property’ invested in the computer programmes. The aforesaid section provides an added dimension to the copyright violation.

4.6.1 HACKING WITH COMPUTER SYSTEM

Section 66 states that –

(1) whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damages to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) whoever commits hacking shall be punished with imprisonment upto three years, or with fine which may extend upto two lakh rupees, or with both.

The offence of hacking may be committed in respect of both tangible (physical) and intangible (non physical) assets. Tangible assets include the hardware components of the computer resource(s) whereas intangible assets include information in the form of electronic, magnetic or optical impulses. For example, a computer hard disc is a physical assets but it may contain non-physical asset in the form of information.

---

9 Supra 6 - p. 142.

10 Supra 6 - p. 145-146.
4.6.2 HACKING AND THE INDIAN PENAL CODE

Surprisingly, the terms of hacking as defined under the Act seem somewhat similar to ‘mischief’ as defined under Sec. 425 of the Indian Penal code, 1860: Thus hacking signifies mischief with the computer resource. It is the mischief regarding destruction or alteration of any information residing in a computer resource. And it is mischief (hacking) with the computer system, i.e. using one computer to hack into another computer.

To brand any computer misuse as hacking would not be fallacious but also against the spirit of the section 66 of the Act. It is important that fulfillment of all the ingredients as given in the aforesaid section are a must before an accused could be pronounced guilty of the offence.\[11\]

4.7 PUBLISHING OF INFORMATION WHICH IS OBSCENE IN ELECTRONIC FORM

Whoever publishes or transmits or causes 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 five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees (Section 67).

4.7.1 PROTECTED SYSTEM

Section 70 provides that –

1. The appropriate Government may, by notification in the Official Gazette declare that only computer, computer system or computer network to be a protected system.

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.

\[11\] Supra 6 - p. 148-149.
4.7.2 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 pursuance 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 (Section 72).

4.8 OFFENCE FOR PUBLISHING DIGITAL SIGNATURE CERTIFICATE FALSE IN CERTAIN PARTICULARS

Section 73 stipulates that –

1. No person shall publish a Digital signature certificate or otherwise make it available to any other person with the knowledge that –
   (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

4.8.1 PUBLICATION FOR FRAUDULENT PURPOSE

Whoever knowingly creates, publishes, or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose 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 (Section 74).

4.8.2 APPLICATION OF THE ACT TO OFFENCE OR CONTRAVENATION COMMITTED OUTSIDE INDIA

Section 75 stipulates that –

(1) subject to the provision 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.
4.9 CONFISCATION

Section 76 of the Information Technology Act 2000, reads as:-

(1) Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

(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.

Following Acts have been necessitated to be amended to comply IT Act:

4.10. 2. AMENDMENTS TO THE INDIAN PENAL CODE, 1860

The Indian Penal Code are amended in the manner specified in the First Schedule to this Act. The amendments made are the following:

Section 29A inserted after Section 29 of the I.P.C.
Sections 167, 172, 173, 175, 192, 204, 463, 464, 466, 468, 469, 470, 471, 474, 476 and 477A.

4.10.1 3. AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872

The Indian Evidence Act 1872 are amended in the manner specified in the second schedule to this Act.

The Information Technology Act, 2000, introduces various amendments in the Indian Evidence Act, 1872.
The following sections have been amended:
Sections 3, 17, Sec. 22A inserted after Sec. 22, 34, 35, 39 Sec. 47A inserted after Sec. 47, Sec. 59, Sec. 65A & 65B inserted after Sec. 65, Sec. 73A inserted after Sec. 73, Sec. 81A inserted after Sec. 81, Sec. 85A & 85B & 85C inserted after Sec. 85, Sec. 88A inserted after Sec. 88, Sec. 90A inserted Sec. 90 and Sec. 131.

4.11 4. APPLICATION OF CRIMINAL PROCEDURE CODE IN CYBER CRIME INVESTIGATION
Clause(3) of Section 80 under Chapter XIII of the Information Technology Act, 2000 states that the provisions of the Code of Criminal Procedure, 1973 (2 of 1974), shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section. The following sections are dealing with cyber crime and Intellectual Property Crimes:
Section – 41, 100, 101, 102, 156, 165, 173(1),

4.11.1 (a) WHEN POLICE MAY ARREST WITHOUT WARRANT
Section 41(1)(a) of the code of Criminal Procedure, 1974 provides that any police officer may without an order from a Magistrate and without a warrant, arrest any person, who has been concerned in any cognizable offence, or against whom a reasonable complaint has been made, or credible information has been received, or a reasonable suspicion exists, of his having been so concerned.

4.12 COMPUTER FORENSIC AND THE PROCESS OF CONFISCATION
Computer Forensic Science

Computer Forensic Science was created to address the specific and articulated needs of law enforcement to make the most of this new form of electronic evidence. Computer forensic science is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media. As a forensic discipline, nothing since DNA technology has had such a large potential effect on specific types of investigations and prosecutions as computer forensic science.

Computer forensic science is, at its core different from traditional forensic disciplines. The computer material that is examined and the technique available to the examiner are products of a market driven private sector. Computer forensic science produces direct information and data that may have significance in a case.
4.12.1 Forensic Results

Forensic Science has historically produced results that have been judged to be both valid and reliable. For example, DNA analysis attempts to develop specific identifying information reactive to an individual. Forensic DNA scientists have gathered extensive statistical data on DNA profiles from which they base their conclusion. Computer forensic science extracts or produces information. The purpose of the computer examination is to find information related to the case. To support the results of a computer forensic examination, procedures are needed to ensure that only the information exists on the computer storage media, unaltered by the examination process.

4.12.2 Examination of Computer Evidence –

Computer evidence represented by physical items such as chips, boards, central processing units (CPUs), storage media, monitors and printers can be described easily and correctly as a unique form of physical evidence. The logging, description, storage, and disposition of physical evidence are well understood. Forensic laboratories have detailed plans describing acceptable methods for handling physical evidence. To the extent that computer evidence has a physical component, it does not represent any particular challenge. However, the evidence while stored in those physical items, is latent and exists only in a metaphysical electronic form. The result that is reported from the examination is the recovery of this latent information. Although forensic laboratories, are very good at ensuring the integrity of the physical items in their control, computer forensics also requires methods to ensure the integrity of the information contained within those physical items. The challenge to computer forensic science is to develop methods and techniques that provide valid and reliable results while protecting the real evidence – the information form ..............

To complicate the matter further, computer evidence almost never exists in isolation. It is a product of the data stored, the application used to create and store it, and the computer system that directed these activities. To a lesser extent, it is also a product of the software tools used in the laboratory to extract it.

Computer forensic science issues must also be addressed in the context of an emerging and rapidly changing environment. However, even as the environment changes, both national and international law enforcement agencies recognize the need
for common technical approaches and are calling for standards (Pollitt 1998).

There are two types of levels at which evidence of internet usage exists:

(a) Individual level
   (i) on an individual’s own computer, computer system or computer network,
   (ii) on the websites accessed by the individual using his own computer,
        computer system or computer network and

(b) ISP Level
   (i) On the servers of individual’s ISP

4.12.3 Collecting Evidence at Individual’s Level

Computers usually store text, graphic, image files, e-mails messages, etc. in the hard disk during its routine use. User may keep on deleting the unwanted material regularly to free up disk space. Similarly, chat rooms, Internet Relay Chat (IRC), Internet telephony sessions are real-time discussions happening on the Internet it is optional for the user to maintain logging files of these sessions.

Caching means copying of a Web Page/Site and storing that copy for the purpose of speeding up subsequent access. It ensures that the load on the servers of origin will be reduced as they can be accessed from the cached servers. With the help of browser software a user can retrieve any web page from the computer’s cache memory rather than going back to the original source site. In most browsers, whether Microsoft Explorer or Netscape Navigator, cache files are kept for many months and some specialist software can be used to view cache files and also associated “history” files, which retain some date-and-time information. Hence, it is possible to determine what the user of a specific computer has been actually viewing/browsing; it may further give the date-and-time of viewing/browsing.

From the Legal standpoint, the information (read: material) saved in a web-browser cache whether or not internationally retained constitutes “possession”.

It is sometimes possible to recover deleted logging files. However, the ........ Is on the person to demonstrate the accuracy and completeness of ‘once-lost, non found’ files.

4.12.4 Collecting Evidence @ ISP Level

Logs maintained by the users using dial up connections to connect top ISP indicate the time and duration on Internet usage connectivity. It will corroborate other
types of evidence that has already been gathered during investigations. Admissibility of such an evidence cannot be questioned as it clearly highlights not only the time and duration of computer’s Internet usage/connectivity, but also the fact that during a specific time period, the user’s computer had been working as a sort of ‘computer network’.

4.12.5 Problems With Preserving Computer Evidence

Preserving evidence is not an easy task. There exists both human and technical barriers to the evidence gathering mechanism. One must be aware of such limitations:

(a) Some of the facilities within the browsers to save www pages to the disk are imperfect as it may save the text but not the associated images.

(b) In case of some very complex pages, involving “frames” and “templates” there could be perceptible difference in what is seen on screen and what is saved on the disk.

(c) The method used to save a file to the disk may not carry and individual labeling, which shows where and when it was obtained. The problem with such saved files are that they could files are that they could be easily modified or forged.

(d) It is difficult to tell when a specific page has lost acquired, thanks to browser cache facility. Thus if one examines a whole series of cached pages, it is not easy to pinpoint which page came first and which later.

(e) It should not be forgotten that many ISPs use proxy servers to speed up the delivery of popular pages. Thus a user of such an ISP may not be sure that what he has received on his computer is the latest version from the source computer (website) is opposed to an earlier cached version held by his ISP12.

Concluding Comments:

This Chapter described the statutes dealing with cyber crimes. The different nations of the world, such as U.S.A, United Kingdom, Australia, Germany, Singapore, Malaysia have passed statutes dealing with cyber crimes. The Indian

---


The India has passed only Information Technology Act, to deal with cyber crimes but has no specific statute to deal with the urgent need of the time.