Commentary on Information Technology Act



By Rohas Nagpal President - Asian School of Cyber Laws



Rohas Nagpal

Rohas Nagpal is a lawyer by qualification, a cyber crime investigator by profession, a hacker at heart and a programmer by passion.

He advises corporates, law firms, Governments and law enforcement agencies on issues relating to technology law, cyber crime investigation, information warfare and cyber terrorism.

He has assisted the Government of India in drafting rules and regulations under the Information Technology Act.

He is an active public speaker on technology issues and has addressed thousands of students, law enforcement personnel, lawyers and other professionals around the world.

He has authored several books in digital forensic investigation, technology law and financial law. One of his publications, the *Cyber Crime Investigation Manual*, has been referred to as a "bible for cyber crime investigators" by Times of India – the world's largest selling English newspaper. He is also the author of the first ever Commentary on the Information Technology Act.

Papers authored by him include *Internet Time Theft & the Indian Law* (Bangalore, 2001), *Legislative Approach to Digital Signatures* (Ecuador, 2001), *Indian Legal position on Cyber* *Terrorism, Encryption and preventive measures* (on behalf of the Karnataka Police for Otto Schily, Interior Minister, Federal Republic of Germany), *Defining Cyber Terrorism* (Nagpur, 2002), *The mathematics of terror* (Nagpur, 2002) and *Cyber Terrorism – A Global Perspective* (Spain, 2002).

He has also co-authored an Internet Draft titled *Biometric based Digital Signature scheme*, which proposes a method of using biometrics to generate keys for use in digital signature creation and verification.

He headed the team that developed the world's smallest cyber crime investigation device, pCHIP a Portable Mega Investigation & Forensic Solution. This device is capable of capturing volatile evidence from a live computer, has an easy to use interface, and provides detailed reports.

He is the founder of CyberAttack, an open community working for cyber security. He also maintains www.bugs.ms, a specialized search engine that tracks bugs and vulnerabilities in Microsoft® products. He is also the founder of the proudIndian.me project and the Woman 2.0 Foundation. He is a member of International Association for Cryptologic Research (IACR).

Commentary on THE INFORMATION TECHNOLOGY ACT, 2000

(No.21 OF 2000)

As amended by the **Information Technology (Amendment) Act, 2008**

Rohas Nagpal Asian School of Cyber Laws

© 2014 Rohas Nagpal. All rights reserved.

INTRODUCTION

In order to arrive at an acceptable definition of the term Cyber Law, we must first understand the meaning of the term law.

Simply put, **law** encompasses the rules of conduct: (1) that have been approved by the government, and (2) which are in force over a certain territory, and (3) which must be obeyed by all persons on that territory. Violation of these rules could lead to government action such as imprisonment or fine or an order to pay compensation.

The term **cyber** or **cyberspace** has today come to signify everything related to computers, the Internet, websites, data, emails, networks, software, data storage devices (such as hard disks, USB disks etc) and even electronic devices such as cell phones, ATM machines etc.

Thus a simplified definition of cyber law is that it is the "**law governing** cyber space". The issues addressed by cyber law include: (1) Cyber crime¹ (2) Electronic commerce² (3) Intellectual Property in as much as it applies to cyberspace³ (4) Data protection & privacy⁴.

² The term electronic commerce or Ecommerce is used to refer to electronic data used in commercial transactions. Electronic commerce laws usually address issues of data authentication by electronic and / or digital signatures.

¹ An interesting definition of cyber crime was provided in the "Computer Crime: Criminal Justice Resource Manual" published in 1989. According to this manual, cyber crime covered the following: (1) computer crime i.e. any violation of specific laws that relate to computer crime (2) computer related crime i.e. violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution (3) computer abuse i.e. intentional acts that may or may not be specifically prohibited by criminal statutes. Any intentional act involving knowledge of computer use or technology is computer abuse if one or more perpetrators made or could have made gain and / or one or more victims suffered or could have suffered loss.

³ This encompasses (1) copyright law in relation to computer software, computer source code, websites, cell phone content, etc (2) software and source code licenses (3) trademark law with relation to domain names, meta tags, mirroring, framing, linking, etc (4) semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts (5) patent law in relation to computer hardware and software.

⁴ Data protection and privacy laws address legal issues arising in collecting, storing and transmitting sensitive personal data by data controllers such as banks, hospitals, email service providers, etc.

For the sake of convenience, we shall briefly discuss the development of cyber law around the world under two heads –

(1) International development of Cyber Law (which includes international measures and national measures) and

(2) Development of Cyber Law in India.

International development of Cyber Law⁵

The first comprehensive international effort dealing with the criminal law problems of computer crime was initiated by the **Organisation for Economic Co-operation and Development** (OECD)⁶.

From 1983 to 1985, an ad hoc committee of OECD discussed the possibilities of an international harmonization of criminal laws in order to fight computer-related economic crime. In September 1985, the committee recommended that member countries consider the extent to which knowingly committed acts in the field of computer-related abuse should be criminalized and covered by national penal legislation.

In 1986, based on a comparative analysis of substantive law, OECD suggested that the following list of acts could constitute a common denominator for the different approaches being taken by member countries:

(1) "The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit an illegal transfer of funds or of another thing of value;

(2) The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit a forgery;

(3) The input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer

⁵ Primary sources: International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime.

⁶ Twenty countries originally signed the Convention on the Organisation for Economic Co-operation and Development on 14 December 1960. Since then, a further ten countries have become members of the Organisation. The Member countries of the Organisation are: Australia, Austria, Belgium, Canada, Czech republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States.

systems, made willfully with the intent to hinder the functioning of a computer and/or telecommunication system;

(4) The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put it on the market;

(5) The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions."

From 1985 to 1989, the Select Committee of Experts on Computer-Related Crime of the **Council of Europe** discussed the legal problems of computer crime. The Select Committee and the European Committee on Crime Problems prepared Recommendation No. R(89)9, which was adopted by the Council on 13 September 1989.

This document "recommends the Governments of Member States to take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime... and in particular the guidelines for the national legislatures".

The guidelines for national legislatures include a minimum list, which reflects the general consensus of the Committee regarding certain computer-related abuses that should be dealt with by criminal law, as well as an optional list, which describes acts that have already been penalized in some States, but on which an international consensus for criminalization could not be reached.

The minimum list contains the following conduct:

(1) **Computer fraud**. The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing that influences the result of data processing, thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person;

(2) **Computer forgery**. The input, alteration erasure or suppression of computer data or computer programs, or other interference with the course of data processing in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence;

(3) **Damage to computer data or computer programs**. The erasure, damaging, deterioration or suppression of computer data or computer programs without right;

(4) **Computer sabotage**. The input, alteration, erasure or suppression of computer data or computer programs, or other interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system;

(5) **Unauthorized access**. The access without right to a computer system or network by infringing security measures;

(6) **Unauthorized interception**. The interception, made without right and by technical means, of communications to, from and within a computer system or network;

(7) **Unauthorized reproduction of a protected computer program**. The reproduction, distribution or communication to the public without right of a computer program which is protected by law;

(8) **Unauthorized reproduction of a topography**. The reproduction without right of a topography protected by law, of a semiconductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semiconductor product manufactured by using the topography.

The optional list contains the following conduct:

(1) Alteration of computer data or computer programs. The alteration of computer data or computer programs without right;

(2) **Computer espionage**. The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person;

(3) **Unauthorized use of a computer**. The use of a computer system or network without right, that either: (i) is made with the acceptance of significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or (ii) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or (iii) causes loss to the person entitled to use the system or harm to the system or its functioning;

(4) **Unauthorized use of a protected computer program**. The use without right of a computer program which is protected by law and which has been reproduced without right, with the intent, either to procure and unlawful economic gain for himself or for another person or to cause harm to the holder of the right.

In 1990, the legal aspects of computer crime were also discussed by the United Nations, particularly at the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, at Havana, as well as at the accompanying symposium on computer crime organized by the Foundation for Responsible Computing.

The Eighth United Nations Congress adopted a resolution on computerrelated crime. In its resolution 45/121, the General Assembly welcomed the instruments and resolutions adopted by the Eighth Congress and invited Governments to be guided by them in the formulation of appropriate legislation and policy directives in accordance with the economic, social, legal, cultural and political circumstances of each country.

The United Nations Commission on International Trade Law (UNCITRAL) formulated the UNCITRAL Model Law on Electronic Commerce in 1996. The Model Law is intended to facilitate the use of modern means of communication and storage of information. It is based on the establishment of a functional equivalent in electronic media for paper-based concepts such as "writing", "signature" and "original".

The *Convention on Cybercrime* of the Council of Europe is currently the only binding international instrument on the issue of cyber crime. The convention serves as a guideline for countries developing a comprehensive national legislation against cybercrime. It also serves as a framework for international cooperation between State Parties to the treaty⁷.

The Convention is supplemented by a *Protocol on Xenophobia and Racism committed through computer systems*.

Being at the forefront of computer technology, and being the country that developed what is today referred to as the Internet, the **USA** has been the global leader in developing laws relating to cyber crime. In 1977, Senator Abraham Ribicoff introduced the first Federal Systems Protection Act Bill. This evolved into House Bill 5616 in 1986, which

⁷ The signatories to the Convention are: Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

resulted in the *Computer Fraud and Abuse Act* of 1987 established as Article 1030, Chapter 47 of Title 18 of Criminal Code. The US states of Florida, Michigan, Colorado, Rhode Island and Arizona were the first to have computer crime laws based on the first Ribicoff bill⁸.

Some of the earlier relevant federal legislations include the *Communications Fraud and Abuse Act* of 1986, the *Electronic Communications Privacy Act* of 1986, the *Credit Card Fraud Act* of 1984, the *Federal Copyright Act* of 1976 and the *Wire Fraud Act*.

Also relevant are provisions of the *Electronic Fund Transfer Act* (Title XX of *Financial Institutions Regulatory and Interest Rate Control Act* of 1978) and the *Federal Privacy Act* of 1974 (codified in 5 USC Sect. 552a).

Some of the more recent US legislations relevant to cyber law are the 'No Electronic Theft' Act (1997), the Digital Millennium Copyright Act (1998), the Internet Tax Freedom Act (1998), the Child Online Protection Act (1998), the U.S. Trademark Cyberpiracy Prevention Act (1999), the Uniform Electronic Transactions Act (UETA) (1999), the Uniform Computer Information Transactions Act (UCITA) (2000), the Electronic Signatures in Global & National Commerce Act (E-Sign) (2000), the Children's Internet Protection Act (2001) and the USA Patriot Act (2001).

Also relevant is the *Uniform Electronic Transactions Act* which is a model law for US states.

In **China**, the relevant laws are the *Computer Information Network and Internet Security, Protection and Management Regulations* (1997), the *Regulations on Computer Software Protection* (2002) and the *Criminal Law of the People's Republic of China* (1979) as revised in 1997.

In Australia, the relevant law for cyber crime is the *Cybercrime Act* (2001) which amended the *Criminal Code Act* (1995). For electronic commerce, the relevant law is the *Electronic Transactions Act* (1999). Also relevant is The *Commonwealth's Privacy Act* (1988).

In **Canada**, the relevant law for cyber crime is the *Criminal Code* as amended to include computer crimes. For electronic commerce, the relevant law is the *Electronic Transactions Act* (2001).

⁸ See "Computer Crime: Criminal Justice Resource Manual" published in 1989.

In **Malaysia**, the relevant law for cyber crime is the *Computer Crimes Act* (1997). For electronic commerce, the relevant law is the *Digital Signatures Act* (1997).

In **Singapore**, the relevant law for cyber crime is the *Computer Misuse Act*. For electronic commerce, the relevant law is the *Electronic Transactions Act* (1998).

In the **United Arab Emirates**, the relevant law for cyber crime is the *Federal Law No. 2 of 2006 Combating Information Technology Crimes*. For electronic commerce, the relevant law is the Law No. 2 of 2002 of the Emirate of Dubai – *Electronic Transactions and Commerce Law*.

In the United Kingdom, the relevant laws for cyber crime are the Forgery and Counterfeiting Act (1981), Computer Misuse Act (1990), Data Protection Act (1998), Terrorism Act (2000), Regulation of Investigatory Powers Act (2000), Anti-terrorism, Crime and Security Act (2001) and Fraud Act (2006). For electronic commerce, the relevant laws are the Electronic Communications Act (2000) and the Electronic Signatures Regulations (2002).

In **Japan**, the relevant laws for cyber crime are the *Unauthorized Computer Access Law* (Law No. 128 of 1999) and the *Online Dating Site Regulating Act* (June 2008).

Development of Cyber Law in India

The chronological development of Indian cyber laws is discussed below:

2000:

The primary source of cyber law in India is the *Information Technology Act, 2000* (hereinafter referred to *Information Technology Act*) which came into force on 17th October 2000.

The primary purpose of the *Information Technology Act* is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

The *Information Technology Act* also penalizes various cyber crimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to crores of rupees).

The *Indian Penal Code* (as amended by the *Information Technology Act*) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.

Digital Evidence is to be collected and proven in court as per the provisions of the *Indian Evidence Act* (as amended by the *Information Technology Act*).

In case of bank records, the provisions of the *Bankers' Book Evidence Act* (as amended by the *Information Technology Act*) are relevant.

Investigation and adjudication of cyber crimes is done in accordance with the provisions of the *Code of Criminal Procedure*, *Civil Procedure Code* and the *Information Technology Act*.

The *Reserve Bank of India Act* was also amended by the *Information Technology Act*.

On 17th October 2000, the *Information Technology (Certifying Authorities) Rules, 2000* also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities. These rules also lay down the technical standards, procedures and security methods to be used by a Certifying Authority.

The *Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000* also came into force on 17th October 2000.

These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal whose primary role is to hear appeals against orders of the Adjudicating Officers.

2001:

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9th July 2001. They provide further technical standards and procedures to be used by a Certifying Authority.

Two important guidelines relating to Certifying Authorities were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the *Information Technology Act*. These guidelines were issued on 9th July 2001.

2002:

An Executive Order dated 12th September 2002 contained instructions relating provisions of the Act with regard to protected systems and application for the issue of a Digital Signature Certificate.

Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates. These were issued on 16th December 2002.

Minor errors in the Act were rectified by the *Information Technology* (*Removal of Difficulties*) Order, 2002 which was passed on 19th September 2002.

The Information Technology Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques.

2003:

On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed.

These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc.

These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

The appointment of adjudicating officers to decide the fate of multi-crore cyber crime cases in India was the result of the Public Interest Litigation (PIL) filed by students of Asian School of Cyber Laws (ASCL).

The Government had not appointed Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the passage of the IT Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers.

The Bombay High Court, in its order dated 9th October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon'ble Justice A.P. Shah and Hon'ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.

Following this, the Central Government passed an order dated 23rd March 2003 appointing the "Secretary of Department of Information Technology of each of the States or of Union Territories" of India as the adjudicating officers.

The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the Cyber Regulations Appellate Tribunal.

Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the Cyber Regulations Appellate Tribunal.

Also relevant are the *Information Technology (Other Standards) Rules,* 2003. An important order relating to blocking of websites was passed on 27th February, 2003. Under this, Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website.

The Information Technology (Certifying Authorities) Rules, 2000 were amended.

2004:

Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 have provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to Government bodies.

The *Information Technology (Security Procedure) Rules, 2004* came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records.

The Information Technology (Certifying Authorities) Rules, 2000 were amended.

2006:

The Information Technology (Certifying Authorities) Rules, 2000 were amended.

2009:

The Information Technology (Amendment) Act, 2008, which came into force on 27th October, 2009 has made sweeping changes to the Information Technology Act.

The following rules have also come into force on 27th October, 2009:

(1) Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. (2) Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

(3) Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

(4) The Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009

(5) Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009.

The Information Technology (Certifying Authorities) Rules, 2000 were amended.

2011

(1) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 passed. These rules define sensitive personal data or information and form the crux of India's data privacy law.

(2) Information Technology (Intermediaries guidelines) Rules, 2011 passed. These rules explain the due diligence to be observed by intermediaries.

(3) *Information Technology (Electronic Service Delivery) Rules, 2011* passed. These rules relate to the system of Electronic Service Delivery by the Government.

TABLE OF CONTENTS

PREAMBLE	19
CHAPTER I - PRELIMINARY	25
1. SHORT TITLE, EXTENT, COMMENCEMENT AND APPLICATION	
CHAPTER – II DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE	67
3. AUTHENTICATION OF ELECTRONIC RECORDS	
CHAPTER – III ELECTRONIC GOVERNANCE	72
 4. LEGAL RECOGNITION OF ELECTRONIC RECORDS	75 76 78
 7A. AUDIT OF DOCUMENTS, ETC., MAINTAINED IN ELECTRONIC FORM 8. PUBLICATION OF RULE, REGULATION, ETC., IN ELECTRONIC GAZETT 9. SECTIONS 6, 7 AND 8 NOT TO CONFER RIGHT TO INSIST DOCUMENT SHOULD BE ACCEPTED IN ELECTRONIC FORM	81 E82 82
ELECTRONIC SIGNATURE	82
10A. VALIDITY OF CONTRACTS FORMED THROUGH ELECTRONIC MEANS CHAPTER IV - ATTRIBUTION. ACKNOWLEDGEMENT AND DESPATCH OF	883
10A. VALIDITY OF CONTRACTS FORMED THROUGH ELECTRONIC MEANS CHAPTER IV - ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS	
CHAPTER IV - ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF	 85 85 90 ORD
CHAPTER IV - ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS	85 90 ORD 96
CHAPTER IV - ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS	85 90 ORD 96 105 105
CHAPTER IV - ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS	85 90 ORD 96 105 105 105 113
CHAPTER IV - ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS	85 90 ORD 96 105 105 113 113 113 114 116

21. LICENCE TO ISSUE ELECTRONIC SIGNATURE CERTIFICATES	117
22. APPLICATION FOR LICENCE	125
23. RENEWAL OF LICENCE	126
24. PROCEDURE FOR GRANT OR REJECTION OF LICENCE	
25. SUSPENSION OF LICENCE	128
26. NOTICE OF SUSPENSION OR REVOCATION OF LICENCE	130
27. POWER TO DELEGATE	
28. POWER TO INVESTIGATE CONTRAVENTIONS	
29. ACCESS TO COMPUTERS AND DATA	
30. CERTIFYING AUTHORITY TO FOLLOW CERTAIN PROCEDURES	
31. CERTIFYING AUTHORITY TO ENSURE COMPLIANCE OF THE ACT,	
32. DISPLAY OF LICENCE	
33. SURRENDER OF LICENCE	
34. DISCLOSURE	136
CHAPTER VII - ELECTRONIC SIGNATURE CERTIFICATES	137
35. CERTIFYING AUTHORITY TO ISSUE ELECTRONIC SIGNATURE	
Certificate	138
36. REPRESENTATIONS UPON ISSUANCE OF DIGITAL SIGNATURE	
Certificate	
37. SUSPENSION OF DIGITAL SIGNATURE CERTIFICATE	
38. REVOCATION OF DIGITAL SIGNATURE CERTIFICATE	144
39. NOTICE OF SUSPENSION OR REVOCATION	145
CHAPTER VIII - DUTIES OF SUBSCRIBERS	145
40. GENERATING KEY PAIR	
40A. DUTIES OF SUBSCRIBER OF ELECTRONIC SIGNATURE CERTIFIC	
41. ACCEPTANCE OF DIGITAL SIGNATURE CERTIFICATE	
42. CONTROL OF PRIVATE KEY	146
CHAPTER IX - PENALITIES, COMPENSATION AND ADJUDICATION	147
43. PENALTY AND COMPENSATION FOR DAMAGE TO COMPUTER, COI SYSTEM. ETC.	
43 A. COMPENSATION FOR FAILURE TO PROTECT DATA	
43 A. COMPENSATION FOR FAILURE TO FROTECT DATA	
44. FENALTY FOR FAILURE TO FORNISH INFORMATION, RETORN, ETC 45. RESIDUARY PENALTY	
45. RESIDUART PENALTT	
47. FACTORS TO BE TAKEN INTO ACCOUNT BY THE ADJUDICATING OF	
CHAPTER X - THE CYBER APPELLATE TRIBUNAL	204
48. ESTABLISHMENT OF CYBER APPELLATE TRIBUNAL	205
49. COMPOSITION OF CYBER APPELLATE TRIBUNAL	
50. QUALIFICATIONS FOR APPOINTMENT AS CHAIRPERSON AND MEN	
OF CYBER APPELLATE TRIBUNAL.	

	51. TERM OF OFFICE, CONDITIONS OF SERVICE, ETC., OF CHAIRPERSON	AND
	MEMBERS	
	52. SALARY, ALLOWANCES AND OTHER TERMS AND CONDITIONS OF SERV	/ICE
	OF CHAIRPERSON AND MEMBERS	208
	52A. POWERS OF SUPERINTENDENCE, DIRECTION, ETC	208
	52B. DISTRIBUTION OF BUSINESS AMONG BENCHES	208
	52C. Power of Chairperson to transfer cases	209
	52D. DECISION BY MAJORITY	209
	53. FILLING UP OF VACANCIES	209
	54. RESIGNATION AND REMOVAL	209
	55. ORDERS CONSTITUTING APPELLATE TRIBUNAL TO BE FINAL AND NOT	то
	INVALIDATE ITS PROCEEDINGS	210
	56. STAFF OF THE CYBER APPELLATE TRIBUNAL	211
	57. APPEAL TO CYBER APPELLATE TRIBUNAL	211
	58. PROCEDURE AND POWERS OF THE CYBER APPELLATE TRIBUNAL	219
	59. RIGHT TO LEGAL REPRESENTATION	229
	60. LIMITATION	230
	61. CIVIL COURT NOT TO HAVE JURISDICTION	
	62. Appeal to High Court	
	63. COMPOUNDING OF CONTRAVENTIONS	
	64. RECOVERY OF PENALTY OR COMPENSATION	232
_		
C	HAPTER XI - OFFENCES	234
	65. TAMPERING WITH COMPUTER SOURCE DOCUMENTS	234
	66. COMPUTER RELATED OFFENCES	241
	66A. PUNISHMENT FOR SENDING OFFENSIVE MESSAGES THROUGH	
	COMMUNICATION SERVICE, ETC	255
	66B. PUNISHMENT FOR DISHONESTLY RECEIVING STOLEN COMPUTER	
	RESOURCE OR COMMUNICATION DEVICE	258
	66C. PUNISHMENT FOR IDENTITY THEFT	260
	66D. PUNISHMENT FOR CHEATING BY PERSONATION BY USING COMPUTE	R
	RESOURCE	264
	66E. PUNISHMENT FOR VIOLATION OF PRIVACY	268
	66F. PUNISHMENT FOR CYBER TERRORISM	271
	67. PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIA	L IN
	ELECTRONIC FORM	274
	67A. PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL	
	CONTAINING SEXUALLY EXPLICIT ACT, ETC., IN ELECTRONIC FORM	280
	67B. PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL	
	DEPICTING CHILDREN IN SEXUALLY EXPLICIT ACT, ETC., IN ELECTRONIC FO	ORM
	67C. PRESERVATION AND RETENTION OF INFORMATION BY INTERMEDIAR	
	68. POWER OF THE CONTROLLER TO GIVE DIRECTIONS	

69. POWER TO ISSUE DIRECTIONS FOR INTERCEPTION OR MONITORING OR DECRYPTION OF ANY INFORMATION THROUGH ANY COMPUTER RESOURCE
69A. POWER TO ISSUE DIRECTIONS FOR BLOCKING PUBLIC ACCESS OF ANY
INFORMATION THROUGH ANY COMPUTER RESOURCE
69B. POWER TO AUTHORISE TO MONITOR AND COLLECT TRAFFIC DATA OR
INFORMATION THROUGH ANY COMPUTER RESOURCE FOR CYBER SECURITY 304
70. PROTECTED SYSTEM
70A. NATIONAL NODAL AGENCY
70B. INDIAN COMPUTER EMERGENCY RESPONSE TEAM TO SERVE AS
NATIONAL AGENCY FOR INCIDENT RESPONSE
71. PENALTY FOR MISREPRESENTATION
72. PENALTY FOR BREACH OF CONFIDENTIALITY AND PRIVACY
72A. PUNISHMENT FOR DISCLOSURE OF INFORMATION IN BREACH OF
LAWFUL CONTRACT
73. PENALTY FOR PUBLISHING ELECTRONIC SIGNATURE CERTIFICATE FALSE IN CERTAIN PARTICULARS
74. PUBLICATION FOR FRAUDULENT PURPOSE
75. ACT TO APPLY FOR OFFENCE OR CONTRAVENTION COMMITTED OUTSIDE
INDIA
76. CONFISCATION
77. COMPENSATION, PENALTIES OR CONFISCATION NOT TO INTERFERE WITH
OTHER PUNISHMENT
77A. COMPOUNDING OF OFFENCES
77B. OFFENCES WITH THREE YEARS IMPRISONMENT TO BE BAILABLE 335
78. POWER TO INVESTIGATE OFFENCE
CHAPTER XII - INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES 350
79. EXEMPTION FROM LIABILITY OF INTERMEDIARY IN CERTAIN CASES 350
CHAPTER XIIA - EXAMINER OF ELECTRONIC EVIDENCE
79A. CENTRAL GOVERNMENT TO NOTIFY EXAMINER OF ELECTRONIC
EVIDENCE
CHAPTER XIII - MISCELLANEOUS
80. POWER OF POLICE OFFICER AND OTHER OFFICERS TO ENTER, SEARCH,
ETC
81. ACT TO HAVE OVERRIDING EFFECT
82. CHAIRPERSON, MEMBERS, OFFICERS AND EMPLOYEES TO BE PUBLIC
SERVANTS
84. PROTECTION OF ACTION TAKEN IN GOOD FAITH
84A. Modes or methods for encryption
84B. PUNISHMENT FOR ABETMENT OF OFFENCES
84C. PUNISHMENT FOR ATTEMPT TO COMMIT OFFENCES

85. OFFENCES BY COMPANIES	366
86. REMOVAL OF DIFFICULTIES	
87. POWER OF CENTRAL GOVERNMENT TO MAKE RULES	
88. CONSTITUTION OF ADVISORY COMMITTEE	
89. POWER OF CONTROLLER TO MAKE REGULATIONS	
90. POWER OF STATE GOVERNMENT TO MAKE RULES	
FIRST SCHEDULE	
THE SECOND SCHEDULE	384
THE SECOND SCHEDULE AMENDMENTS TO THE INDIAN PENAL CODE	
	385
AMENDMENTS TO THE INDIAN PENAL CODE	385 390

ANNEXURE 1 – SAMPLE FIRST INFORMATION REPORT	405
ANNEXURE 2 – SAMPLE CRIMINAL COMPLAINT	409
ANNEXURE 3 – SAMPLE PROPERTY SEARCH & SEIZURE FORM	411
ANNEXURE 4 – FINAL FORM / REPORT	414
ANNEXURE 5 – SAMPLE COMPLAINT TO ADJUDICATING OFFICER	421
ANNEXURE 6 – REAL WORLD CASES	424
1. SOCIAL NETWORKING SITES RELATED CASES	424
2. EMAIL ACCOUNT HACKING	426
3. Credit Card Fraud	
4. ONLINE SHARE TRADING FRAUD	
5. TAX EVASION AND MONEY LAUNDERING	
6. Source Code Theft	
7. THEFT OF CONFIDENTIAL INFORMATION	
8. Software Piracy	435
9. MUSIC PIRACY	436
10. Email Scams	
11. Phishing	
12. Cyber Pornography	
13. ONLINE SALE OF ILLEGAL ARTICLES	440
14. USE OF INTERNET AND COMPUTERS BY TERRORISTS	
15. VIRUS ATTACKS	
16. Web Defacement	444

ANNEXURE 7 – RELEVANT INDIAN CASES	445
DIEBOLD SYSTEMS PVT LTD VS. COMMISSIONER OF COMMERCIAL TAXES	i
	445
P.R. TRANSPORT AGENCY VS. UNION OF INDIA	461
FIROS VS. STATE OF KERALA	467
AVNISH BAJAJ VS. STATE	476
SYED ASIFUDDIN VS. STATE OF ANDHRA PRADESH	513
STATE BANK OF INDIA VS. RIZVI EXPORTS LTD.	528
EXTRACTS FROM PARLIAMENT ATTACK CASE	536
ANNEXURE 8 – RELEVANT US CASES	557
BRIGGS V STATE OF MARYLAND	557
Pennsylvania v. Michael Murgallis	568
LIST OF ADJUDICATING OFFICERS	573
For the States	573
For the Union Territories	576

THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000)

Preamble

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the India Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

COMMENTS:

According to article 2(b) of the UNCITRAL Model Law on Electronic Commerce, "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information.

Electronic Data Interchange (EDI) is the exchange of standardized business documents from computer to computer. The key to EDI is the fact that all the documents exchanged conform to a common computerreadable format. Instead of sending email messages (which do not follow a set format), EDI allows for structured information to be exchanged. The most important EDI standard is the UN/EDIFACT (United Nations Electronic Data Interchange for Administration, Commerce & Transport).

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this term, as quoted below.

34. The Model Law does not settle the question whether the definition of EDI necessarily implies that EDI messages are communicated electronically from computer to computer, or whether that definition, while primarily covering situations where data messages are communicated through a telecommunications system, would also cover exceptional or incidental types of situation where data structured in the form of an EDI message would be communicated by means that do not involve telecommunications systems, for example, the case where

magnetic disks containing EDI messages would be delivered to the addressee by courier. However, irrespective of whether digital data transferred manually is covered by the definition of "EDI", it should be regarded as covered by the definition of "data message" under the Model Law.

Para 7 and 8 of the *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)* discuss the concept of electronic commerce in some detail, as quoted below.

7. The title of the Model Law refers to "electronic commerce". While a definition of "electronic data interchange (EDI)" is provided in article 2, the Model Law does not specify the meaning of "electronic commerce". In preparing the Model Law, the Commission decided that, in addressing the subject matter before it, it would have in mind a broad notion of EDI, covering a variety of trade-related uses of EDI that might be referred to broadly under the rubric of "electronic commerce" (see A/CN.9/360, paras. 28-29), although other descriptive terms could also be used. Among the means of communication encompassed in the notion of "electronic commerce" are the following modes of transmission based on the use of electronic techniques: communication by means of EDI defined narrowly as the computer-to-computer transmission of data in a standardized format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission of free-formatted text by electronic means, for example through the INTERNET. It was also noted that, in certain circumstances, the notion of "electronic commerce" might cover the use of techniques such as telex and telecopy.

8. It should be noted that, while the Model Law was drafted with constant reference to the more modern communication techniques, e.g., EDI and electronic mail, the principles on which the Model Law is based, as well as its provisions, are intended to apply also in the context of less advanced communication techniques, such as telecopy. There may exist situations where digitalized information initially dispatched in the form of a standardized EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of a telecopy of a computer printout. A data message may be initiated as an oral communication and end up in the form of a telecopy, or it may start as a telecopy and end up as an EDI message. A characteristic of electronic commerce is that it covers programmable messages, the computer

programming of which is the essential difference between such messages and traditional paper-based documents. Such situations are intended to be covered by the Model Law, based on a consideration of the users' need for a consistent set of rules to govern a variety of communication techniques that might be used interchangeably. More generally, it may be noted that, as a matter of principle, no communication technique is excluded from the scope of the Model Law since future technical developments need to be accommodated.

Para 15 and 16 of the *Guide to Enactment of the UNCITRAL Model Law* on *Electronic Commerce (1996)* discuss the functional-equivalent approach, as quoted below.

15. The Model Law is based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication. In the preparation of the Model Law, consideration was given to the possibility of dealing with impediments to the use of electronic commerce posed by such requirements in national laws by way of an extension of the scope of such notions as "writing", "signature" and "original", with a view to encompassing computer-based techniques. Such an approach is used in a number of existing legal instruments, e.g., article 7 of the UNCITRAL Model Law on International Commercial Arbitration and article 13 of the United Nations Convention on Contracts for the International Sale of Goods. It was observed that the Model Law should permit States to adapt their domestic legislation to developments in communications technology applicable to trade law without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements. At the same time, it was said that the electronic fulfilment of writing requirements might in some cases necessitate the development of new rules. This was due to one of many distinctions between EDI messages and paper based documents, namely, that the latter were readable by the human eve, while the former were not so readable unless reduced to paper or displayed on a screen.

16. The Model Law thus relies on a new approach, sometimes referred to as the "functional equivalent approach", which is based on an analysis of the purposes and functions of the traditional paper- based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-

commerce techniques. For example, among the functions served by a paper document are the following: to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts. It should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment.

WHEREAS the General Assembly of the United Nations by resolution A/RES/ 51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends *inter alia* that all States give favourable consideration to the said Model Law when they 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;

COMMENTS:

Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/51/628)] recommends that "...all States give favourable consideration to the Model Law when they 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;".

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:-

COMMENTS:

Statement of objects and reasons of the Information Technology Act, 2000 are:

New communication systems and digital technology have made dramatic changes in the way we live. A revolution is occurring in the way people transact business. Business and consumer are increasingly using computers to create transmit and store information in the electronic from instead of traditional paper documents. Information stored form has many advantages.

It is cheaper easier to store retrieve and speedier to communicate. Although people are aware of these advantages they are reluctant to conduct business or conclude any transaction in the electronic form due to lack of appropriate legal framework.

The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirement as to writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and document and records which should bear signatures.

The law of evidence it traditionally based upon paper based records and oral testimony. Since electronic commerce eliminates the need for paper-based transactions, hence to facilitate ecommerce the need for legal changes have become an urgent necessity. International trade through the medium of ecommerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to ecommerce.

The United Nations commission on international trade law (UNCITRAL) adopted the model laws on electronic commerce on 1986. the general assembly of united nations by its resolution no.51/162 dated 30th January, 1997 recommended that all states should give favourable considerations to the said model law when they enact or revise their laws. The model law provides for equal treatment of users of electronic communication and paper based communication.

Pursuant to a recent declaration by member countries, the world trade organization is likely to form a work programme to handle its work in this area including the possible creation of multilateral trade deals through the medium of electronic commerce. There is a need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. It is, therefore, proposed to provide for legal recongnition of electronic records and digital signature.

This will enable the conclusion of contracts and the creation of rights and obligations through the electronic medium. It is also proposed for a regulatory regime to supervise the certifying authorities issuing digital signature certificates.

To prevent the possible misuse arising out of transactions and other dealings concluded over the electronic medium, it is also proposed to create civil liabilities for contravention of the provisions of the proposed legislation. With a view to facilitate electronic governance, it is proposed to provide for the use and acceptance of electronic records and digital signatures in the government office and its agencies.

This will make the citizens interaction with the government offices hassle free. The proposal was also circulated to the state governments. They have supported the proposed legislation and have also expressed urgency for such legislation.

Statement of objects and reasons of the Information Technology (Amendment) Act, 2008 are:

1. The Information Technology act was enacted in the year 2000 with a view to give a fillip to the growth of electronic, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.

2. With proliferation of information technology enable services such as e-governance, e-commerce and e-transactions, protection of personal data and information and implementation of security practices and procedures relation to these application of electronic communications have assumed greater importance and they require harmonization with the provision of the information technology act. Further, protection of critical information infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary to declare such infrastructure as protected system as to restrict its access.

3. A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit material in electronic form, video voyeurism and breach of confidentially and leakage of data by intermediary, e-commerce frauds like personation commonly known as phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the information technology act, the Indian penal code, the Indian evidence act and the code of criminal procedure to prevent such crimes.

4. The United Nations commission on international trade law (UNCITRAL) in the year 2001 adopted the model law on electronic signatures. The general assembly of the united nations by its resolution no. 56/80, dated 12th December, 2001, recommended that all states accord favourable consideration to the said model law on electronic signature since the digital signature are linked to a specific technology under the existing provisions of the information technology act, it has become necessary to provide for alternate technology of electronic signature for bringing harmonization with model law.

5. The service providers may be authorized by the central government or the state government to set up, maintain and upgrade the computerised facilites and also collect, retain and appropriate service charges for providing such services at such as may be specified by the Central Government or the State Government.

CHAPTER I - PRELIMINARY

1. Short title, extent, commencement and application

(1) This Act may be called the Information Technology Act, 2000.

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

COMMENTS:

To understand the extent and jurisdiction of the Information Technology Act, we must examine sections 1(2) and 75 of the Act. Not only does it apply to the whole of India, but also to contraventions committed outside India, by anyone, involving a computer located in India.

Illustration: Kylie Minogue, an Australian national, residing in USA, gains unauthorized access to a computer located in India and deletes information. In this case, she will be liable under the provisions of the IT Act.

However, there are exceptions to the term "any person". Certain persons are exempt from prosecution under the IT Act. These include the President of India and the Governors of Indian states⁹, Foreign Heads of State and Ambassadors of foreign countries¹⁰.

(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.¹¹

COMMENTS:

The *Information Technology Act, 2000* was published in the official gazette on 9th June, 2000. Subsequently, it came into force on 17th October, 2000 vide notification quoted below:

G.S.R 788(E) In exercise of the powers conferred by sub-section (3) of section 1 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby appoints 17th Day of October 2000 as the date on which the provisions of the said Act comes into force. [No. 1(20)/97-IID(NII)/F6] (P.M.Singh) Joint Secretary.

⁹ Article 361(2) of the Constitution of India states that "No criminal proceedings whatsoever shall be instituted or continued against the President, or the Governor of a State, in any court during his term of office." Article 361(3) states "No process for the arrest or imprisonment of the President, or the Governor of a State, shall issue from any court during his term of office."

¹⁰ The principle of diplomatic immunity is enshrined in the "Vienna Convention on Diplomatic Relations" of 1961. The convention mentions that "the purpose of such privileges and immunities is not to benefit individuals but to ensure the efficient performance of the functions of diplomatic missions as representing States". This has been codified in India under the Diplomatic Relations (Vienna Convention) Act, 1972. Similar immunities are conferred on United Nations officers by the United Nations (Privileges and Immunities) Act, 1947.

¹¹ The Act came into force on 17th October 2000

The *Information Technology (Amendment) Act, 2008* came into force on 27th October, 2009.

(4) Nothing in this Act shall apply to documents or transactions specified in the First Schedule:

Provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries thereto.¹² COMMENTS:

The Act does not apply to:

1. A negotiable instrument (other than a cheque) as defined in section 13 of the *Negotiable Instruments Act, 1881*. Section 13(1) of the *Negotiable Instruments Act, 1881* defines a "negotiable instrument" as a promissory note, bill of exchange or cheque payable either to order or to bearer.

When the Information Technology Act was originally passed in 2000, it did not apply to negotiable instruments. This changed after the *Negotiable Instruments (Amendments & Miscellaneous Provisions) Act, 2002* came into force and amended the Information Technology Act.

Now the Information Technology Act applies to cheques but not to other negotiable instruments such as bills of exchange, promissory notes etc. *Negotiable Instruments (Amendments & Miscellaneous Provisions) Act* also introduced two concepts that have had a major impact on banking in India. These concepts are "cheque in the electronic form" and "truncated cheque".

A cheque in the electronic form contains the exact mirror image of a paper cheque. It is generated, written and affixed with a digital signature in a secure system.

¹² Substituted by Information Technology (Amendment) Act, 2008 for "Nothing in this Act shall apply to,- (a) a negotiable instrument (other than a cheque)¹² as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881); (b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882 (7 of 1882); (c) a trust as defined in section 3 of the Indian Trusts Act, 1882 (2 of 1882); (d) a will as defined in clause (h) of section (2) of the Indian Succession Act, 1925 (39 of 1925), including any other testamentary disposition by whatever name called; (e) any contract for the sale or conveyance of immovable property or any interest in such property; (f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette."

Cheque Truncation is the settlement of clearing transactions on the basis of images and electronic data without the physical movement of the cheques.

2. A power-of-attorney as defined in section 1A of the *Powers-of-Attorney Act, 1882.* According to section 1A of the *Powers-of-Attorney Act, 1882,* a power-of-attorney includes any instruments empowering a specified person to act for and in the name of the person executing it.

3. A trust as defined in section 3 of the *Indian Trusts Act, 1882.* According to section 3 of the Indian Trusts Act, 1882, a trust is an obligation annexed to the ownership of property.

4. A will as defined in clause (h) of section 2 of the *Indian Succession Act, 1925.* According to section 2(h) of the *Indian Succession Act, 1925,* "will" means the legal declaration of the intention of a testator with respect to his property which he desires to be carried into effect after his death.

5. Any contract for the sale or conveyance of immovable property or any interest in such property.

According to section 2(h) of the *Indian Contract Act, 1872*, an agreement enforceable by law is a contract.

According to section 3(26) of *General Clauses Act, 1897*, "immovable property" shall include land, benefits to arise out of land, and things attached to the earth, or permanently fastened to anything attached to the earth.

According to section 5 of the *Transfer of Property Act, 1882*, "transfer of property" means an act by which a living person conveys property, in present or in future, to one or more other living persons, or to himself and one or more other living persons; and "to transfer property" is to perform such act.

According to section 3 of the *Transfer of Property Act, 1882*, "immoveable property" does not include standing timber, growing crops or grass.

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.¹³

2. Definitions.

¹³ Inserted by Information Technology (Amendment) Act, 2008.

(1) In this Act, unless the context otherwise requires,-

(a) "access" with its grammatical variations and cognate expressions, means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

COMMENTS:

Essentials of the term "access" are: (A) Gaining entry into a computer, computer system or computer network (B) Instructing the logical, arithmetical, or memory function resources of a computer, computer system or computer network (C) Communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Grammatical variations of access include terms such as accesses, accessed, accessing etc. *Cognate expressions* are related words and phrases. Depending upon the situation, these could include "log on", "retrieve" etc. *Gaining entry into* applies to physical access. The terms computer, computer system and computer network have been defined very widely under the IT Act. These terms may include the physical box (cabinet) in which a computer is housed. They may also include the physical room in which a computer network or super computer is housed.

Illustration: A massive super computer is housed in particular premises. Sameer breaks open the door and enters the premises. He has gained entry into the computer.

Illustration: A Government computer contains critical information in its hard disk. Sameer unscrews the cabinet of the computer in order to steal the hard disk. He has gained entry into the computer.

Instructing means "to give orders" or "to direct". Instructing is essentially a one way process which does not require two-way communication between the instructor and the instructed.

Illustration: A Government computer contains critical information. Sameer enters the room where the computer is located and keys in some commands into the keyboard. He does not realise that the keyboard is disconnected from the computer. Here, Sameer has not instructed the logical, arithmetic or memory functions of the computer.

Illustration: Sameer has set up his computer in such a way that he can remotely shut it down by sending an SMS. The process is as under:

- i. He sends an SMS with the words "shutdown" to a particular service provider.
- ii. The service provider automatically forwards the contents of the SMS to Sameer's personal email address.
- iii. Sameer's computer is running an email client (e.g. Microsoft Outlook) that is configured to automatically download emails from his account every 5 minutes.
- iv. The email client is also configured to run a file called "shutdown.bat" every time it downloads an email with the words "shutdown" in it.
- v. This "shutdown.bat" files shuts down Sameer's computer within a few seconds.
- vi. This enables Sameer to shutdown his computer even when he is not in the same country.

This is an illustration of instructing the logical, arithmetic or memory functions of the computer.

Communicating with is essentially a two-way process that involves exchange of information.

Illustration: Sameer is a hacker attempting to steal some information from Sanya's computer. He first remotely scans Sanya's computer using specialised software. The software sends out queries to Sanya's computer which replies to the queries. As a result of this, Sameer obtains details of the operating system installed on Sanya's computer. Sameer has communicated with Sanya's computer.

AUSTRALIA:

According to section 476.1 of *The Criminal Code* "access to data held in a computer" means: (a) the display of the data by the computer or any other output of the data from the computer; or (b) the copying or moving of the data to any other place in the computer or to a data storage device; or (c) in the case of a program—the execution of the program.

MALAYSIA:

A relevant provision is section 2(2) of the *Computer Crimes Act*, which states-

(2) For the purposes of this Act, a person secures access to any program or data held in a computer if, by causing a computer to perform any function, he—

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held whether by having it displayed or in any other manner,

and references to access to a program or data and to an intent to secure such access shall be construed accordingly.

Also relevant is section 2(3) of the Computer Crimes Act, which states-

For the purposes of paragraph (2)(c), a person uses a program if the function he causes the computer to perform—

(a) causes the program to be executed; or

(b) is itself a function of the program.

Also relevant is section 2(4) of the Computer Crimes Act, which states-

(4) For the purposes of paragraph (2)(d), the form in which any program or data is output and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer is immaterial.

SINGAPORE:

A relevant provision is section 2(2) of the *Computer Misuse Act*, which states-

(2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he —

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner),

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

Also relevant is section 2(3) of the Computer Misuse Act, which states-

(3) For the purposes of subsection (2)(c), a person uses a program if the function he causes the computer to perform —

(a) causes the program to be executed; or

(b) is itself a function of the program.

Also relevant is section 2(4) of the Computer Misuse Act, which states-

(4) For the purposes of subsection (2)(d), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

UNITED KINGDOM:

A relevant provision is section 17(2) of the *Computer Misuse Act*, which states-

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he—

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

Also relevant is section 17(3) of the Computer Misuse Act, which states-

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform—

(a) causes the program to be executed; or

(b) is itself a function of the program.

Also relevant is section 17(4) of the Computer Misuse Act, which states-

(4) For the purposes of subsection (2)(d) above—

(a) a program is output if the instructions of which it consists are output; and

(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

COMMENTS:

In most electronic transactions there are at least 3 parties – the originator, the addressee and the intermediary.

Illustration: Pooja uses her gmail.com email account to send an email to Sameer. Pooja is the originator of the email. Gmail.com is the intermediary. Sameer is the addressee.

According to article 2(d) of the UNCITRAL Model Law on Electronic Commerce, "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message.

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this term, as quoted below:

36. The "addressee" under the Model Law is the person with whom the originator intends to communicate by transmitting the data message, as opposed to any person who might receive, forward or copy the data message in the course of transmission. The "originator" is the person who generated the data message even if that message was transmitted by another person. The definition of "addressee" contrasts with the definition of "originator", which is not focused on intent. It should be noted that, under the definitions of "originator" and "addressee" in the Model Law, the originator and the addressee of a given data message could be the same person, for example in the case where the data message was intended for storage by its author. However, the addressee who stores a message transmitted by an originator".

(c) "adjudicating officer" means an adjudicating officer appointed under sub-section (1) of section 46;

COMMENTS:

The appointment of adjudicating officers to decide the fate of multi-crore cyber crime cases in India was the result of the Public Interest Litigation (PIL) filed by students of Asian School of Cyber Laws (ASCL).

The Government had not appointed Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the passage of the Information Technology Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers.

The Bombay High Court, in its order dated 9th October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon'ble Justice A.P. Shah and Hon'ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.

Following this, the Central Government passed an order dated 23rd March 2003 appointing the "Secretary of Department of Information Technology of each of the States or of Union Territories" of India as the adjudicating officers. The order is quoted below:

O R D E R

G.S.R.240(E) In exercise of the powers conferred by sub-section (1) of section 46 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following order/appointments viz. -

1. Whereas sub-section (1) of the section 46 makes provision for appointment of one or more Adjudicating Officers not below the rank of Director to the Central Government and subsection (3) requires that such an officer should possess experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government and whereas such experience necessary for appointment as Adjudicating Officer has been notified by the Central Government as per the Gazette Notification for Information Technology Rules 2003 under the short title Qualification and Experience of Adjudicating Officer and Manner of Holding Enquiry vide Gazette Notification GSR dated March, 2003.

2. Further Whereas the Secretary of the Department of Information Technology of each of the States or Union Territories are normally not below the rank of Director and possess the requisite experience in the field of Information Technology and also possess legal/judicial experience as required, therefore the Secretary of Department of Information Technology of each of the States or of Union Territories is hereby appointed as Adjudicating Officer for the purposes of the Information Technology Act, 2000.

3. The Department of Information Technology of each of the States or of Union Territories shall provide the infrastructure and maintain the records of the matters handled by Adjudicating Officer functioning in the States/Union Territories.

(d) "affixing electronic signature"¹⁴, with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of electronic signature;

COMMENTS:

This issue is discussed under the comments on section 2(1)(ta) and section 3A.

(e) "appropriate Government " means as respects any matter,-

(i) enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution,

the State Government and in any other case, the Central Government;

COMMENTS:

Article 246 of the Constitution of India is as under:

246. (1) Notwithstanding anything in clauses (2) and (3), Parliament has exclusive power to make laws with respect to any of the matters enumerated in List I in the Seventh Schedule (in this Constitution referred to as the "Union List").

¹⁴ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

(2) Notwithstanding anything in clause (3), Parliament, and, subject to clause (1), the Legislature of any State also, have power to make laws with respect to any of the matters enumerated in List III in the Seventh Schedule (in this Constitution referred to as the "Concurrent List").

(3) Subject to clauses (1) and (2), the Legislature of any State has exclusive power to make laws for such State or any part thereof with respect to any of the matters enumerated in List II in the Seventh Schedule (in this Constitution referred to as the "State List").

(4) Parliament has power to make laws with respect to any matter for any part of the territory of India not included in a State notwithstanding that such matter is a matter enumerated in the State List.

List I—Union List of the seventh schedule to the *Constitution of India* contains items including defence of India, naval, military and air forces, atomic energy, Central Bureau of Intelligence and Investigation, foreign affairs, foreign jurisdiction, citizenship, naturalisation and aliens, extradition, railways, national highways, shipping and navigation on national waterways, maritime shipping and navigation, airways, posts and telegraphs, etc.

List II—State List of the seventh schedule to the *Constitution of India* contains items including public order, police, prisons, local government, agriculture, water supply, trade and commerce within the state, betting and gambling, etc.

List III— Concurrent List of the seventh schedule to the *Constitution of India* contains items including criminal law, criminal procedure, marriage and divorce, contracts, civil procedure, education, electricity, newspapers, books and printing presses, etc.

(f) "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

COMMENTS:

The term asymmetric crypto system has been discussed in the UNCITRAL publication titled *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods*, para 26 of which is quoted below:

26. Digital signatures are created and verified by using cryptography, the branch of applied mathematics that is concerned with transforming messages into a seemingly unintelligible form and then back into their original form. Digital signatures use what is known as public key cryptography, which is often based on the use of algorithmic functions to generate two different but mathematically related "keys" (i.e. large numbers produced using a series of mathematical formulae applied to prime numbers). One key is used for creating a digital signature or transforming data into a seemingly unintelligible form, and the other key is used for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively referred to as "cryptosystems" or, more specifically, "asymmetric cryptosystems" where they rely on the use of asymmetric algorithms.

(g) "Certifying Authority" means a person who has been granted a licence to issue a Electronic Signature Certificate¹⁵ under section 24; COMMENTS:

Article 2(e) of the UNCITRAL Model Law on Electronic Signatures, defines "Certification service provider" as a person that issues certificates and may provide other services related to electronic signatures.

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this provision, as quoted below:

53. To associate a key pair with a prospective signatory, a certification service provider (or certification authority) issues a certificate, an electronic record that lists a public key together with the name of the certificate subscriber as the "subject" of the certificate, and may confirm that the prospective signatory identified in the certificate holds the corresponding private key. The principal function of a certificate is to bind a public key with a particular signatory. A "recipient" of the certificate desiring to rely upon a digital signature created by the signatory named in the certificate can use the public key listed in the certificate to verify that the digital signature was created with the corresponding

¹⁵ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

private key. If such verification is successful, a level of assurance is provided technically that the digital signature was created by the signatory and that the portion of the message used in the hash function (and, consequently, the corresponding data message) has not been modified since it was digitally signed.

54. To assure the authenticity of the certificate with respect to both its contents and its source, the certification service provider digitally signs it. The issuing certification service provider's digital signature on the certificate can be verified by using the public key of the certification service provider listed in another certificate by another certification service provider (which may but need not be on a higher level in a hierarchy), and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness. Among other possible ways of verifying the digital signature of the certification service provider, that digital signature can also be recorded in a certificate issued by that certification service provider itself, and sometimes referred to as a "root certificate". In each case, the issuing certification service provider must digitally sign its own certificate during the operational period of the other certificate used to verify the certification service provider's digital signature. Under the laws of some States, a way of building trust in the digital signature of the certification service provider might be to publish the public key of the certification service provider (see A/CN.9/484, para. 41) or certain data pertaining to the root certificate (such as a "digital fingerprint") in an official bulletin.

105. No distinction has been drawn in the Model Law between situations where a certification service provider engages in the provision of certification services as its main activity or as an ancillary business, on a habitual or an occasional basis, directly or through a subcontractor. The definition covers all entities that provide certification services within the scope of the Model Law, that is, "in the context of commercial activities". However, in view of that limitation in the scope of application of the Model Law, entities that issued certificates for internal purposes and not for commercial purposes would not fall under the category "certification service providers" as defined in Article 2.

(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that

the Certifying Authority employs in issuing Electronic Signature¹⁶ Certificates;

COMMENTS:

Annexure I to Circular No. 1/2001 dated 9th July 2001 titled "Guidelines for submission of application for licence to operate as a Certifying Authority under the IT Act, 2000" issued by Office of Controller of Certifying Authorities provides a detailed explanation of the contents of a certification practice statement. It is as below:

CERTIFICATION PRACTICE STATEMENT

The CPS framework given below is based on RFC-2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. All the components listed in the framework must be specified in the CPS.

GENERAL PROVISIONS

This component specifies any applicable presumptions on a range of legal and general practice topics and shall contain,-

(a) **Obligations**

This sub-component shall contain the type of entity, the provisions relating to the entity's obligations to other entities and may include:

- 1. Certifying Authority (CA) obligations,
- 2. Subscriber obligations,
- 3. Relying party obligations,
- 4. Repository obligations

(b) Liability

This sub-component shall contain provisions regarding apportionment of liability for each type of entity such as, -

1. Warranties and limitations on warranties;

^{2.} Kinds of damages covered (e.g., indirect, special, consequential, incidental, punitive, liquidated damages, negligence and fraud) and disclaimers;

¹⁶ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

3. Loss limitations (caps) per certificate or per transaction;

4. Other exclusions (e.g., Acts of God, other party responsibilities, etc).

(c) Financial Responsibility

This sub-component shall consist of provisions relating to financial responsibilities of the Certifying Authority and repository such as:

1. Indemnification of Certifying Authority by relying parties;

2. Fiduciary relationships (or lack thereof) between the various entities;

3. Administrative processes (e.g., accounting, audit, etc.).

(d) Interpretation and Enforcement

This sub-component will contain provisions relating to the interpretation and enforcement of the Certificate Policy and the Certification Practice Statement and shall address the following topics:

1. Governing laws;

- 2. Severability of provisions, survival, merger, and notice; and
- 3. Dispute resolution procedures.

(e) Fees

This sub-component shall consist of provisions relating to the fees charged by the Certifying Authorities and repositories such as:

1. Certificate issuance or renewal fees;

- 2. Certificate access fee;
- 3. Revocation or status information access fee;
- 4. Fees for other services such as policy information; and
- 5. Refund policy.

Note.-

(i) In respect of issuance, renewal, access, revocation and status information the fee structure shall be based on the class of certificate.

(ii) The different classes of certificates issued must be specified.

(iii) In addition to four classes of certificates given below, the Certifying Authority may issue more classes of Public Key Certificates, but these must be explicitly defined including the purpose for which each class is used and the verification methods underlying the issuance of the certificate. The suggested four classes are the following :-

Class 0 Certificate: This certificate shall be issued only for demonstration/test purposes.

Class 1 Certificate: Class 1 certificates shall be issued to individuals/private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.

Class 2 Certificate: These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.

Class 3 Certificate: This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.

(f) Publication and Repositories

This sub-component shall contain all applicable provisions regarding:

1. Certifying Authority's obligations to publish information regarding its practices, its certificates, and the current status of such certificates;

2. Frequency of publication;

3. Access control on published information objects including certificate policy definitions, Certificate Practice Statements, certificates, certificate status, and CRLs; and

4. Requirements pertaining to the use of repositories operated by Certifying Authorities or by other independent parties.

(g) Compliance Audit

This sub-component shall contain the following information:

- 1. Frequency of compliance audits for each entity;
- 2. Identity/qualifications of the auditor;
- 3. Auditor's relationship to the entity being audited;
- 4. List of topics covered under the compliance audit;

5. Actions taken as a result of a deficiency found during compliance audit;

6. Compliance audit results: with whom they are shared with (e.g. Certifying Authorities and/or end entities), who provides them, auditors and how they are audited and how the audits are communicated.

(h) Policy of Confidentiality

This sub-component will address the following:

1. Types of information that must be kept confidential by Certifying Authority;

2. Types of information that are not considered confidential;

3. Who is entitled to be informed of reasons for revocation and suspension of certificates?

4. Policy on release of information to law enforcement officials;

5. Information that can be revealed as part of civil discovery;

6. Conditions upon which Certifying Authority may disclose upon owner's request; and

7. Any other circumstances under which confidential information may be disclosed.

(i) Intellectual Property Rights

This sub-component shall consist of ownership rights of certificates, practice/policy specifications, names, and keys.

IDENTIFICATION AND AUTHENTICATION

This component will describe the procedures used to authenticate a certificate applicant to a Certifying Authority prior to certificate issuance. It will also describe how parties requesting re-key or revocation are authenticated. It will contain naming practices, including recognition of name ownership and name dispute resolution.

This component will have the following sub-components:

- (a) Initial Registration;
- (b) Routine Re-key;
- (c) Re-key After Revocation; and
- (d) Revocation Request.

OPERATIONAL REQUIREMENTS

This component will specify requirements imposed upon issuing Certifying Authority or end entities with respect to various operational activities and will contain the following subcomponents:

(a) Certificate Application;

(b) Certificate Issuance;

(c) Certificate Acceptance;

(d) Certificate Suspension and Revocation;

(e) Security Audit Procedures;

(f) Records Archival;

(g) Key Changeover;

(h) Compromise and Disaster Recovery; and

(i) Certifying Authority Termination/Suspension.

PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

(i) This component will describe the matters relating to nontechnical security controls (that is, physical, procedural, and personnel controls) used by the issuing Certifying Authority to perform securely the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

(ii) This component can also be used to define non-technical security controls on repository and end entities.

(iii) These non-technical security controls are critical to trusting the certificates since lack of security may compromise Certifying Authority operations resulting, for example, in the creation of certificates or CRLs with erroneous information or the compromise of the Certifying Authority private key.

This component will consist the following three sub-components:

(a) Physical Security Controls;

(b) Procedural Controls; and

(c) Personnel Security Controls.

TECHNICAL SECURITY CONTROLS

(i) This component will be utilized to define the security measures taken by the issuing Certifying Authorities to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually held key shares). This component may also be used to impose constraints on repositories and end entities to protect their cryptographic keys and critical security parameters. Secure key management is critical and the component will ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

(ii) This component will also contain other technical security controls used by the issuing Certifying Authority to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, audit, and archival. Technical controls will include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

(iii) This component can also be used to define other technical security controls on repositories and end entities.

This component shall have the following sub-components:

- (a) Key Pair Generation and Installation;
- (b) Private Key Protection;
- (c) Other Aspects of Key Pair Management;
- (d) Activation Data;
- (e) Computer Security Controls;
- (f) Life-Cycle Security Controls;
- (g) Network Security Controls; and
- (h) Cryptographic Module Engineering Controls.

CERTIFICATE AND CRL PROFILES

This component will specify the certificate format and, if CRLs are used, the CRL format. Assuming use of the X.509 certificate and CRL formats, this includes information on profiles, versions, and extensions used.

This component will have two sub-components:

- (a) Certificate Profile; and
- (b) CRL Profile.

SPECIFICATION ADMINISTRATION

This component will contain the specifications as to how particular certificate policy definition or CPS will be maintained and shall contain the following sub-components:

(a) Specification Change Procedures;

(b) Publication and Notification Procedures; and

(c) CPS Approval Procedures.

OUTLINE OF A SET OF PROVISIONS

This component will contain outlines for a set of provisions, intended to serve as a checklist or a standard template for use by certificate policy or CPS writers. Such an outline will facilitate:

(a) Comparison of two certificate policies during cross-certification (for the purpose of equivalency mapping).

(b) Comparison of a Certificate Practice Statement with a certificate policy definition to ensure that the CPS faithfully implements the policy.

(c) Comparison of two Certificate Practice Statements.

Rules 18 of the *Information Technology (Certifying Authorities) Rules,* 2000 is also relevant in this regard. It states:

18. Governing Laws.-

The Certification Practice Statement of the Certifying Authority shall comply with, and be governed by, the laws of the country.

(ha) "communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;¹⁷

(i) "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or relates to the computer in a computer system or computer network;

COMMENTS:

Simply put, a computer has the following characteristics:

- 1. It is a high-speed data processing device or system.
- 2. It may be electronic, magnetic, optical, etc.
- 3. It performs logical, arithmetic, and memory functions.

¹⁷ Inserted by Information Technology (Amendment) Act, 2008.

4. These functions are performed by manipulations of electronic, magnetic or optical impulses.

Computer includes all input facilities, all output facilities, all processing facilities, all storage facilities, all computer software facilities, and all communication facilities which are connected or related to the computer in a computer system or network.

Let us examine the important terms used in this definition.

According to American law, *electronic* means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. [Title 15, Chapter 96, Sub-chapter I, section 7006(2), US Code].

Magnetic means having the properties of a magnet; i.e. of attracting iron or steel e.g. parts of a hard disk are covered with a thin coat of magnetic material.

Simply put, an optical computer uses light instead of electricity to manipulate, store and transmit data. Development of this technology is still in a nascent stage.

Optical data processing can perform several operations simultaneously (in parallel) much faster and more easily than electronic data processing.

Optical fibre is the medium and the technology associated with the transmission of information as light pulses along a glass or plastic wire or fibre.

Optical fibre carries much more information than conventional copper wire and is in general not subject to electromagnetic interference.

A *data processing device or system* is a mechanism that can perform predefined operations upon information.

The following are illustrations of *functions* in relation to a conventional desktop personal computer: (1) saving information on a hard disk (2) logging on to the Internet (3) retrieving stored information (4) calculating mathematical formulae.

Logical functions, simply put, refer to non-arithmetic processing that arranges numbers or letters according to a pre-defined format e.g. arranging numbers in ascending order, arranging words alphabetically etc.

Arithmetic functions, simply put, are operations concerned or involved with mathematics and the addition, subtraction, multiplication and division of numbers.

Memory functions, simply put, refer to operations involving storage of data.

Input facilities are those which transfer information from the outside world into a computer system. E.g. keyboard, mouse, touch screen, joystick, microphone, scanner, etc.

Output facilities are those which transfer data out of the computer in the form of text, images, sounds etc to a display screen, printer, storage device, etc.

Hard disks, USB disks, floppies act as both input and output facilities.

Processing facilities primarily refers to the Central Processing Unit (CPU) of a computer. Referred to as the "brain" of the computer, the CPU processes instructions and data.

Storage facilities include hard disks and other data storage facilities. This term would also include the physical cabinet in which a computer is housed.

Computer software facilities refer to the operating system and application software that are essential for a computer to function in a useful manner.

Communication facilities include the network interface cards, modems and other devices that enable a computer to communicate with other computers.

Illustration: Considering the wide definition given to the term computer by the IT Act the following are examples of "computers": (1) desktop personal computers (2) mobile phones (3) microwave ovens (4) computer printers (4) scanners (5) installed computer software (6) Automatic Teller Machine (ATM) (7) "smart" homes which can be controlled through the Internet.

Case Law: Diebold Systems Pvt Ltd vs. Commissioner of Commercial Taxes ILR 2005 KAR 2210, [2006] 144 STC 59(Kar)

In an interesting case, the Karnataka High Court laid down that ATMs are not computers, but are electronic devices under the Karnataka Sales Tax Act, 1957.

Diebold Systems Pvt Ltd [a manufacturer and supplier of Automated Teller Machines (ATM)] had sought a clarification from the Advance Ruling Authority (ARA) in Karnataka on the rate of tax applicable under the Karnataka Sales Tax Act, 1957 on sale of ATMs.

The majority view of the ARA was to classify ATMs as "computer terminals" liable for 4% basic tax as they would fall under Entry 20(ii)(b) of Part 'C' of Second Schedule to the Karnataka Sales Tax Act.

The Chairman of the ARA dissented from the majority view. In his opinion, ATMs would fit into the description of electronic goods, parts and accessories thereof. They would thus attract 12% basic tax and would fall under Entry 4 of Part 'E' of the Second Schedule to the KST Act.

The Commissioner of Commercial Taxes was of the view that the ARA ruling was erroneous and passed an order that ATMs cannot be classified as computer terminals.

The High Court of Karnataka acknowledged that the IT Act provided an enlarged definition of "computers". However, the Court held that such a wide definition could not be used for interpreting a taxation related law such as the Karnataka Sales Tax Act, 1957.

The High Court also said that an ATM is not a computer by itself and it is connected to a computer that performs the tasks requested by the persons using the ATM. The computer is connected electronically to many ATMs that may be located at some distance from the computer.

MALAYSIA:

A relevant provision is section 2(2) of the *Computer Crimes Act*, which states-

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

SINGAPORE:

A relevant provision is section 2(1) of the *Computer Misuse Act*, which states-

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —

(a) an automated typewriter or typesetter;

(b) a portable hand-held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may, by notification in the Gazette, prescribe;

(j) "computer network" means the inter-connection of one or more computers or computer systems or communication device through –

(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the inter-connection is continuously maintained;¹⁸ COMMENTS:

Simply put, a computer network is the interconnection of one or more computers or computer systems or devices through:

(1) **Satellite**: Satellite Internet connection is an arrangement in which the outgoing and incoming data travels through a satellite. Each subscriber's hardware includes a satellite dish antenna and a transceiver (transmitter / receiver). The dish antenna transmits and receives signals.

(2) **Microwave**: The term microwave refers to electromagnetic waves of a particular frequency. Microwave frequencies are used in radars, Bluetooth devices, radio astronomy, GSM mobile phone networks, broadcasting and telecommunication transmissions etc.

(3) **Terrestrial line**: Terrestrial lines include fibre optic cables, telephone lines, etc.

(4) **Other communication media**: Communication media refers to any instrument or means that facilitates the transfer of data, as between a

¹⁸ Substituted by Information Technology (Amendment) Act, 2008 for: "computer network" means the inter-connection of one or more computers through- (i) the use of satellite, microwave, terrestrial line or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

computer and peripherals or between two computers. Other ways in which computers can be connected include cables, hubs, switches, etc.

UNITED STATES OF AMERICA:

Case Law: Reno v. ACLU [521 U.S. 844, 117 S.Ct. 2329, 138 L.Ed.2d 874, 884 (1997)]

This was probably the first judgment of a Supreme Court in the world wherein the meaning of the Internet and related technologies was discussed in great detail. The following is an extract of the judgment of the Court:

The Internet

The Internet is an international network of interconnected computers. It is the outgrowth of what began in 1969 as a military program called "ARPANET," [An acronym for the network developed by the Advanced Research Project Agency] which was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is "a unique and wholly new medium of worldwide human communication."

The Internet has experienced "extraordinary growth." The number of "host" computers—those that store information and relay communications—increased from about 300 in 1981 to approximately 9,400,000 by the time of the trial in 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet at the time of trial, a number that is expected to mushroom to 200 million by 1999.

Individuals can obtain access to the Internet from many different sources, generally hosts themselves or entities with a host affiliation. Most colleges and universities provide access for their students and faculty; many corporations provide their employees with access through an office network; many communities and local libraries provide free access; and an increasing number of storefront "computer coffee shops" provide access for a small hourly fee. Several major national "online services" such as America Online, CompuServe, the Microsoft Network, and Prodigy offer access to their own extensive proprietary networks as well as a link to the much larger resources of the Internet. These commercial online services had almost 12 million individual subscribers at the time of trial.

Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail (e-mail), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium-known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet. E-mail enables an individual to send an electronic message-generally akin to a note or letter-to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt. A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers. Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day. In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real-time dialogue—in other words, by typing messages to one another that appear almost immediately on the others' computer screens. The District Court found that at any given time "tens of thousands of users are engaging in conversations on a huge range of subjects." It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought." The best known category of communication over the Internet is the World Wide Web, which

allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web "pages," are also prevalent. Each has its own address—"rather like a telephone number."

Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or "site's") author. They generally also contain "links" to other documents created by that site's author or to other (generally) related sites. Typically, the links are either blue or underlined text—sometimes images. Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links.

Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. "Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal 'home pages,' the equivalent of individualized newsletters about that person or organization, which are available to everyone on the Web."]

Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web."

(k) "computer resources" means computer, computer system, computer network, data, computer data base or software;

(I) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

COMMENTS:

Simply put, a computer system has the following characteristics: (1) it is a device or collection of devices which contain data or programs, (2) it performs functions such as logic, storage, arithmetic etc, (3) it includes input and output support systems, (4) it excludes non-programmable calculators.

UNITED STATES OF AMERICA:

Case Law: State of Pennsylvania v. Murgallis [No. 189 MDA 1999 (Pa. Super.Ct., June 2, 200)].

In this judgment, it was held that the Internet falls under the definition of computer system and the use of email is accessing a computer.

CONVENTION ON CYBERCRIME:

According to Article 1(a) of the *Convention on Cybercrime* of the Council of Europe, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber Appellate Tribunal¹⁹ established under sub-section (1) of section 48;

(na) "Cyber café" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public;²⁰

"cyber protecting (nb) security" means information. equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, disclosure, disruption, use, modification or destruction;²¹

(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

SINGAPORE:

A relevant provision is section 2(1) of the *Computer Misuse Act*, which defines *data* as representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer.

MALAYSIA:

A relevant provision is section 2(2) of the *Computer Crimes Act*, which defines *data* as representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer.

¹⁹ The words "Cyber Appellate Tribunal" substituted for "Cyber Regulations Appellate Tribunal" by Information Technology (Amendment) Act, 2008.

²⁰ Inserted by Information Technology (Amendment) Act, 2008.

²¹ Inserted by Information Technology (Amendment) Act, 2008.

CONVENTION ON CYBERCRIME:

According to article 1(b) of the *Convention on Cybercrime* of the Council of Europe, "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

(p) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

COMMENTS:

Simply put, a person can authenticate a document by affixing his digital signature. Let us take a simple illustration to understand how digital signatures work.

Illustration: Sanya uses her computer to generate a public and private key pair. Simply put, these keys are very large numbers.

She then stores her private key very securely on her computer. She uploads her public key to the website of a licensed certifying authority. She also couriers a filled in application form and photocopies of her passport and Income Tax PAN card to the certifying authority.

After following some verification procedures, the certifying authority sends Sanya a hardware device by post. This device contains Sanya's digital signature certificate. The digital signature certificate contains Sanya's public key along with some information about her and the certifying authority.

Sanya then has to accept her digital signature certificate.

Each certifying authority stores digital signature certificates issued by it in an online repository.

In order to digitally sign an electronic record, Sanya uses her private key.

In order to verify the digital signature, any person can use Sanya's public key (which is contained in her digital signature certificate).

In case Sanya had originally generated her private key on a smart card or USB Crypto Token, then the subsequent signatures created by her would be secure digital signatures.

Note: The smart card / crypto token have a chip built into it, which has crypto modules to enable the signing operation to happen in the device itself. The private key does not come out of the device in its original form.

In case Sanya had generated and stored her private key on a hard disk, floppy, CD, pen drive, etc, then subsequent signatures are not secure digital signatures.

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35;

COMMENTS:

Simply put, a digital signature certificate contains a public key as "certified" by a Certifying Authority (CA).

Let us take a simple illustration. Rohas Nagpal wants to digitally sign emails and electronic contracts. The first step he would take is to generate a private-public key pair. Once he has done that, he can use his private key to sign contracts etc. Anyone can use Mr. Nagpal's public key to verify his signature. That's where the problem begins.

How can anyone be sure which is Mr. Nagpal's public key? What if Mr. Nagpal denies that a particular public key is actually his? To solve this problem digital signature certificates are used.

Mr. Nagpal would apply to a licenced CA for a digital signature certificate. As part of the application process he would submit identification documents (such as passport, PAN card etc). He would also send his public key to the CA. The CA would then "certify" the public key as belonging to Mr. Nagpal and issue a digital signature certificate that contains Mr. Nagpal's public key along with information identifying him.

Let us now discuss the contents of a digital signature certificate in detail. For the purposes of this discussion we will discuss the digital signature certificate issued to Mr. Rohas Nagpal by the TCS CA.

To view digital signature certificates stored by default on your computer, you can open up the Microsoft Internet Explorer program and click on Tools \rightarrow Internet Options \rightarrow Content \rightarrow Certificates option.

To make this section easy to understand, the language used is in the first person. References to "I", "me", etc refer to "Rohas Nagpal", the author of this book.

Let us discuss my digital signature certificate (DSC) in detail. I have been issued a DSC by TCS CA which is licenced by the Controller of Certifying Authorities of India. The DSC has been imported into my personal computer that also has the Microsoft Internet Explorer program installed.

To view my DSC, I first open up the Microsoft Internet Explorer program and click on Tools \rightarrow Internet Options \rightarrow Content \rightarrow Certificates option.



The first view of the DSC displays the **Certificate Information** which contains the following basic information: (1) Purposes for which the certificate is intended (2) Person to whom it is issued (3) Issuer of the certificate (4) Validity period of the certificate.

As can be seen from figure 1, the certificate is intended to do the following: (1) Prove my identity to another computer (2) Protect email messages.

The certificate is issued to me by Tata Consultancy Services Certifying Authority (TCS CA) and is valid from 20^{th} November 2007 to 19^{th} November 2008.

Please notice that the DSC states that "You have a private key that corresponds to this certificate". This is because the DSC is on my personal computer and my private key is also on this computer. If you were to download my DSC onto your computer, then this statement would not show up as your computer does not have my private key.

Clicking on the "Issuer Statement" button on the DSC opens up the Relying Party Agreement from the TCS website.

The Relying Party Agreement is an agreement between TCS CA and the person relying on a DSC (or verifying a DSC). The agreement must be read along with the TCS-CA trust network certification practice statement (CPS) posted at the TCS-CA web site (<u>https://www.tcs-ca.tcs.co.in</u>) as amended from time to time.

Clicking on the **Details** tab, displays the certificate details.

Certificate	?×
General Details Certification Path	
Show: <all></all>	
Field Value	
Version V3 Serial number 03 59 aa Signature algorithm sha1R5A Issuer AP, admin@tcs-ca.tcs.co.in, H. Valid from Tuesday, November 20, 2007 Valid to Wednesday, November 19, 20 Subject rn@asianlaws.org, IN, Mahara Public key R5A (1024 Bits)	
30 81 89 02 81 81 00 c6 ab ce c5 33 61 a9 09 94 3a a5 24 51 ff df 6e 10 1e 70 a8 ac d4 fd 63 8e 26 d7 51 52 54 80 1c 51 64 cd 2f 70 9a 6d f2 c6 f5 54 49 ca b5 00 86 cc	
99 be f7 be 89 8d 9e 0f 59 4f 70 b6 98 5d 63 c9 37 09 6d c9 94 ac d7 82 d3 45 99 f6 50 87 4d 47 f2 07 7a 88 e7 ef dc 13 d4 54 f3 73 07 ad 93 68 19 32 f0 a0 6b b7 bb 86 19 2b 43 6f 3f 2a 13 61 ac 5f 02 1a 1b d5	 •
Edit Properties	
	ок

The following are some of the details of the certificate:

- 1. Version: This is stated as V3. This signifies that the DSC is based on the X509 version 3 technology standards.
- 2. Serial number: The serial number is a positive integer assigned by the CA to each DSC issued by it. This number is unique for each DSC issued by the CA.

Note: "03 59 aa" is a hexadecimal number that corresponds to the decimal number 50696362.

- 3. **Signature Algorithm:** This field identifies the mathematical algorithm used by the CA to sign the certificate [sha1RSA is this case]. *sha1* stands for Secure Hash Algorithm 1 while *RSA* stands for Rivest Shamir Adleman.
- 4. **Issuer:** This field identifies the CA who has issued this DSC. The table below summarizes the information as contained in the

DSC and the brief explanation of what that information stands for.

Information on DSC	Explanation
S = AP	State = Andhra Pradesh
E = admin@tcs-ca.tcs.co.in	Email = admin@tcs-ca.tcs.co.in
L = Hyderabad	Location = Hyderabad
CN = Tata Consultancy Services Certifying Authority	Common Name = Tata Consultancy Services Certifying Authority
OU = TCS CA	Organizational-unit = TCS CA,
O = India PKI	Organization = India PKI
C = IN	Country = India

- 5. Valid From: This indicates that the DSC is valid from 11:31:07 AM on Tuesday, November 20, 2007.
- 6. Valid To: This indicates that the DSC is valid till 11:31:07 AM on November 19, 2008.
- 7. **Subject:** The subject field identifies the person to whom this DSC has been issued by the CA Rohas Nagpal in this case. The table below summarizes the information as contained in the DSC and the brief explanation of what that information stands for.

Information on DSC	Explanation
E = rn@asianlaws.org	Email = rn@asianlaws.org
C = IN	Country = India
S = Maharashtra	State = Maharashtra
L = Pune	Location = Pune
O = Tata Consultancy Services - Certifying Authority	Organisation = Tata Consultancy Services - Certifying Authority
OU = Class 3 Certificate	Organization Unit = Class 3 Certificate ²²
OU = Individual - Others	Organization Unit = Individual - Others ²³

²² Class-3 Certificates are legally recognized digital signatures as per the IT Act, 2000.

OU = TCS-CA - Registration	Organization Unit = TCS-CA -
Authority	Registration Authority
CN = Rohas Nagpal	Common Name= Rohas Nagpal

8. **Public Key:** This field specifies my public key (see below), the algorithm used by me to generate the key (RSA) and the key size (1024 bits).

 30
 81
 89
 02
 81
 81
 00
 c6
 ab
 ce
 c5
 33
 61
 a9
 09
 94
 3a
 a5
 24
 51
 ff

 df
 6e
 10
 1e
 70
 a8
 ac
 d4
 fd
 63
 8e
 26
 d7
 51
 52
 54
 80
 1c
 51
 64
 cd

 2f
 70
 9a
 6d
 f2
 c6
 f5
 54
 49
 ca
 b5
 00
 86
 cc
 99
 be
 f7
 be
 89
 8d
 9e
 0f
 59
 4f
 70
 b6
 98
 5d
 63
 c9
 37
 09
 6d
 c2
 93
 45
 99
 f6

 50
 87
 4d
 47
 f2
 07
 7a
 88
 e7
 ef
 dc
 13
 d4
 54
 73
 07
 ad
 93
 68
 19

 32
 f0
 a0
 6b
 b7
 bb
 86
 19

9. **CRL Distribution Points:** A certificate revocation list (CRL) is a list of serial numbers of those digital signature certificates which should not be relied upon because they: (1) have been revoked, or (2) are no longer valid. This field indicates the URL from where the relevant Certification Revocation List can be downloaded, which in this case is- <u>http://www.tcs-</u> ca.tcs.co.in/crl 2785.crl

Clicking on the **Certification Path** tab, displays the certification path. This shows that my digital signature certificate has been issued by TCS CA. It also shows that the TCS CA digital signature certificate has been issued by the Controller of Certifying Authorities.

(r)"electronic form", with reference to information means, any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means Official Gazette published in the electronic form;

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

²³ The basic options are Company user, Government user and Individual user. Under Individual user the options are Banking, Government and Others.

(ta) "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;²⁴

COMMENTS:

The term electronic signature has been discussed at length in the UNCITRAL publication titled *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods*, para 15 and 16 of which are quoted below:

15. The terms "electronic authentication" and "electronic signature" are used to refer to various techniques currently available on the market or still under development for the purpose of replicating in an electronic environment some or all of the functions identified as characteristic of handwritten signatures or other traditional authentication methods.

16. A number of different electronic signature techniques have been developed over the years. Each technique aims at satisfying different needs and providing different levels of security, and entails different technical requirements. Electronic authentication and signature methods may be classified in three categories: those based on the knowledge of the user or the recipient (e.g. passwords, personal identification numbers (PINs)), those based on the physical features of the user (e.g. biometrics) and those based on the possession of an object by the user (e.g. codes or other information stored on a magnetic card). A fourth category might include various types of authentication and signature methods that, without falling under any of the above categories, might also be used to indicate the originator of an electronic communication (such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message). Technologies currently in use include digital signatures within a public key infrastructure (PKI), biometric devices, PINs, userdefined or assigned passwords, scanned handwritten signatures, signature by means of a digital pen, and clickable "OK" or "I accept" boxes. Hybrid solutions based on a combination of different technologies are becoming increasingly popular, such as, for instance, in the case of the combined use of passwords and

²⁴ Inserted by Information Technology (Amendment) Act, 2008.

transport layer security/secure sockets layer (TLS/SSL), which is a technology using a mix of public and symmetric key encryptions.

(tb) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate;²⁵

(u) "function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and retrieval and communication or telecommunication from or within a computer;

MALAYSIA:

A relevant provision is section 2(2) of the *Computer Crimes Act*, which defines *function* as "includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer";

SINGAPORE:

A relevant provision is section 2(1) of the *Computer Misuse Act*, which defines *function* as includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

(ua) "Indian Computer Emergency Response Team" means an agency established under sub-section (1) of section 70B;²⁶

(v) "information" includes data, message²⁷, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

(w) "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

²⁵ Inserted by Information Technology (Amendment) Act, 2008.

²⁶ Inserted by Information Technology (Amendment) Act, 2008.

²⁷ The word "message" inserted by Information Technology (Amendment) Act, 2008.

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;²⁸

COMMENTS:

According to Article 2(e) of the UNCITRAL Model Law on Electronic Commerce, "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message.

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this term, as quoted below:

38. The focus of the Model Law is on the relationship between the originator and the addressee, and not on the relationship between either the originator or the addressee and any intermediary. However, the Model Law does not ignore the paramount importance of intermediaries in the field of electronic communications. In addition, the notion of "intermediary" is needed in the Model Law to establish the necessary distinction between originators or addressees and third parties.

39. The definition of "intermediary" is intended to cover both professional and non-professional intermediaries, i.e., any person (other than the originator and the addressee) who performs any of the functions of an intermediary. The main functions of an intermediary are listed in subparagraph (e), namely receiving, transmitting or storing data messages on behalf of another person. Additional "value-added services" may be performed by network operators and other intermediaries, such as formatting, translating, recording, authenticating, certifying and preserving data messages and providing security services for electronic transactions.

"Intermediary" under the Model Law is defined not as a generic category but with respect to each data message, thus recognizing that the same person could be the originator or addressee of one data message and an intermediary with respect to another data message. The Model Law, which is focused on the relationships

²⁸ Substituted by Information Technology (Amendment) Act, 2008 for: "intermediary" with respect to any particular electronic message, means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

between originators and addressees, does not, in general, deal with the rights and obligations of intermediaries.

CONVENTION ON CYBERCRIME:

According to Article 1(c) of the *Convention on Cybercrime* of the Council of Europe, "service provider" means:

(i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

(ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service;

(x) "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y)"law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be, Regulations made by the President under Article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of Article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

(z)"licence" means a licence granted to a Certifying Authority under section 24;

(za) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

COMMENTS:

According to Article 2(b) of the UNCITRAL Model Law on Electronic Commerce, (c) "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this term, as quoted below: 37. The definition of "originator" should cover not only the situation where information is generated and communicated, but also the situation where such information is generated and stored without being communicated. However, the definition of "originator" is intended to eliminate the possibility that a recipient who merely stores a data message might be regarded as an originator.

(zb) "prescribed" means prescribed by rules made under this Act;

(zc) "private key" means the key of a key pair used to create a digital signature;

(zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

COMMENTS:

The term "Public and private keys" has been discussed at length in the UNCITRAL publication titled *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods*, para 27 of which is quoted below:

27. A complementary key used for digital signatures is named the "private key", which is used only by the signatory to create the digital signature and should be kept secret, while the "public key" is ordinarily more widely known and is used by a relying party to verify the digital signature. The private key is likely to be kept on a smart card or to be accessible through a personal identification number (PIN) or a biometric identification device, such as thumbprint recognition. If many people need to verify the signatory's digital signature, the public key must be available or distributed to all of them, for example by attaching the certificates to the signature or by other means that ensure that the relying parties, and only those who have to verify the signatures, can obtain the related certificates. Although the keys of the pair are mathematically related, if an asymmetric cryptosystem has been designed and implemented securely it is virtually impossible to derive the private key from knowledge of the public key. The most common algorithms for encryption through the use of public and private keys are based on an important feature of large prime numbers: once they are multiplied together to produce a new number, it is particularly difficult and time-consuming to determine which two prime numbers created that new, larger number. Thus, although many people may know the public key of a given signatory and use it to verify that signatory's signature, they cannot discover that signatory's private key and use it to forge digital signatures.

(ze) "secure system" means computer hardware, software and procedure that-

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

(zf) "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg) "subscriber" means a person in whose name the Electronic Signature²⁹ Certificate is issued;

(zh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether-

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

COMMENTS:

The term "Verification of digital signature" has been discussed at length in the UNCITRAL publication titled *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods*, para 30 and 31 of which are quoted below:

²⁹ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

30. Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key. Verification of a digital signature is accomplished by computing a new hash result for the original message, by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks whether the digital signature was created using the corresponding private key and whether the newly computed hash result matches the original hash result that was transformed into the digital signature during the signing process.

31. The verification software will confirm the digital signature as "verified" from a cryptographic viewpoint if (a) the signatory's private key was used to sign digitally the message, which is known to be the case if the signatory's public key was used to verify the signature because the signatory's public key will verify only a digital signature created with the signatory's private key; and (b) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER – II DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE³⁰

3. Authentication of electronic records.

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

³⁰ Substituted for "DIGITAL SIGNATURE" by Information Technology (Amendment) Act, 2008.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation - For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

COMMENTS:

Subscriber is a person in whose name the Digital Signature Certificate is issued. *Authenticate* means "to give legal validity to", "establish the genuineness of".

Illustration: Pooja has issued a certificate stating that Sameer has been employed in her company for 3 years. Pooja affixes her digital signature to this certificate. Pooja has authenticated the certificate.

Electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

Affixing digital signature means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

Asymmetric crypto system is a system of using mathematically related keys to create and verify digital signatures. The key pair consists of a *private key* and a *public key*. The private key pair is used in conjunction with a one-way hash function to create digital signatures. The public key is used to verify the digital signatures created by the corresponding private key.

A one-way *hash function* takes variable-length input – say, a message of any length – and produces a fixed-length output; say, 160-bits. The hash function ensures that, if the information is changed in any way – even by just one bit – an entirely different output value is produced.

In interpreting this provision, the term "digital signature" must not be compared to "signature" in the conventional sense. This is because although a person usually has one conventional handwritten signature for all messages, he will have a different digital signature for every message that he signs.

Illustration: Mr. Sen writes a message as under:

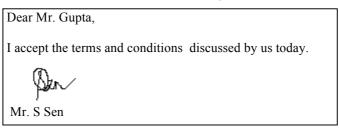


Figure 1: Conventionally signed message Here, Mr. Sen's signature is as marked in the above message. Every document he signs will bear this signature. However, his digital signature for this message could be

iQA/AwUBO0BCsFPnhMicaZh0EQJllgCgt1q
tfqazO2ppYNdZN685h2QtYQsAoOgZ
eH3gqHf5Tisz1C7tzvHC09zx
=g/BR

Figure 2: Digital Signature

Although his digital signature for the message in Figure 1 is as shown in Figure 2, his digital signature for any and every other message will be different. E.g. if he changes the word "today" in the message in Figure 1 to "yesterday", his digital signature for the new message could be:

iQA/AwUBO0BDdlPnhMicaZh0EQIOBQCgi u0vAT47Q7VJsgeQYWU69OtV+MMAoL77 2XDQBvzPYOKSWDS6wjucho1T =TSAn

Figure 3: New Digital Signature

What the law implies here is that a person may authenticate an electronic record by means of a digital signature, which is unique to the message being digitally signed.

The public key and private key are basically two very large numbers that are mathematically related to each other. If a particular private key was used to "sign" a message, then only the corresponding public key will be able to verify the "signature".

The law also lays down that the private key and public key are unique to each subscriber. This implies that no two subscribers should have the same public and private key pair. This is practically achieved by using very large numbers (hundreds of digits) as keys. The probability of two persons generating the same key pair is thus extremely remote.

3A. Electronic Signature³¹

(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which –

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if –

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

³¹ Inserted by Information Technology (Amendment) Act, 2008.

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfils such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule:

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.

COMMENTS:

The Information Technology Act, 2000 took a "technology dependent" approach to the issue of electronic authentication. This was done by specifying digital signatures as the means of authentication. Digital signatures are one type of technology coming under the wider term "electronic signatures".

The defect in this approach is that the law is bound by a specific technology, which in due course of time may be proven weak. The advantage of using a technology neutral approach is that if one technology is proven weak, others can be used without any legal complexities arising out of the issue.

An example of this is the MD5 hash algorithm that at one time was considered suitable. MD5 was prescribed as suitable by Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000³².

³² "Rule 6. Standards.—The Information Technology (IT) architecture for Certifying Authorities may support open standards and accepted de facto standards; the most important standards that may be considered for different

MD5 was subsequently proven weak by mathematicians. In fact, Asian School of Cyber Laws had filed a Public Interest Litigation (PIL) in the Bombay High Court on the same issue.

Subsequently, the Information Technology (Certifying Authorities) Amendment Rules, 2009³³ amended the Rule 6 mentioned above and MD5 was replaced by SHA-2.

The Information Technology (Amendment) Act, 2008 amends the technology dependent approach and introduces the concept of electronic signatures in addition to digital signatures.

CHAPTER – III ELECTRONIC GOVERNANCE

4. Legal recognition of electronic records.

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

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference. COMMENTS:

This section is based upon Article 5 of the UNCITRAL Model Law on Electronic Commerce, titled "Legal recognition of data messages". The Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce elaborates upon this provision, as quoted below:

46. Article 5 embodies the fundamental principle that data messages should not be discriminated against, i.e., that there should be no disparity of treatment between data messages and paper documents. It is intended to apply notwithstanding any statutory requirements for a "writing" or an original. That fundamental principle is intended to find general application and its scope should not be limited to evidence or other matters covered in chapter II. It should be noted, however, that such a principle is not intended to override any of the requirements

activities associated with the Certifying Authority's functions are as under:.....Digital Hash Function: MD5 and SHA-1.

³³ Gazette notification dated 5th August, 2009 issued by the Department of Information Technology, Ministry of Communications and Information Technology.

contained in articles 6 to 10. By stating that "information shall not be denied legal effectiveness, validity or enforceability solely on the grounds that it is in the form of a data message", article 5 merely indicates that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability. However, article 5 should not be misinterpreted as establishing the legal validity of any given data message or of any information contained therein.

46-1. Article 5 bis was adopted by the Commission at its thirtyfirst session, in June 1998. It is intended to provide guidance as to how legislation aimed at facilitating the use of electronic commerce might deal with the situation where certain terms and conditions, although not stated in full but merely referred to in a data message, might need to be recognized as having the same degree of legal effectiveness as if they had been fully stated in the text of that data message. Such recognition is acceptable under the laws of many States with respect to conventional paper communications, usually with some rules of law providing safeguards, for example rules on consumer protection. The expression "incorporation by reference" is often used as a concise means of describing situations where a document refers generically to provisions which are detailed elsewhere, rather than reproducing them in full.

46-2. In an electronic environment, incorporation by reference is often regarded as essential to widespread use of electronic data interchange (EDI), electronic mail, digital certificates and other forms of electronic commerce. For example, electronic communications are typically structured in such a way that large numbers of messages are exchanged, with each message containing brief information, and relying much more frequently than paper documents on reference to information accessible elsewhere. In electronic communications, practitioners should not have imposed upon them an obligation to overload their data messages with quantities of free text when they can take advantage of extrinsic sources of information, such as databases, code lists or glossaries, by making use of abbreviations, codes and other references to such information.

46-3. Standards for incorporating data messages by reference into other data messages may also be essential to the use of public key certificates, because these certificates are generally brief records with rigidly prescribed contents that are finite in size. The trusted third party which issues the certificate, however, is likely to require the inclusion of relevant contractual terms limiting its liability. The scope, purpose and effect of a certificate in commercial practice, therefore, would be ambiguous and uncertain without external terms being incorporated by reference. This is the case especially in the context of international communications involving diverse parties who follow varied trade practices and customs.

46-4. The establishment of standards for incorporating data messages by reference into other data messages is critical to the growth of a computer-based trade infrastructure. Without the legal certainty fostered by such standards, there might be a significant risk that the application of traditional tests for determining the enforceability of terms that seek to be incorporated by reference might be ineffective when applied to corresponding electronic commerce terms because of the differences between traditional and electronic commerce mechanisms.

46-5. While electronic commerce relies heavily on the mechanism of incorporation by reference, the accessibility of the full text of the information being referred to may be considerably improved by the use of electronic communications. For example, a message may have embedded in it uniform resource locators (URLs), which direct the reader to the referenced document. Such URLs can provide "hypertext links" allowing the reader to use a pointing device (such as a mouse) to select a key word associated with a URL. The referenced text would then be displayed. In assessing the accessibility of the referenced text, factors to be considered may include: availability (hours of operation of the repository and ease of access); cost of access; integrity (verification of content, authentication of sender, and mechanism for communication error correction); and the extent to which that term is subject to later amendment (notice of updates; notice of policy of amendment).

46-6. One aim of article 5 bis is to facilitate incorporation by reference in an electronic context by removing the uncertainty prevailing in many jurisdictions as to whether the provisions dealing with traditional incorporation by reference are applicable to incorporation by reference in an electronic environment. However, in enacting article 5 bis, attention should be given to avoid introducing more restrictive requirements with respect to incorporation by reference in electronic commerce than might already apply in paper-based trade.

46-7. Another aim of the provision is to recognize that consumer protection or other national or international law of a mandatory nature (e.g., rules protecting weaker parties in the context of contracts of adhesion) should not be interfered with. That result could also be achieved by validating incorporation by reference in an electronic environment "to the extent permitted by law", or by listing the rules of law that remain unaffected by article 5 bis. Article 5 bis is not to be interpreted as creating a specific legal regime for incorporation by reference in an electronic environment. Rather, by establishing a principle of nondiscrimination, it is to be construed as making the domestic rules applicable to incorporation by reference in a paper-based environment equally applicable to incorporation by reference for the purposes of electronic commerce. For example, in a number of jurisdictions, existing rules of mandatory law only validate incorporation by reference provided that the following three conditions are met: (a) the reference clause should be inserted in the data message; (b) the document being referred to, e.g., general terms and conditions, should actually be known to the party against whom the reference document might be relied upon; and (c) the reference document should be accepted, in addition to being known, by that party.

5. Legal recognition of electronic signatures³⁴.-

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature³⁵ affixed in such manner as may be prescribed by the Central Government.

Explanation- For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, means affixing of his hand written

³⁴ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

³⁵ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

signature or any mark on any document and the expression "signature" shall be construed accordingly.

COMMENTS:

Para 2, Introduction to the UNCITRAL publication titled *Promoting* confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods, states:

The relevancy of a document as a piece of evidence is established by connecting it with a person, place or thing, a process which in some common law jurisdictions is known as "authentication". [Farm Credit Bank of St. Paul v. William G. Huether, 12th April 1990 (454 N.W.2d 710, 713) (United States, Supreme Court of North Dakota, North Western Reporter).]

Signing a document is a common—albeit not exclusive—means of "authentication", and, depending on the context, the terms "to sign" and "to authenticate" may be used as synonyms. In the context of the revised article 9 of the United States Uniform Commercial Code, for example, "authenticate" is defined as "(A) to sign; or (B) to execute or otherwise adopt a symbol, or encrypt or similarly process a record in whole or in part, with the present intent of the authenticating person to identify the person and adopt or accept a record".

6. Use of electronic records and digital signatures in Government and its agencies.-

(1) Where any law provides for-

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

COMMENTS:

Rule 3 of the Information Technology (Use of electronic records and digital signatures) Rules, 2004 is relevant to this issue and states-

3. Filing of form, application or any other document:-

Any form, application or any other document referred to in clause (a) of sub-section (1) of section 6 of the Act may be filed with any office, authority, body or agency owned or controlled by the appropriate Government using the software specified by it and such office, authority, body or agency shall, while generating such software, take into account the following features of the electronic record, namely:-

- (a) life time;
- (b) preservability;
- (c) accessibility;
- (d) readability;
- (e) comprehensibility in respect of linked information;
- (f) evidentiary value in terms of authenticity and integrity;
- (g) controlled destructibility; and
- (h) augmentability.

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

COMMENTS:

Rule 4 of the Information Technology (Use of electronic records and digital signatures) Rules, 2004 is relevant to this issue and states-

4. Issue or grant of any licence, permit, sanction or approval:-

Any licence, permit, sanction or approval whatever name called referred to in clause (b) of sub-section (1) of section 6 of the Act may be issued or granted by using the software specified under rule 3.

(c) the receipt or payment of money in a particular manner,

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe-

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

COMMENTS:

Rule 5 of the Information Technology (Use of electronic records and digital signatures) Rules, 2004 is relevant to this issue and states-

5. Payment and receipt of fee or charges:-

The payment of receipt of any fee or charges for filing, creation or issue of any electronic record under clause (a) of sub-section (2) of section 6 of the Act may be made in a cheque in the electronic form.

"A cheque in the electronic form" has the meaning assigned to it in clause (a) of Explanation 1 to section 6 of the Negotiable Instrument Act, 1881.

6A. Delivery of services by service provider³⁶.-

(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorise, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify by notification in the Official Gazette.

Explanation – For the purposes of this section, service provider so authorised includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(2) The appropriate Government may also authorise any service provider authorised under sub-section (1) to collect, retain and appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(3) Subject to the provisions of sub-section (2), the appropriate Government may authorise the service providers

³⁶ Inserted by Information Technology (Amendment) Act, 2008.

to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.

7. Retention of electronic records.-

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if-

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

COMMENTS:

This section is based upon Article 10 of the UNCITRAL Model Law on Electronic Commerce, titled "Retention of data messages", quoted below:

Article 10. Retention of data messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this provision, as quoted below:

72. Article 10 establishes a set of alternative rules for existing requirements regarding the storage of information (e.g., for accounting or tax purposes) that may constitute obstacles to the development of modern trade.

73. Paragraph (1) is intended to set out the conditions under which the obligation to store data messages that might exist under the applicable law would be met. Subparagraph (a) reproduces the conditions established under article 6 for a data message to satisfy a rule which prescribes the presentation of a "writing".

Subparagraph (b) emphasizes that the message does not need to be retained unaltered as long as the information stored accurately reflects the data message as it was sent. It would not be appropriate to require that information should be stored unaltered, since usually messages are decoded, compressed or converted in order to be stored.

74. Subparagraph (c) is intended to cover all the information that may need to be stored, which includes, apart from the message itself, certain transmittal information that may be necessary for the identification of the message. Subparagraph (c), by imposing the

retention of the transmittal information associated with the data message, is creating a standard that is higher than most standards existing under national laws as to the storage of paper-based communications. However, it should not be understood as imposing an obligation to retain transmittal information additional to the information contained in the data message when it was generated, stored or transmitted, or information contained in a separate data message, such as an acknowledgement of receipt. Moreover, while some transmittal information is important and has to be stored, other transmittal information can be exempted without the integrity of the data message being compromised. That is the reason why subparagraph (c) establishes a distinction between those elements of transmittal information that are important for the identification of the message and the very few elements of transmittal information covered in paragraph (2) (e.g., communication protocols), which are of no value with regard to the data message and which, typically, would automatically be stripped out of an incoming data message by the receiving computer before the data message actually entered the information system of the addressee.

75. In practice, storage of information, and especially storage of transmittal information, may often be carried out by someone other than the originator or the addressee, such as an intermediary. Nevertheless, it is intended that the person obligated to retain certain transmittal information cannot escape meeting that obligation simply because, for example, the communications system operated by that other person does not retain the required information. This is intended to discourage bad practice or wilful misconduct. Paragraph (3) provides that in meeting its obligations under paragraph (1), an addressee or originator may use the services of any third party, not just an intermediary.

7A. Audit of documents, etc., maintained in electronic form.³⁷

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in the electronic form.

³⁷ Inserted by Information Technology (Amendment) Act, 2008.

8. Publication of rule, regulation, etc., in Electronic Gazette.

Where any law provides that any rule, regulation, order, byelaw, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, by-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to make rules by Central Government in respect of electronic signature³⁸

The Central Government may, for the purposes of this Act, by rules, prescribe-

(a) the type of electronic signature³⁹;

(b) the manner and format in which the electronic signature⁴⁰ shall be affixed;

³⁸ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

³⁹ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁴⁰ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

(c) the manner or procedure which facilitates identification of the person affixing the electronic signature⁴¹;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to electronic signatures 42 .

10A. Validity of contracts formed through electronic means.⁴³

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

COMMENTS:

This section is based upon Article 11 of the UNCITRAL Model Law on Electronic Commerce, titled "Formation and validity of contracts", quoted below:

Article 11. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following: [...].

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this provision, as quoted below:

⁴¹ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁴² The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁴³ Inserted by Information Technology (Amendment) Act, 2008.

76. Article 11 is not intended to interfere with the law on formation of contracts but rather to promote international trade by providing increased legal certainty as to the conclusion of contracts by electronic means. It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed. In certain countries, a provision along the lines of paragraph (1) might be regarded as merely stating the obvious, namely that an offer and an acceptance, as any other expression of will, can be communicated by any means, including data messages. However, the provision is needed in view of the remaining uncertainties in a considerable number of countries as to whether contracts can validly be concluded by electronic means. Such uncertainties may stem from the fact that, in certain cases, the data messages expressing offer and acceptance are generated by computers without immediate human intervention, thus raising doubts as to the expression of intent by the parties. Another reason for such uncertainties is inherent in the mode of communication and results from the absence of a paper document.

77. It may also be noted that paragraph (1) reinforces, in the context of contract formation, a principle already embodied in other articles of the Model Law, such as articles 5, 9 and 13, all of which establish the legal effectiveness of data messages. However, paragraph (1) is needed since the fact that electronic messages may have legal value as evidence and produce a number of effects, including those provided in articles 9 and 13, does not necessarily mean that they can be used for the purpose of concluding valid contracts.

78. Paragraph (1) covers not merely the cases in which both the offer and the acceptance are communicated by electronic means but also cases in which only the offer or only the acceptance is communicated electronically. As to the time and place of formation of contracts in cases where an offer or the acceptance of an offer is expressed by means of a data message, no specific rule has been included in the Model Law in order not to interfere with national law applicable to contract formation. It was felt that such a provision might exceed the aim of the Model Law, which should be limited to providing that electronic communications would achieve the same degree of legal certainty as paper-based communications. The combination of existing rules on the formation of contracts with the provisions contained in article 15 is designed to dispel uncertainty as to the time and place of

formation of contracts in cases where the offer or the acceptance are exchanged electronically.

79. The words "unless otherwise stated by the parties", which merely restate, in the context of contract formation, the recognition of party autonomy expressed in article 4, are intended to make it clear that the purpose of the Model Law is not to impose the use of electronic means of communication on parties who rely on the use of paper-based communication to conclude contracts. Thus, article 11 should not be interpreted as restricting in any way party autonomy with respect to parties not involved in the use of electronic communication.

80. During the preparation of paragraph (1), it was felt that the provision might have the harmful effect of overruling otherwise applicable provisions of national law, which might prescribe specific formalities for the formation of certain contracts. Such forms include notarization and other requirements for "writings", and might respond to considerations of public policy, such as the need to protect certain parties or to warn them against specific risks. For that reason, paragraph (2) provides that an enacting State can exclude the application of paragraph (1) in certain instances to be specified in the legislation enacting the Model Law.

CHAPTER IV - ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS

11. Attribution of electronic records.

An electronic record shall be attributed to the originator-

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by any information system programmed by or on behalf of the originator to operate automatically.

COMMENTS:

According to section 2(1)(za) of the IT Act, **originator** is a person who: sends, generates, stores or transmits any electronic message or causes

any electronic message to be sent, generated, stored or transmitted to any other person. The term originator does not include an intermediary.

Illustration: Pooja uses her gmail.com email account to send an email to Sameer. Pooja is the originator of the email. Gmail.com is the intermediary.

This section can best be understood with the help of suitable illustrations. **Illustration:** Pooja logs in to her web-based gmail.com email account. She composes an email and presses the "Send" button, thereby sending the email to Sameer. The electronic record (email in this case) will be attributed to Pooja (the originator in this case) as Pooja herself has sent it.

Illustration: Pooja instructs her assistant Siddharth to send the above-mentioned email. In this case also, the email will be attributed to Pooja (and not her assistant Siddharth). The email has been sent by a person (Siddharth) who had the authority to act on behalf of the originator (Pooja) of the electronic record (email).

Illustration: Pooja goes on vacation for a week. In the meanwhile, she does not want people to think that she is ignoring their emails. She configures her gmail.com account to automatically reply to all incoming email messages with the following message:

"Thanks for your email. I am on vacation for a week and will reply to your email as soon as I get back".

Now every time that gmail.com replies to an incoming email on behalf of Pooja, the automatically generated email will be attributed to Pooja as it has been sent by an information system programmed on behalf of the originator (i.e. Pooja) to operate automatically.

This section is based upon Article 13 of the UNCITRAL Model Law on Electronic Commerce, titled "Attribution of data messages", quoted below:

Article 13. Attribution of data messages

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this provision, as quoted below: 83. Article 13 has its origin in article 5 of the UNCITRAL Model Law on International Credit Transfers, which defines the obligations of the sender of a payment order. Article 13 is intended to apply where there is a question as to whether a data message was really sent by the person who is indicated as being the originator. In the case of a paper based communication the problem would arise as the result of an alleged forged signature of the purported originator. In an electronic environment, an unauthorized person may have sent the message but the authentication by code, encryption or the like would be accurate. The purpose of article 13 is not to assign responsibility. It deals rather with attribution of data messages by establishing a presumption that under certain circumstances a data message would be considered as a message of the originator, and goes on to qualify that presumption in case the addressee knew or ought to have known that the data message was not that of the originator.

84. Paragraph (1) recalls the principle that an originator is bound by a data message if it has effectively sent that message. Paragraph (2) refers to the situation where the message was sent by a person other than the originator who had the authority to act on behalf of the originator. Paragraph (2) is not intended to displace the domestic law of agency, and the question as to whether the other person did in fact and in law have the authority to act on behalf of the originator is left to the appropriate legal rules outside the Model Law.

85. Paragraph (3) deals with two kinds of situations, in which the addressee could rely on a data message as being that of the originator: firstly, situations in which the addressee properly applied an authentication procedure previously agreed to by the originator; and secondly, situations in which the data message resulted from the actions of a person who, by virtue of its relationship with the originator, had access to the originator's authentication procedures. By stating that the addressee "is entitled to regard a data as being that of the originator", paragraph (3) read in conjunction with paragraph (4)(a) is intended to indicate that the addressee could act on the assumption that the data message is that of the originator up to the point in time it received notice from the originator that the data message was not that of the originator, or up to the point in time when it knew or should have known that the data message was not that of the originator.

86. Under paragraph (3)(a), if the addressee applies any authentication procedures previously agreed to by the originator and such application results in the proper verification of the originator as the source of the message, the message is presumed to be that of the originator. That covers not only the situation where an authentication procedure has been agreed upon by the originator and the addressee but also situations where an originator, unilaterally or as a result of an agreement with an intermediary, identified a procedure and agreed to be bound by a data message that met the requirements corresponding to that procedure. Thus, agreements that became effective not through direct agreement between the originator and the addressee but through the participation of third-party service providers are intended to be covered by paragraph (3)(a). However, it should be noted that paragraph (3)(a) applies only when the communication between the originator and the addressee is based on a previous agreement, but that it does not apply in an open environment.

87. The effect of paragraph (3)(b), read in conjunction with paragraph (4)(b), is that the originator or the addressee, as the case may be, is responsible for any unauthorized data message that can be shown to have been sent as a result of negligence of that party.

88. Paragraph (4)(a) should not be misinterpreted as relieving the originator from the consequences of sending a data message, with retroactive effect, irrespective of whether the addressee had acted on the assumption that the data message was that of the originator. Paragraph (4) is not intended to provide that receipt of a notice under subparagraph (a) would nullify the original message retroactively. Under subparagraph (a), the originator is released from the binding effect of the message after the time notice is received and not before that time. Moreover, paragraph (4) should not be read as allowing the originator to avoid being bound by the data message by sending notice to the addressee under subparagraph (a), in a case where the message had, in fact, been sent by the originator and the addressee properly applied agreed or reasonable authentication procedures. If the addressee can prove that the message is that of the originator, paragraph (1) would apply and not paragraph (4)(a). As to the meaning of "reasonable" time", the notice should be such as to give the addressee sufficient time to react. For example, in the case of just-in-time supply, the addressee should be given time to adjust its production chain.

89. With respect to paragraph (4)(b), it should be noted that the Model Law could lead to the result that the addressee would be

entitled to rely on a data message under paragraph (3)(a) if it had properly applied the agreed authentication procedures, even if it knew that the data message was not that of the originator. It was generally felt when preparing the Model Law that the risk that such a situation could arise should be accepted, in view of the need for preserving the reliability of agreed authentication procedures.

90. Paragraph (5) is intended to preclude the originator from disavowing the message once it was sent, unless the addressee knew, or should have known, that the data message was not that of the originator. In addition, paragraph (5) is intended to deal with errors in the content of the message arising from errors in transmission.

91. Paragraph (6) deals with the issue of erroneous duplication of data messages, an issue of considerable practical importance. It establishes the standard of care to be applied by the addressee to distinguish an erroneous duplicate of a data message from a separate data message.

12. Acknowledge of receipt

(1) Where the originator has not stipulated⁴⁴ that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgement may be given by-

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

COMMENT:

According to section 2(1)(b) of the *Information Technology Act*, addressee means a person who is intended by the originator to receive the electronic record but does not include any intermediary.

⁴⁴ The word "stipulated" substituted for the words "agreed with the addressee" by Information Technology (Amendment) Act, 2008.

Illustration: Pooja uses her gmail.com email account to send an email to Sameer. Pooja is the originator of the email. Gmail.com is the intermediary. Sameer is the addressee.

Section 12(1) provides for methods in which the acknowledgment of receipt of an electronic record may be given, provided no particular method has been agreed upon between the originator and the recipient.

One method for giving such acknowledgement is any communication (automated or otherwise) made by the addressee in this regard.

Illustration: Let us go back to the earlier example of Pooja going on vacation for a week. She has configured her email account to automatically reply to all incoming email messages with the following message:

"Thanks for your email. I am on vacation for a week and will reply to your email as soon as I get back".

The incoming message is also affixed at the bottom of the above-mentioned message.

Now when Siddharth sends an electronic record to Pooja by email, he will receive Pooja's pre-set message as well as a copy of his own message. This automated communication will serve as an acknowledgement that Pooja has received Siddharth's message.

Another method is any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received. Let us take another illustration.

Illustration: Rohit sends an email to Pooja informing her that he would like to purchase a car from her and would like to know the prices of the cars available for sale. Pooja subsequently sends Rohit a catalogue of prices of the cars available for sale.

It can now be concluded that Pooja has received Rohit's electronic record. This is because such a conduct on the part of Pooja (i.e. sending the catalogue) is sufficient to indicate to Rohit (the originator) that his email (i.e. the electronic record) has been received by the addressee (i.e. Pooja).

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then unless acknowledgement has been so received, the electronic record shall be deemed to have been never sent by the originator.

COMMENT:

Illustration: Suppose Pooja wants to sell a car to Sameer. She sends him an offer to buy the car. In her email, Pooja asks Sameer to send her an acknowledgement that he has received her email. Sameer does not send her an acknowledgement. In such a situation it shall be assumed that the email sent by Pooja was never sent.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

COMMENT:

Illustration: Rohit sends the following email to Sameer:

Further to our discussion, I am ready to pay Rs 25 lakh for the source code for the PKI software developed by you. Let me know as soon as you receive this email.

Sameer does not acknowledge receipt of this email. Rohit sends him another email as follows:

I am resending you my earlier email in which I had offered to pay Rs 25 lakh for the source code for the PKI software developed by you. Please acknowledge receipt of my email latest by next week.

Sameer does not acknowledge the email even after a week. The initial email sent by Rohit will be treated to have never been sent.

Section 12 of the *Information Technology Act* is based upon Article 14 of the *UNCITRAL Model Law on Electronic Commerce*, titled "Acknowledgement of receipt", quoted below:

Article 14. Acknowledgement of receipt

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise, or

(b) any conduct of the addressee sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set

forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this provision, as quoted below:

93. The use of functional acknowledgements is a business decision to be made by users of electronic commerce; the Model Law does not intend to impose the use of any such procedure. However, taking into account the commercial value of a system of acknowledgement of receipt and the widespread use of such systems in the context of electronic commerce, it was felt that the Model Law should address a number of legal issues arising from the use of acknowledgement procedures. It should be noted that the notion of "acknowledgement" is sometimes used to cover a variety of procedures, ranging from a mere acknowledgement of receipt of an unspecified message to an expression of agreement with the content of a specific data message. In many instances, the procedure of "acknowledgement" would parallel the system known as "return receipt requested" in postal systems. Acknowledgements of receipt may be required in a variety of instruments, e.g., in the data message itself, in bilateral or multilateral communication agreements, or in "system rules". It should be borne in mind that variety among acknowledgement procedures implies variety of the related costs.

The provisions of article 14 are based on the assumption that acknowledgement procedures are to be used at the discretion of the originator.

Article 14 is not intended to deal with the legal consequences that may flow from sending an acknowledgement of receipt, apart from establishing receipt of the data message. For example, where an originator sends an offer in a data message and requests acknowledgement of receipt, the acknowledgement of receipt simply evidences that the offer has been received. Whether or not sending that acknowledgement amounted to accepting the offer is not dealt with by the Model Law but by contract law outside the Model Law.

94. The purpose of paragraph (2) is to validate acknowledgement by any communication or conduct of the addressee (e.g., the

shipment of the goods as an acknowledgement of receipt of a purchase order) where the originator has not agreed with the addressee that the acknowledgement should be in a particular form. The situation where an acknowledgement has been unilaterally requested by the originator to be given in a specific form is not expressly addressed by article 14, which may entail as a possible consequence that a unilateral requirement by the originator as to the form of acknowledgements would not affect the right of the addressee to acknowledge receipt by any communication or conduct sufficient to indicate to the originator that the message had been received. Such a possible interpretation of paragraph (2) makes it particularly necessary to emphasize in the Model Law the distinction to be drawn between the effects of an acknowledgement of receipt of a data message and any communication in response to the content of that data message, a reason why paragraph (7) is needed. 95. Paragraph (3), which deals with the situation where the originator has stated that the data message is conditional on receipt of an acknowledgement, applies whether or not the originator has specified that the acknowledgement should be received by a certain time.

96. The purpose of paragraph (4) is to deal with the more common situation where an acknowledgement is requested, without any statement being made by the originator that the data message is of no effect until an acknowledgement has been received. Such a provision is needed to establish the point in time when the originator of a data message who has requested an acknowledgement of receipt is relieved from any legal implication of sending that data message if the requested acknowledgement has not been received. An example of a factual situation where a provision along the lines of paragraph (4) would be particularly useful would be that the originator of an offer to contract who has not received the requested acknowledgement from the addressee of the offer may need to know the point in time after which it is free to transfer the offer to another party. It may be noted that the provision does not create any obligation binding on the originator, but merely establishes means by which the originator, if it so wishes, can clarify its status in cases where it has not received the requested acknowledgement. It may also be noted that the provision does not create any obligation binding on the addressee of the data message, who would, in most circumstances, be free to rely or not to rely on any given data message, provided that it would bear the risk of the data message being unreliable for lack

of an acknowledgement of receipt. The addressee, however, is protected since the originator who does not receive a requested acknowledgement may not automatically treat the data message as though it had never been transmitted, without giving further notice to the addressee. The procedure described under paragraph (4) is purely at the discretion of the originator. For example, where the originator sent a data message which under the agreement between the parties had to be received by a certain time, and the originator requested an acknowledgement of receipt, the addressee could not deny the legal effectiveness of the message simply by withholding the requested acknowledgement.

97. The rebuttable presumption established in paragraph (5) is needed to create certainty and would be particularly useful in the con text of electronic communication between parties that are not linked by a trading-partners agreement. The second sentence of paragraph (5) should be read in conjunction with paragraph (5) of article 13, which establishes the conditions under which, in case of an inconsistency between the text of the data message as sent and the text as received, the text as received prevails.

98. Paragraph (6) corresponds to a certain type of acknowledgement, for example, an EDIFACT message establishing that the data message received is syntactically correct, i.e., that it can be processed by the receiving computer. The reference to technical requirements, which is to be construed primarily as a reference to "data syntax" in the context of EDI communications, may be less relevant in the context of the use of other means of communication, such as telegram or telex. In addition to mere consistency with the rules of "data syntax", technical requirements set forth in applicable standards may include, for example, the use of procedures verifying the integrity of the contents of data messages.

99. Paragraph (7) is intended to dispel uncertainties that might exist as to the legal effect of an acknowledgement of receipt. For example, paragraph (7) indicates that an acknowledgement of receipt should not be confused with any communication related to the contents of the acknowledged message.

13. Time and place of despatch and receipt of electronic record.

(1) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs

when it enters a computer resources outside the control of the originator.

COMMENT:

Illustration: Pooja composes a message for Rohit at 11.56 a.m. At exactly 12.00 noon she presses the "Submit" or "Send" button. When she does that the message leaves her computer and begins its journey across the Internet.

It is now no longer in Pooja's control. The time of despatch of this message will be 12.00 noon.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:-

(a) if the addressee has designated a computer resource for the purpose of receiving electronic record,-

(i) receipt occurs at the time when the electronic record enters the designated computer resources; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

COMMENT:

Illustration: The marketing department of a company claims that it would make the delivery of any order within 48 hours of receipt of the order. For this purpose, they have created an order form on their website. The customer only has to fill in the form and press submit and the message reaches the designated email address of the marketing department.

Now Suresh, a customer, fills in this order form and presses submit. The moment the message reaches the company's server, the order is deemed to have been received.

Karan, on the other hand, emails his order to the information division of the company. One Mr. Sharma, who is out on vacation, checks this account once a week. Mr. Sharma comes back two weeks later and logs in to the account at 11.30 a.m. This is the time of receipt of the message although it was sent two weeks earlier.

Now suppose the company had not specified any address to which orders can be sent by email. Had Karan then sent the order to the information division, the time of receipt of the message would have been the time when it reached the server of the company.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

COMMENT:

Illustration: Sameer is a businessman operating from his home in Pune, India. Sameer sent an order by email to a company having its head office in New York, USA. The place of despatch of the order would be Sameer's home and the place of receipt of the order would be the company's office.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

COMMENT:

Illustration: Let us consider the illustration mentioned above of Sameer and the New York based company. Even if the company has its mail server located physically at Canada, the place of receipt of the order would be the company's office in New York USA.

(5) For the purpose of this section,-

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c)"usual place of residence ", in relation to a body corporate, means the place where it is registered.

COMMENT:

Illustration: Sameer sent an order by email to a company having its head office in New York, USA. The company has offices in 12 countries. The place of business will be the principal place of business (New York in this case).

Sameer is a businessman operating from his home in Pune, India. He does not have a separate place of business. Sameer's residence will be deemed to be the place of business.

Case Law: P.R. Transport Agency vs. Union of India & others [AIR2006All23, 2006(1)AWC504]

Appellants: P.R. Transport Agency through its partner Sri Prabhakar Singh Vs. Respondent: Union of India (UOI) through Secretary, Ministry of Coal, Bharat Coking Coal Ltd. through its Chairman, Chief Sales Manager Road Sales, Bharat Coking Coal Ltd. and Metal and Scrap Trading Corporation Ltd. (MSTC Ltd.) through its Chairman cum Managing Director

Background of the case:

Bharat Coking Coal Ltd (BCC) held an e-auction for coal in different lots. P.R. Transport Agency's (PRTA) bid was accepted for 4000 metric tons of coal from Dobari Colliery.

The acceptance letter was issued on 19th July 2005 by e-mail to PRTA's e-mail address. Acting upon this acceptance, PRTA deposited the full amount of Rs. 81.12 lakh through a cheque in favour of BCC. This cheque was accepted and encashed by BCC.

BCC did not deliver the coal to PRTA. Instead it e-mailed PRTA saying that the sale as well as the e-auction in favour of PRTA stood cancelled "due to some technical and unavoidable reasons".

The only reason for this cancellation was that there was some other person whose bid for the same coal was slightly higher than that of PRTA. Due to some flaw in the computer or its programme or feeding of data the higher bid had not been considered earlier.

This communication was challenged by PRTA in the High Court of Allahabad. [Note: Allahabad is in the state of Uttar Pradesh (UP)]

BCC objected to the "territorial jurisdiction" of the Court on the grounds that no part of the cause of action had arisen within U.P.

Issue raised by BCC:

The High Court at Allahabad (in U.P.) had no jurisdiction as no part of the cause of action had arisen within U.P.

Issues raised by PRTA:

1. The communication of the acceptance of the tender was received by the petitioner by e-mail at Chandauli (U.P.). Hence, the contract (from which the dispute arose) was completed at Chandauli (U.P). The completion of the contract is a part of the "cause of action".

2. The place where the contract was completed by receipt of communication of acceptance is a place where 'part of cause of action' arises.

Points considered by the court

1. With reference to contracts made by telephone, telex or fax, the contract is complete when and where the acceptance is received. However, this principle can apply only where the transmitting terminal and the receiving terminal are at fixed points.

2. In case of e-mail, the data (in this case acceptance) can be transmitted from anywhere by the e-mail account holder. It goes to the memory of a 'server' which may be located anywhere and can be retrieved by the addressee account holder from anywhere in the world. Therefore, there is no fixed point either of transmission or of receipt.

3. Section 13(3) of the Information Technology Act has covered this difficulty of "no fixed point either of transmission or of receipt". According to this section "...an electronic record is

deemed to be received at the place where the addressee has his place of business."

4. The acceptance of the tender will be deemed to be received by PRTA at the places where it has place of business. In this case it is Varanasi and Chandauli (both in U.P.)

Decision of the court

1. The acceptance was received by PRTA at Chandauli / Varanasi. The contract became complete by receipt of such acceptance.

2. Both these places were within the territorial jurisdiction of the High Court of Allahabad. Therefore, a part of the cause of action had arisen in U.P. and the court had territorial jurisdiction.

Section 13 of the *Information Technology Act* is based upon Article 15 of the *UNCITRAL Model Law on Electronic Commerce*, titled "Time and place of dispatch and receipt of data messages", quoted below:

Article 15. Time and place of dispatch and receipt of data messages

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business.

For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

(5) The provisions of this article do not apply to the following: [...].

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce* elaborates upon this provision, as quoted below:

100. Article 15 results from the recognition that, for the operation of many existing rules of law, it is important to ascertain the time and place of receipt of information. The use of electronic communication techniques makes those difficult to ascertain. It is not uncommon for users of electronic commerce to communicate from one State to another without knowing the location of information systems through which communication is operated. In addition, the location of certain communication systems may change without either of the parties being aware of the change. The Model Law is thus intended to reflect the fact that the location of information systems is irrelevant and sets forth a more objective criterion, namely, the place of business of the parties. In that connection, it should be noted that article 15 is not intended to establish a conflict-of-laws rule.

101. Paragraph (1) defines the time of dispatch of a data message as the time when the data message enters an information system outside the control of the originator, which may be the information system of an intermediary or an information system of the addressee. The concept of "dispatch" refers to the commencement of the electronic transmission of the data message. Where "dispatch" already has an established meaning, article 15 is intended to supplement national rules on dispatch and not to displace them. If dispatch occurs when the data message reaches an information system of the addressee, dispatch under paragraph (1) and receipt under paragraph (2) are simultaneous, except where the data message is sent to an information system of the addressee that is not the information system designated by the addressee under paragraph (2)(a).

102. Paragraph (2), the purpose of which is to define the time of receipt of a data message, addresses the situation where the addressee unilaterally designates a specific information system for the receipt of a message (in which case the designated system may or may not be an information system of the addressee), and the data message reaches an information system of the addressee), and the data message reaches an information system of the addressee that is not the designated system. In such a situation, receipt is deemed to occur when the data message is retrieved by the addressee. By "designated information system", the Model Law is intended to cover a system that has been specifically designated by a party, for instance in the case where an offer expressly specifies the address to which acceptance should be sent. The mere indication of an electronic mail or telecopy address on a letterhead or other document should not be regarded as express designation of one or more information systems.

103. Attention is drawn to the notion of "entry" into an information system, which is used for both the definition of dispatch and that of receipt of a data message. A data message enters an information system at the time when it becomes available for processing within that information system. Whether a data message which enters an information system is intelligible or usable by the addressee is outside the purview of the Model Law. The Model Law does not intend to overrule provisions of national law under which receipt of a message may occur at the time when the message enters the sphere of the addressee, irrespective of whether the message is intelligible or usable by the addressee. Nor is the Model Law intended to run counter to trade usages, under which certain encoded messages are deemed to be received even before they are usable by, or intelligible for, the addressee. It was felt that the Model Law should not create a more stringent requirement than currently exists in a paper-based environment, where a message can be considered to be received even if it is not intelligible for the addressee or not intended to be intelligible to the addressee (e.g., where encrypted data is transmitted to a depository for the sole purpose of retention in the context of intellectual property rights protection).

104. A data message should not be considered to be dispatched if it merely reached the information system of the addressee but failed to enter it. It may be noted that the Model Law does not expressly address the question of possible malfunctioning of information systems as a basis for liability. In particular, where the information system of the addressee does not function at all or functions improperly or, while functioning properly, cannot be entered into by the data message (e.g., in the case of a telecopier that is constantly occupied), dispatch under the Model Law does not occur. It was felt during the preparation of the Model Law that the addressee should not be placed under the burdensome obligation to maintain its information system functioning at all times by way of a general provision.

105. The purpose of paragraph (4) is to deal with the place of receipt of a data message. The principal reason for including a rule on the place of receipt of a data message is to address a circumstance characteristic of electronic commerce that might not be treated adequately under existing law, namely, that very often the information system of the addressee where the data message is received, or from which the data message is retrieved, is located in a jurisdiction other than that in which the addressee itself is located. Thus, the rationale behind the provision is to ensure that the location of an information system is not the determinant element, and that there is some reasonable connection between the addressee and what is deemed to be the place of receipt, and that that place can be readily ascertained by the originator. The Model Law does not contain specific provisions as to how the designation of an information system should be made, or whether a change could be made after such a designation by the addressee.

106. Paragraph (4), which contains a reference to the "underlying transaction", is intended to refer to both actual and contemplated underlying transactions. References to "place of business", "principal place of business" and "place of habitual residence" were adopted to bring the text in line with article 10 of the United Nations Convention on Contracts for the International Sale of Goods.

107. The effect of paragraph (4) is to introduce a distinction between the deemed place of receipt and the place actually reached by a data message at the time of its receipt under paragraph (2). That distinction is not to be interpreted as apportioning risks between the originator and the addressee in case of damage or loss of a data message between the time of its receipt under paragraph (2) and the time when it reached its place of receipt under paragraph (4). Paragraph (4) merely establishes an irrebuttable presumption regarding a legal fact, to be used where another body of law (e.g., on formation of contracts or conflict of laws) require determination of the place of receipt of a data message. However, it was felt during the preparation of the Model Law that introducing a deemed place of receipt, as distinct from the place actually reached by that data message at the time of its receipt, would be inappropriate outside the context of computerized transmissions (e.g., in the context of telegram or telex). The provision was thus limited in scope to cover only computerized transmissions of data messages.

CHAPTER V - SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES⁴⁵

14. Secure electronic record.

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure electronic signature.⁴⁶

An electronic signature shall be deemed to be a secure electronic signature if –

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

⁴⁵ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008. Also refer to Information Technology (Security Procedure) Rules, 2004.

⁴⁶ Substituted by Information Technology (Amendment) Act, 2008 for 15. Secure digital signature.- If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was – (a) unique to the subscriber affixing it; (b) capable of identifying such subscriber; (c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which related in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature."

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation. – In case of digital signature, the "signature creation data" means the private key of the subscriber.

COMMENTS:

According to notification G.S.R. 735 (E), notified by the Central Government on the 29th of October, 2004, a secure digital signature is one to which the following security procedure has been applied:

(a) a smart card or hardware token, as the case may be, with cryptographic module in it, is used to create the key pair;

(b) the private key used to create the digital signature always remains in the smart card or hardware token as the case may be;

(c) the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system;

(d) the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature;

(e) the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person;

(f) the standards referred to in rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and

(g) the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated.

This section is based upon Article 6 of the UNCITRAL Model Law on Electronic Signatures, titled "Compliance with a requirement for a signature", quoted below:

Article 6. Compliance with a requirement for a signature

1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement. 2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

4. Paragraph 3 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.

5. The provisions of this article do not apply to the following: [...].

The *Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures* elaborates upon this provision, as quoted below:

Importance of article 6

115. Article 6 is one of the core provisions of the Model Law. Article 6 is intended to build upon article 7 of the UNCITRAL Model Law on Electronic Commerce and to provide guidance as to how the test of reliability in paragraph 1 (b) of article 7 can be satisfied. In interpreting article 6, it should be borne in mind that the purpose of the provision is to ensure that, where any legal consequence would have flowed from the use of a handwritten signature, the same consequence should flow from the use of a reliable electronic signature.

Paragraphs 1, 2 and 5

116. Paragraphs 1, 2 and 5 of article 6 introduce provisions drawn from article 7, paragraphs (1) (b), (2) and (3) of the UNCITRAL Model Law on Electronic Commerce, respectively. Wording inspired by article 7, paragraph 1 (a), of the UNCITRAL Model

Law on Electronic Commerce is already included in the definition of "electronic signature" under article 2, subparagraph (a).

Notions of "identity" and "identification"

117. The Working Group agreed that, for the purpose of defining "electronic signature" under the Model Law, the term "identification" could be broader than mere identification of the signatory by name. The concept of identity or identification includes distinguishing him or her, by name or otherwise, from any other person, and may refer to other significant characteristics,

such as position or authority, either in combination with a name or without reference to the name. On that basis, it is not necessary to distinguish between identity and other significant characteristics, nor to limit the Model Law to those situations in which only identity certificates that name the signatory are used (A/CN.9/467, paras. 56-58).

Effect of the Model Law varying with level of technical reliability

118. In the preparation of the Model Law, the view was expressed that (either through a reference to the notion of "enhanced electronic signature" or through a direct mention of criteria for establishing the technical reliability of a given signature technique) a dual purpose of article 6 should be to establish: (a) that legal effects would result from the application of those electronic signature techniques that were recognized as reliable; and (b), conversely, that no such legal effects would flow from the use of techniques of a lesser reliability. It was generally felt, however, that a more subtle distinction might need to be drawn between the various possible electronic signature techniques, since the Model Law should avoid discriminating against any form of electronic signature, unsophisticated and insecure though it might appear in given circumstances. Therefore, any electronic signature technique applied for the purpose of signing a data message under article 7, paragraph 1 (a), of the UNCITRAL Model Law on Electronic Commerce would be likely to produce legal effects, provided that it was sufficiently reliable in the light of all the circumstances, including any agreement between the parties. However, under article 7 of the UNCITRAL Model Law on Electronic Commerce, the determination of what constitutes a reliable method of signature in the light of the circumstances, can be made only by a court or other trier of fact intervening ex post, possibly long after the electronic signature has been used. In contrast, the new Model Law is expected to create a benefit in

favour of certain techniques, which are recognized as particularly reliable, irrespective of the circumstances in which they are used. That is the purpose of paragraph 3, which is expected to create certainty (through either a presumption or a substantive rule), at or before the time any such technique of electronic signature is used (ex ante), that using a recognized technique will result in legal effects equivalent to those of a handwritten signature. Thus, paragraph 3 is an essential provision if the new Model Law is to meet its goal of providing more certainty than readily offered by the UNCITRAL Model Law on Electronic Commerce as to the legal effect to be expected from the use of particularly reliable types of electronic signatures (see A/CN.9/465, para. 64).

Presumption or substantive rule

119. In order to provide certainty as to the legal effect resulting from the use of an electronic signature as defined under article 2, paragraph 3 expressly establishes the legal effects that would result from the conjunction of certain technical characteristics of an electronic signature (see A/CN.9/484, para. 58). As to how those legal effects would be established, enacting States, depending on their law of civil and commercial procedure, should be free to adopt a presumption or to proceed by way of a direct assertion of the linkage between certain technical characteristics and the legal effect of a signature (see A/CN.9/467, paras. 61 and 62).

Intent of signatory

120. A question remains as to whether any legal effect should result from the use of electronic signature techniques that may be made with no clear intent by the signatory of becoming legally bound by approval of the information being electronically signed. In any such circumstance, the second function described in article 7, paragraph (1) (a), of the UNCITRAL Model Law on Electronic Commerce is not fulfilled since there is no "intent of indicating any approval of the information contained in the data message". The approach taken in the Model Law is that the legal consequences of the use of a handwritten signature should be replicated in an electronic environment. Thus, by appending a signature (whether handwritten or electronic) to certain information, the signatory should be presumed to have approved the linking of its identity with that information. Whether such a linking should produce legal effects (contractual or other) would result from the nature of the information being signed, and from any other circumstances, to be assessed according to the law applicable outside the Model Law. In that context, the Model Law is not intended to interfere with the general law of contracts or obligations (see A/CN.9/465, para. 65).

Criteria of technical reliability

121. Subparagraphs (a)-(d) of paragraph 3 are intended to express objective criteria of technical reliability of electronic signatures. Subparagraph (a) focuses on the objective characteristics of the signature creation data, which must be "linked to the signatory and to no other person". From a technical point of view, the signature creation data could be uniquely "linked" to the signatory, without being "unique" in itself. The linkage between the data used for creation of the signature and the signatory is the essential element (A/CN.9/467, para. 63). While certain electronic signature creation data may be shared by a variety of users, for example where several employees would share the use of a corporate signature creation data, that data must be capable of identifying one user unambiguously in the context of each electronic signature.

Sole control of signature creation data by the signatory

122. Subparagraph (b) deals with the circumstances in which the signature creation data are used. At the time they are used, the signature creation data must be under the sole control of the signatory. In relation to the notion of sole control by the signatory, a question is whether the signatory would retain its ability to authorize another person to use the signature creation data on its behalf. Such a situation might arise where the signature creation data are used in the corporate context where the corporate entity would be the signatory but would require a number of persons to be able to sign on its behalf (A/CN.9/467, para. 66). Another example may be found in business applications such as the one where signature creation data exist on a network and are capable of being used by a number of people. In that situation, the network would presumably relate to a particular entity which would be the signatory and maintain control over the signature creation data. If that was not the case, and the signature creation data were widely available, they should not be covered by the Model Law (A/CN.9/467, para. 67). Where a single key is operated by more than one person in the context of a "split-key" or other "sharedsecret" scheme, reference to "the signatory" means a reference to those persons jointly (A/CN.9/483, para. 152).

Agency

123. Subparagraphs (a) and (b) converge to ensure that the signature creation data are capable of being used by only one person at any given time, principally the time of signing, and not by some other person as well (see above, para. 103). The question of agency or authorized use of the signature creation data is addressed in the definition of "signatory" (A/CN.9/467, para. 68).

Integrity

124. Subparagraphs (c) and (d) deal with the issues of integrity of the electronic signature and integrity of the information being signed electronically.

It would have been possible to combine the two provisions to emphasize the notion that, where a signature is attached to a document, the integrity of the document and the integrity of the signature are so closely related that it is difficult to conceive of one without the other. However, it was decided that the Model Law should follow the distinction drawn in the UNCITRAL Model Law on Electronic Commerce between articles 7 and 8. Although some technologies provide both authentication (art. 7 of the UNCITRAL Model Law on Electronic Commerce) and integrity (art. 8 of the UNCITRAL Model Law on Electronic Commerce), those concepts can be seen as distinct legal concepts and treated as such. Since a handwritten signature provides neither a guarantee of the integrity of the document to which it is attached nor a guarantee that any change made to the document would be detectable, the functional equivalence approach requires that those concepts should not be dealt with in a single provision. The purpose of paragraph 3 (c) is to set forth the criterion to be met in order to demonstrate that a particular method of electronic signature is reliable enough to satisfy a requirement of law for a signature. That requirement of law could be met without having to demonstrate the integrity of the entire document (see A/CN.9/467, paras. 72-80).

125. Subparagraph (d) is intended primarily for use in those countries where existing legal rules governing the use of handwritten signatures could not accommodate a distinction between integrity of the signature and integrity of the information being signed. In other countries, subparagraph (d) might create a signature that would be more reliable than a handwritten signature

and thus go beyond the concept of functional equivalent to a signature.

In certain jurisdictions, the effect of subparagraph (d) may be to create a functional equivalent to an original document (see A/CN.9/484, para. 62).

Electronic signature of portion of a message

126. In subparagraph (d), the necessary linkage between the signature and the information being signed is expressed so as to avoid the implication that the electronic signature could apply only to the full contents of a data message. In fact, the information being signed, in many instances, will be only a portion of the information contained in the data message. For example, an electronic signature may relate only to information appended to the message for transmission purposes.

Variation by agreement

127. Paragraph 3 is not intended to limit the application of article 5 and of any applicable law recognizing the freedom of the parties to stipulate in any relevant agreement that a given signature technique would be treated among themselves as a reliable equivalent of a handwritten signature.

128. Paragraph 4 (a) is intended to provide a legal basis for the commercial practice under which many commercial parties would regulate by contract their relationships regarding the use of electronic signatures (see A/CN.9/484, para. 63).

Possibility to adduce evidence of the non-reliability of an electronic signature

129. Paragraph 4 (b) is intended to make it clear that the Model Law does not limit any possibility that may exist to rebut the presumption contemplated in paragraph 3 (see A/CN.9/484, para. 63).

Exclusions from the scope of article 6

130. The principle embodied in paragraph 5 is that an enacting State may exclude from the application of article 6 certain situations to be specified in the legislation enacting the Model Law. An enacting State may wish to exclude specifically certain types of situations, depending in particular on the purpose for which a formal requirement for a handwritten signature has been established. A specific exclusion might be considered, for example, in the context of formalities required pursuant to international treaty obligations of the enacting State and other kinds of situations and areas of law that are beyond the power of the enacting State to change by means of a statute.

131. Paragraph 5 was included with a view to enhancing the acceptability of the Model Law. It recognizes that the matter of specifying exclusions should be left to enacting States, an approach that would take better account of differences in national circumstances. However, it should be noted that the objectives of the Model Law would not be achieved if paragraph 5 were used to establish blanket exceptions, and the opportunity provided by paragraph 5 in that respect should be avoided. Numerous exclusions from the scope of article 6 would raise needless obstacles to the development of electronic signatures, since what the Model Law contains are very fundamental principles and approaches that are expected to find general application (see A/CN.9/484, para. 63).

16. Security procedures and practices.⁴⁷

The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices:

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

CHAPTER VI - REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers.

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities

⁴⁷ Substituted by Information Technology (Amendment) Act, 2008 for 16. Security procedure.- The Central Government shall for the purpose of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including- (a) the nature of the transaction; (b) the level of sophistication of the parties with reference to their technological capacity; (c) the volume of similar transactions engaged in by other parties; (d) the availability of alternatives offered to but rejected by any party; (e) the cost of alternative procedures; and (f) the procedures in general use for similar types of transaction or communications."

for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers, Assistant Controllers, other officers and employees⁴⁸ as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers, Assistant Controllers, other officers and employees ⁴⁹ shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Officer of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller.

The Controller may perform all or any of the following function, namely:-

(a) exercising supervision over the activities of Certifying Authorities;

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

⁴⁸ The words "and Assistant Controllers" substituted by the words "Assistant Controllers, other officers and employees" by Information Technology (Amendment) Act, 2008.

⁴⁹ The words "and Assistant Controllers" substituted by the words "Assistant Controllers, other officers and employees" by Information Technology (Amendment) Act, 2008.

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Electronic Signature⁵⁰ Certificate and the public key;

(g) specifying the form and content of a Electronic Signature⁵¹ Certificate and the key;

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(I) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Rule 22 of the *Information Technology (Certifying Authorities) Rules,* 2000 is relevant in this regard. It states:

22. Database of Certifying Authorities.—

The Controller shall maintain a database of the disclosure record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority, containing inter alia the following details:

⁵⁰ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁵¹ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

(a) the name of the person/names of the Directors, nature of business, Income tax Permanent Account Number, web address, if any, office and residential address, location of facilities associated with functions of generation of Digital Signature Certificate, voice and facsimile telephone numbers, electronic mail address(es), administrative contacts and authorized representatives;

(b) the public key(s), corresponding to the private key(s) used by the Certifying Authority and recognized foreign Certifying Authority to digitally sign Digital Signature Certificate;

(c) current and past versions of Certification Practice Statement of Certifying Authority;

(d) time stamps indicating the date and time of- (i) grant of licence; (ii) confirmation of adoption of Certification Practice Statement and its earlier versions by Certifying Authority; (iii) commencement of commercial operations of generation and issue of Digital Signature Certificate by the Certifying Authority; (iv) revocation or suspension of licence of Certifying Authority; (v) commencement of operation of Cross Certifying Authority; (vi) issue of recognition of foreign Certifying Authority; (vii) revocation or suspension of recognition of foreign Certifying Authority; Authority; (vii) assue of recognition of recognition of foreign Certifying Authority; (vii) revocation or suspension of recognition of foreign Certifying Authority; (vii) revocation or suspension of recognition of foreign Certifying Authority; (vii) revocation or suspension of recognition of foreign Certifying Authority.

19. Recognition of foreign Certifying Authorities

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under subsection (1), the Electronic Signature⁵² Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1), he may, for reasons to be recorded in writing,

⁵² The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

by notification in the Official Gazette, revoke such recognition.

20. Omitted by Information Technology (Amendment) Act, $2008^{\rm 53}$

21. Licence to issue Electronic Signature⁵⁴ Certificates

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue Electronic Signature⁵⁵ Certificates.

(2) No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Electronic Signature⁵⁶ Certificates as may be prescribed by the Central Government.

(3) A licence granted under this sections shall-

- (a) be valid for such period as may be prescribed by the Central Government;
- (b) not be transferable or heritable;
- (c) be subject to such terms and conditions as may be specified by the regulations.

⁵³ Controller to act as repository. -(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act. (2) The Controller shall-(a) make use of hardware, software and procedures that are secure from intrusion and misuse; (b) observe such other standards as may be prescribed by the Central Government; to ensure that the secrecy and security of the digital signatures are assured. (3) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

⁵⁴ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁵⁵ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁵⁶ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

COMMENTS:

Rule 8 of the Information Technology (Certifying Authorities) Rules, 2000 as amended by the Information Technology (Certifying Authorities) (Amendment) Rules, 2003 is relevant in this regard. It states:

8. Licensing of Certifying Authorities.—

(1) The following persons may apply for grant of a licence to issue Digital Signature Certificates, namely:-

(a) an individual, being a citizen of India and having a capital of five crores of rupees or more in his business or profession;

(b) a company having–(i) paid up capital of not less than five crores of rupees; and (ii) net worth of not less than fifty crores of rupees:

Provided that no company in which the equity share capital held in aggregate by the Non-resident Indians, Foreign Institutional Investors, or foreign companies, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence:

Provided further that in a case where the company has been registered under the Companies Act, 1956 (1 of 1956) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in subclause (ii) of this clause shall be the aggregate net worth of its majority shareholders holding at least 51% of paid equity capital, being the Hindu Undivided Family, firm or company:

Provided also that the majority shareholders referred to in the second proviso shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company:

Provided also that the majority shareholders of a company referred to in the second proviso whose net worth has been determined on the basis of such majority shareholders, shall not sell or transfer its equity shares held in such company-(i) unless such a company acquires or has its own net worth of not less than fifty crores of rupees; (ii) without prior approval of the Controller;

(c) a firm having - (i) capital subscribed by all partners of not less than five crores of rupees; and (ii) net worth of not less than fifty crores of rupees:

Provided that no firm, in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence: Provided further that in a case where the firm has been registered under the Indian Partnership Act, 1932 (9 of 1932) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in subclause (ii) of this clause shall be the aggregate net worth of all of its partners:

Provided also that the partners referred to in the second proviso shall not include Non-resident Indian and foreign national:

Provided also that the partners of a firm referred to in the second proviso whose net worth has been determined on the basis of such partners, shall not sell or transfer its capital held in such firm-(i) unless such firm has acquired or has its own net worth of not less than fifty crores of rupees; (ii) without prior approval of the Controller;

(d) Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.

Explanation.- For the purpose of this rule,-

(i) "company" shall have the meaning assigned to it in clause 17 of section 2 of the Income-tax Act, 1961 (43 of 1961);

(ii) "firm", "partner" and "partnership" shall have the meanings respectively assigned to them in the Indian Partnership Act, 1932 (9 of 1932); but the expression "partner" shall also include any person who, being a minor has been admitted to the benefits of partnership;

(iii) "foreign company" shall have the meaning assigned to it in clause (23A) of section 2 of the Income-tax Act, 1961 (43 of 1961);

(iv) "net worth" shall have the meaning assigned to it in clause (ga) of subsection (1) of section 3 of the Sick Industrial Companies (Special Provisions) Act, 1985 (1 of 1986);

(v) "Non-resident" shall have the meaning assigned to it as in clause 26 of section 2 of the Income-tax Act, 1961 (43 of 1961).

(2) The applicant being an individual, or a company, or a firm under sub-rule (1), shall furnish a performance bond in the form of a banker's guarantee from a scheduled bank in favour of the Controller in such form and in such manner as may be approved by the Controller for an amount of not less than fifty lakhs of rupees and the performance bond in the form of banker's guarantee shall remain valid for a period of six years from the date of its submission:

Provided that the company and firm referred to in the second proviso to clause (b) and the second proviso to clause (c) of subrule (1) shall furnish a performance bond in the form of a banker's guarantee" for one crore of rupees:

Provided further that nothing in the first proviso shall apply to the company or firm after it has acquired or has its net worth of fifty crores of rupees.

(3) Without prejudice to any penalty which may be imposed or prosecution may be initiated for any offence under the Act or any other law for the time being in force, the performance bond in the form of banker's guarantee may be invoked–

(a) when the Controller has suspended the licence under subsection (2) of section 25 of the Act; or

(b) for payment of an offer of compensation made by the Controller; or

(c) for payment of liabilities and rectification costs attributed to the negligence of the Certifying Authority, its officers or employees; or

(d) for payment of the costs incurred in the discontinuation or transfer of operations of the licensed Certifying Authority, if the Certifying Authority's licence or operations is discontinued; or

(e) any other default made by the Certifying Authority in complying with the provisions of the Act or rules made thereunder.

Explanation.- "transfer of operation" shall have the meaning assigned to it in clause (47) of section 2 of the Income-tax Act, 1961 (43 of 1961).

Rule 13 of the *Information Technology (Certifying Authorities) Rules,* 2000 is also relevant in this regard. It states:

13. Validity of licence.—

(1) A licence shall be valid for a period of five years from the date of its issue.

(2) The licence shall not be transferable.

Regulation 3 of the *Information Technology (Certifying Authority) Regulations, 2001* is also relevant in this regard. It states:

3. Terms and conditions of licence to issue Digital Signature Certificate:-

Every licence to issue Digital Signature Certificates shall be granted under the Act subject to the following terms and conditions, namely: -

(i) General-

(a) The licence shall be valid for a period of five years from the date of issue.

(b) The licence shall not be transferable or heritable;

(c) The Controller can revoke or suspend the licence in accordance with the provisions of the Act.

(d) The Certifying Authority shall be bound to comply with all the parameters against which it was audited prior to issue of licence and shall consistently and continuously comply with those parameters during the period for which the licence shall remain valid.

(e) The Certifying Authority shall subject itself to periodic audits to ensure that all conditions of the licence are consistently complied with by it. As the cryptographic components of the Certifying Authority systems are highly sensitive and critical, the components must be subjected to periodic expert review to ensure their integrity and assurance.

(f) The Certifying Authority must maintain secure and reliable records and logs for activities that are core to its operations.

(g) Public Key Certificates and Certificate Revocation Lists must be archived for a minimum period of seven years to enable verification of past transactions.

(h) The Certifying Authority shall provide Time Stamping Service for its subscribers. Error of the Time Stamping clock shall not be more than $1 \text{ in } 10^9$.

(i) The Certifying Authority shall use methods, which are approved by the Controller, to verify the identity of a subscriber before issuing or renewing any Public Key Certificate.

(j) The Certifying Authority shall publish a notice of suspension or revocation of any certificate in the Certificate Revocation List in its repository immediately after receiving an authorised request of such suspension or revocation.

(k) The Certifying Authority shall always assure the confidentiality of subscriber information.

(1) All changes in Certificate Policy and certification practice statement shall be published on the web site of the Certifying Authority and brought to the notice of the Controller well in advance of such publication. However any change shall not contravene any provision of the Act, rule or regulation or made there under.

(m) The Certifying Authority shall comply with every order or direction issued by the Controller within the stipulated period.

(ii) Overall Management and Obligations-

(a) The Certifying Authority shall manage its functions in accordance with the levels of integrity and security approved by the Controller from time to time.

(b) The Certifying Authority shall disclose information on the assurance levels of the certificates that it issues and the limitations of its liabilities to each of its subscribers and relying parties.

(c) The Certifying Authority shall as approved, in respect of security and risk management controls continuously ensure that security policies and safeguards are in place. Such controls include personnel security and incident handling measures to prevent fraud and security breaches.

(iii) Certificate and Key Management-

(a) To ensure the integrity of its digital certificates, the Certifying Authority shall ensure the use of approved security controls in the certificate management processes, i.e. certificate registration, generation, issuance, publication, renewal, suspension, revocation and archival.

(b) The method of verification of the identity of the applicant of a Public Key Certificates shall be commensurate with the level of assurance accorded to the certificate.

(c) The Certifying Authority shall ensure the continued accessibility and availability of its Public Key Certificates and Certificate Revocation Lists in its repository to its subscribers and relying parties.

(d) In the event of a compromise of the private key the Certifying Authority shall follow the established procedures for immediate revocation of the affected subscribers' certificates.

(e) The Certifying Authority shall make available the information relating to certificates issued and/or revoked by it to the Controller for inclusion in the National Repository.

(f) The private key of the Certifying Authority shall be adequately secured at each phase of its life cycle, i.e. key generation, distribution, storage, usage, backup, archival and destruction.

(g) The private key of the Certifying Authority shall be stored in high security module in accordance with FIPS 140-1 level 3 recommendations for Cryptographic Modules Validation List.

(h) Continued availability of the private key be ensured through approved backup measures in the event of loss or corruption of its private key.

(i) All submissions of Public Key Certificates and Certificate Revocation Lists to the National Repository of the Controller must ensure that subscribers and relying parties are able to access the National Repository using LDAP ver 3 for X.500 Directories.

(j) The Certifying Authority shall ensure that the subscriber can verify the Certifying Authority's Public Key Certificate, if he chooses to do so, by having access to the Public Key Certificate of the Controller.

(iv) Systems and Operations-

(a) The Certifying Authority shall prepare detailed manuals for performing all its activities and shall scrupulously adhere to them.

(b) Approved access and integrity controls such as intrusion detection, virus scanning, prevention of denial-of service attacks and physical security measures shall be followed by the Certifying Authority for all its systems that store and process the subscribers' information and certificates.

(c) The Certifying Authority shall maintain records of all activities and review them regularly to detect any anomaly in the system.

(v) Physical, procedural and personnel security-

(a) Every Certifying Authority shall get an independent periodic audit done through an approved auditor. Such periodic audits shall focus on the following issues among others :-

(i) changes/additions in physical controls such as site location, access, etc;

(ii) re-deployment of personnel from an approved role/task to a new one;

(iii) appropriate security clearances for outgoing employees such as deletion of keys and all access privileges;

(iv) thorough background checks, etc. during employment of new personnel.

(b) The Certifying Authority shall follow approved procedures to ensure that all the activities referred to in (i) to (iv) in subregulation (a) are recorded properly and made available during audits.

(vi) Financial-

(a) Every Certifying Authority shall comply with all the financial parameters during the period of validity of the licence, issued under the Act.

(b) Any loss to the subscriber, which is attributable to the Certifying Authority, shall be made good by the Certifying Authority.

(vii) Compliance Audits-

(a) The Certifying Authority shall subject itself to Compliance Audits that shall be carried out by one of the empanelled Auditors duly authorized by the Controller for the purpose. Such audits shall be based on the Internet Engineering Task Force document RFC 2527 – Internet X.509 PKI Certificate Policy and Certification Practices Framework.

(b) If a Digital Signature Certificate issued by the Certifying Authority is found to be fictitious or that proper identification procedures have not been followed by the Certifying Authority while issuing such certificate, the Certifying Authority shall be liable for any losses resulting out of this lapse and shall be liable to pay compensation as decided by the Controller.

22. Application for licence.⁵⁷

(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by-

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

COMMENTS:

Rules 10 and 11 of the *Information Technology (Certifying Authorities) Rules, 2000* are relevant in this regard. They state:

10. Submission of Application.-

Every application for a licensed Certifying Authority shall be made to the Controller,-

(i) in the form given at Schedule-l; and

(ii) in such manner as the Controller may, from time to time, determine, supported by such documents and information as the Controller may require and it shall inter alia include-

(a) a Certification Practice Statement (CPS);

(b) a statement including the procedures with respect to identification of the applicant;

(c) a statement for the purpose and scope of anticipated Digital Signature Certificate technology, management, or operations to be outsourced;

(d) certified copies of the business registration documents of Certifying Authority that intends to be licensed;

⁵⁷ Also refer to Circular No. 1/2001 dated 9th July 2001 titled "GUIDELINES FOR SUBMISSION OF APPLICATION FOR LICENCE TO OPERATE AS A CERTIFYING AUTHORITY UNDER THE IT ACT, 2000" issued by Office of Controller of Certifying Authorities.

(e) a description of any event, particularly current or past insolvency, that could materially affect the applicant's ability to act as a Certifying Authority;

(f) an undertaking by the applicant that to its best knowledge and belief it can and will comply with the requirements of its Certification Practice Statement;

(g) an undertaking that the Certifying Authority's operation would not commence until its operation and facilities associated with the functions of generation, issue and management of Digital Signature Certificate are audited by the auditors and approved by the Controller in accordance with rule 20;

(h) an undertaking to submit a performance bond or banker's guarantee in accordance with sub-rule (2) of rule 8 within one month of Controller indicating his approval for the grant of licence to operate as a Certifying Authority;

(i) any other information required by the Controller.

11. Fee.—

(1) The application for the grant of a licence shall be accompanied by a nonrefundable fee of twenty-five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(2) The application submitted to the Controller for renewal of Certifying Authority's licence shall be accompanied by a non-refundable fee of five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(3) Fee or any part thereof shall not be refunded if the licence is suspended or revoked during its validity period.

23. Renewal of licence.

An application for renewal of a licence shall be-

(a) in such form;

(b) accompanied by such fees, not exceeding five thousand rupees,

as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

COMMENTS:

Rule 15 of the *Information Technology (Certifying Authorities) Rules,* 2000 is relevant in this regard. It states:

15. Renewal of licence.—

(1) The provisions of rule 8 to rule 13, shall apply in the case of an application for renewal of a licence as it applies to a fresh application for licensed Certifying Authority.

(2) A Certifying Authority shall submit an application for the renewal of its licence not less than forty-five days before the date of expiry of the period of validity of licence.

(3) The application for renewal of licence may be submitted in the form of electronic record subject to such requirements as the Controller may deem fit.

24. Procedure for grant or rejection of licence.

The Controller may, on receipt of an application under subsection (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application:

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

COMMENTS:

Rules 16 and 17 of the *Information Technology (Certifying Authorities) Rules, 2000* are relevant in this regard. They state:

16. Issuance of Licence.—

(1) The Controller may, within four weeks from the date of receipt of the application, after considering the documents accompanying the application and such other factors, as he may deem fit, grant or renew the licence or reject the application:

Provided that in exceptional circumstances and for reasons to be recorded in writing, the period of four weeks may be extended to such period, not exceeding eight weeks in all as the Controller may deem fit.

(2) If the application for licensed Certifying Authority is approved, the applicant shall-

(a) submit a performance bond or furnish a banker's guarantee within one month from the date of such approval to the Controller in accordance with sub-rule (2) of rule 8; and

(b) execute an agreement with the Controller binding himself to comply with the terms and conditions of the licence and the provisions of the Act and the rules made thereunder.

17. Refusal of Licence.—

The Controller may refuse to grant or renew a licence if-

(i) the applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or

(ii) the applicant is in the course of being wound up or liquidated; or

(iii) a receiver has, or a receiver and manager have, been appointed by the court in respect of the applicant; or

(iv) the applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these rules; or

(v) the Controller has invoked performance bond or banker's guarantee; or

(vi) a Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement; or

(vii) a Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with rule 31; or

(viii) the audit report recommends that the Certifying Authority is not worthy of continuing Certifying Authority's operation; or

(ix) a Certifying Authority fails to comply with the directions of the Controller.

25. Suspension of licence.

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,-

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

(c) failed to maintain the procedures and standards specified in section 30⁵⁸.

(d) contravened any provisions of this Act, rule, regulation or order made thereunder,

revoke the licence:

Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under subsection (1), by order suspend such licence pending the completion of any inquiry ordered by him:

Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose licence has been suspended shall issue any Electronic Signature⁵⁹ Certificate during such suspension.

COMMENTS:

Rule 14 of the Information Technology (Certifying Authorities) Rules, 2000 is relevant in this regard. It states:

14. Suspension of Licence.—

(1) The Controller may by order suspend the licence in accordance with the provisions contained in sub-section (2) of section 25 of the Act.

(2) The licence granted to the persons referred to in clauses (a) to

(c) of subrule (1) of rule 8 shall stand suspended when the

⁵⁸ Substituted for the words "(c) failed to maintain the standards specified under clause (b) of sub-section (2) of section 20;" by Information Technology (Removal of Difficulties) Order, 2002 ⁵⁹ The words "electronic signature" substituted for "digital signature" by

Information Technology (Amendment) Act, 2008.

performance bond submitted or the banker's guarantee furnished by such persons is invoked under sub-rule (2) of that rule.

26. Notice of suspension or revocation of licence.

(1) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data base maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories:

Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publicise the contents of data base in such electronic or other media, as he may consider appropriate.

27. Power to delegate.

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions.

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961, (43 of 1961), and shall exercise such powers, subject to such limitations laid down under that Act.

COMMENTS:

Some of the provisions under Chapter XIII of the *Income-tax Act, 1961*, are power regarding discovery, production of evidence, etc., search and seizure, power to requisition books of account, etc., application of seized or requisitioned assets, power to call for information, power of survey,

power to collect certain information, power to inspect registers of companies.

29. Access to computers and data.

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Chapter⁶⁰ has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures.

Every Certifying Authority shall,-

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the electronic signatures 61 are assured;

(ca) be the repository of all Electronic Signature Certificates issued under this Act;⁶²

⁶⁰ The words "any contravention of the provisions of this Chapter" substituted for "any contravention of the provisions of this Act, rules or regulations made thereunder" by Information Technology (Amendment) Act, 2008.

⁶¹ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁶² Inserted by Information Technology (Amendment) Act, 2008.

(cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and⁶³

(d) observe such other standards as may be specified by regulations.

Rule 19 of the *Information Technology (Certifying Authorities) Rules,* 2000 is relevant in this regard. It states:

19. Security Guidelines for Certifying Authorities.—

(1) The Certifying Authorities shall have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labeling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.

(2) Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of Certifying Authority are given in Schedule-III and Schedule-III respectively.

(3) The Certifying Authority shall formulate its Information Technology and Security Policy for operation complying with these guidelines and submit it to the Controller before commencement of operation:

Provided that any change made by the Certifying Authority in the Information Technology and Security Policy shall be submitted by it within two weeks to the Controller.

Regulations 4 and 5 of the *Information Technology (Certifying Authority) Regulations, 2001* are also relevant in this regard. They state:

4. The standards followed by the Certifying Authority for carrying out its functions: –

(1) Every Certifying Authority shall observe the following standards for carrying out different activities associated with its functions.

(a) PKIX (Public Key Infrastructure)

Public Key Infrastructure as recommended by Internet Engineering Task Force (IETF) document draft-ietf-pkix-

⁶³ Inserted by Information Technology (Amendment) Act, 2008.

roadmap-05 for "Internet X.509 Public Key Infrastructure" (March 10, 2000); (b) Public-key cryptography based on the emerging Institute of Electrical and Electronics Engineers (IEEE) standard P1363 for three families: Discrete Logarithm (DL) systems Elliptic Curve Discrete Logarithm (EC) systems Integer Factorization (IF) systems; (c) Public-key Cryptography Standards (PKCS) PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit) PKCS#3 Diffie-Hellman Key Agreement Standard PKCS#5 Password Based Encryption Standard PKCS#6 Extended-Certificate Syntax Standard PKCS#7 Cryptographic Message Syntax standard PKCS#8 Private Key Information Syntax standard PKCS#9 Selected Attribute Types PKCS#10 RSA Certification Request PKCS#11 Cryptographic Token Interface Standard PKCS#12 Portable format for storing/transporting a user's private keys and certificates PKCS#13 Elliptic Curve Cryptography Standard Cryptographic PKCS#15 Token Information Format Standard; (d) Federal Information Processing Standards (FIPS) FIPS 180-1, Secure Hash Standard FIPS 186-1, Digital Signature Standard (DSS) FIPS 140-1 level 3, Security Requirement for Cryptographic Modules; (e) Discrete Logarithm (DL) systems Diffie-Hellman, MQV key agreement DSA, Nyberg-Rueppel signatures; (f) Elliptic Curve (EC) systems Elliptic curve analogs of DL systems; (g) Integer Factorization (IF) systems **RSA** encryption RSA, Rabin-Williams signatures; 133

(h) Key agreement schemes

(i) Signature schemes

DL/EC scheme with message recovery

PSS, FDH, PKCS #1 encoding methods for IF family

PSS-R for message recovery in IF family;

(ii) Encryption schemes

Abdalla-Bellare-Rogaway DHAES for DL/EC family;

(i) Form and size of the key pairs

(1) The minimum key length for Asymmetric cryptosystem (RSA Algorithm) shall be 2048 for the Certifying Authority's key pairs and 1024 for the key pairs used by subscribers.

(2) The Certifying Authority's key pairs shall be changed every three to five years (except during exigencies as in the case of key compromise when the key shall be changed immediately). The Certifying Authority shall take appropriate steps to ensure that key changeover procedures as mentioned in the approved Certificate Practice Statements are adhered to.

(3) The subscriber's key pairs shall be changed every one to two years;

(j) Directory Services (LDAP ver 3)

X.500 for publication of Public Key Certificates and Certificate Revocation

Lists

X.509 version 3 Certificates as specified in ITU RFC 1422

X.509 version 2 Certificate Revocation Lists;

(i) Publication of Public Key Certificate.

The Certifying Authority shall, on acceptance of a Public Key Certificate by a subscriber, publish it on its web site for access by the subscribers and relying parties. The Certifying Authority shall be responsible and shall ensure the transmission of Public Key Certificates and Certificate Revocation Lists to the National Repository of the Controller, for access by subscribers and relying parties. The National Repository shall conform to X.500 Directory Services and provide for access through LDAP Ver 3. The Certifying Authority shall be responsible for ensuring that Public Key Certificates and Certificate Revocation Lists integrate

seamlessly with the National Repository on their transmission;

k) Public Key Certificate Standard

All Public Key Certificates issued by the Certifying Authorities shall conform to International Telecommunication Union X.509 version 3 standard.

(l) Certificate Revocation List Standard -

CRL and CRL Extensions Profile - The CRL contents as per International Telecommunications Union standard ver 2

(2) The list of standards specified in sub-regulation (1) shall be updated at least once a year to include new standards that may emerge from the international bodies. In addition, if any Certifying Authority or a group of Certifying Authorities brings a set of standards to the Controller for a specific user community, the Controller shall examine the same and respond to them within ninety days.

5. (1) Every Certifying Authority shall disclose :-

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any Certification Practice Statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority Certificate, if any; and

(d) any other fact that materially or adversely affect either the reliability of a Digital Signature Certificate, which that Authority has issued by it or the Authority's ability to perform its services.

(2) The above disclosure shall be made available to the Controller through filling up of online forms on the Web site of the Controller on the date and time the information is made public. The Certifying Authority shall digitally sign the information.

31. Certifying Authority to ensure compliance of the Act, etc.

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

32. Display of licence.

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of licence.

(1) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

(2) Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offences and shall be punished with imprisonment which may extend upto six months or a fine which may extend upto ten thousand rupees or with both.

34. Disclosure.

(1) Every Certifying Authority shall disclose in the manner specified by regulations-

(a) its Electronic Signature⁶⁴ Certificate;⁶⁵

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority Certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Electronic Signature⁶⁶ Certificate, which that Authority has issued, or the Authority's ability to perform its services.

⁶⁴ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁶⁵ The words "which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate" omitted by Information Technology (Amendment) Act, 2008.

⁶⁶ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Electronic Signature⁶⁷ Certificate was granted, then, the Certifying Authority shall-

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence: or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

COMMENTS:

Regulation 6 of the *Information Technology (Certifying Authority) Regulations, 2001* is also relevant in this regard. It states:

6. Communication of compromise of Private Key.-

(1) Where the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, the subscriber shall communicate the same without any delay to the Certifying Authority.

(2) An application for revocation of the key pair shall be made in Form online on the web site of the concerned Certifying Authority to enable revocation and publication in the Certificate Revocation List. The Subscriber shall encrypt this transaction by using the public key of the Certifying Authority. The transaction shall be further authenticated with the private key of the subscriber even though it may have already been compromised.

CHAPTER VII - ELECTRONIC SIGNATURE⁶⁸ CERTIFICATES

⁶⁷ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁶⁸ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

35. Certifying Authority to issue Electronic Signature Certificate.⁶⁹

(1) Any person may make an application to the Certifying Authority for the issue of a Electronic Signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.⁷⁰

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Electronic Signature Certificate or for reasons to be recorded in writing, reject the application:

Provided that no Electronic Signature Certificate shall be granted unless the Certifying Authority is satisfied that-

(a) omitted by Information Technology (Amendment) Act, 2008. ⁷¹

(b) the applicant holds a private key, which is capable of creating a electronic signature;

⁶⁹ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

⁷⁰ Also refer to Executive Order dated 12th September, 2002 which states inter alia that "For the purpose of sub-sections (3) and (4) of Section 35 of the Information Technology Act, 2000.... every application for the issue of a Digital Signature Certificate shall not be required to be accompanied by a certificate practice statement as required under the said sub-sections."

⁷¹ (a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(c) the public key to be listed in the certificate can be used to verify a electronic signature affixed by the private key held by the applicant:

Provided that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

COMMENTS:

Rules 23, 24, 25, 26, 27, 28 and 30 of the *Information Technology* (*Certifying Authorities*) *Rules*, 2000 are relevant in this regard. They state:

23. Digital Signature Certificate.—

The Certifying Authority shall, for issuing the Digital Signature Certificates, while complying with the provisions of section 35 of the Act, also comply with the following, namely:-

(a) the Digital Signature Certificate shall be issued only after a Digital Signature Certificate application in the form provided by the Certifying Authority has been submitted by the subscriber to the Certifying Authority and the same has been approved by it:

Provided that the application Form contains, inter alia, the particulars given in the modal Form given in Schedule-IV;

(b) no interim Digital Signature Certificate shall be issued;

(c) the Digital Signature Certificate shall be generated by the Certifying Authority upon receipt of an authorised and validated request for:-(i) new Digital Signature Certificates; (ii) Digital Signature Certificates renewal;

(d) the Digital Signature Certificate must contain or incorporate, by reference such information, as is sufficient to locate or identify one or more repositories in which revocation or suspension of the Digital Signature Certificate will be listed, if the Digital Signature Certificate is suspended or revoked;

(e) the subscriber identity verification method employed for issuance of Digital Signature Certificate shall be specified in the Certification Practice Statement and shall be subject to the approval of the Controller during the application for a licence;

(f) where the Digital Signature Certificate is issued to a person (referred to in this clause as a New Digital Signature Certificate) on the basis of another valid Digital Signature Certificate held by the said person (referred in this clause as an Originating Digital Signature Certificate) and subsequently the originating Digital Signature Certificate has been suspended or revoked, the Certifying Authority that issued the new Digital Signature Certificate shall conduct investigations to determine whether it is necessary to suspend or revoke the new Digital Signature Certificate;

(g) the Certifying Authority shall provide a reasonable opportunity for the subscriber to verify the contents of the Digital Signature Certificate before it is accepted;

(h) if the subscriber accepts the issued Digital Signature Certificate, the Certifying Authority shall publish a signed copy of the Digital Signature Certificate in a repository;

(i) where the Digital Signature Certificate has been issued by the licensed Certifying Authority and accepted by the subscriber, and the Certifying Authority comes to know of any fact, or otherwise, that affects the validity or reliability of such Digital Signature Certificate, it shall notify the same to the subscriber immediately;

(j) all Digital Signature Certificates shall be issued with a designated expiry date.

24. Generation of Digital Signature Certificate.-

The generation of the Digital Signature Certificate shall involve:

(a) receipt of an approved and verified Digital Signature Certificate request;

(b) creating a new Digital Signature Certificate;

(c) binding the key pair associated with the Digital Signature Certificate to a Digital Signature Certificate owner;

(d) issuing the Digital Signature Certificate and the associated public key for operational use;

(e) a distinguished name associated with the Digital Signature Certificate owner; and

(f) a recognized and relevant policy as defined in Certification Practice Statement.

25. Issue of Digital Signature Certificate.—

Before the issue of the Digital Signature Certificate, the Certifying Authority shall:-

(i) confirm that the user's name does not appear in its list of compromised users;

(ii) comply with the procedure as defined in his Certification Practice Statement including verification of identification and/or employment;

(iii) comply with all privacy requirements;

(iv) obtain a consent of the person requesting the Digital Signature Certificate, that the details of such Digital Signature Certificate can be published on a directory service.

26. Certificate Lifetime.—

(1) A Digital Signature Certificate,- (a) shall be issued with a designated expiry date; (b) which is suspended shall return to the operational use, if the suspension is withdrawn in accordance with the provisions of section 37 of the Act; (c) shall expire automatically upon reaching the designated expiry date at which time the Digital Signature Certificate shall be archived; (d) on expiry, shall not be re-used.

(2) The period for which a Digital Signature Certificate has been issued shall not be extended, but a new Digital Signature Certificate may be issued after the expiry of such period.

27. Archival of Digital Signature Certificate.—

A Certifying Authority shall archive-

(a) applications for issue of Digital Signature Certificates;

(b) registration and verification documents of generated Digital Signature Certificates;

(c) Digital Signature Certificates;

(d) notices of suspension;

(e) information of suspended Digital Signature Certificates;

(f) information of revoked Digital Signature Certificates;

(g) expired Digital Signature Certificates, for a minimum period of seven years or for a period in accordance with legal requirement.

28. Compromise of Digital Signature Certificate.—

Digital Signature Certificates in operational use that become compromised shall be revoked in accordance with the procedure

defined in the Certification Practice Statement of Certifying Authority.

Explanation : Digital Signature Certificates shall,-

(a) be deemed to be compromised where the integrity of:- (i) the private key associated with the Digital Signature Certificate is in doubt; (ii) the Digital Signature Certificate owner is in doubt, as to the use, or attempted use of his key pairs, or otherwise, for malicious or unlawful purposes;

(b) remain in the compromised state for only such time as it takes to arrange for revocation.

30. Fees for issue of Digital Signature Certificate.-

(1) The Certifying Authority shall charge such fee for the issue of Digital Signature Certificate as may be prescribed by the Central Government under sub-section (2) of section 35 of the Act.

(2) Fee may be payable in respect of access to Certifying Authority's X.500 directory for certificate downloading. Where fees are payable, Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing fee schedule on a nominated website.

(3) Fees may be payable in respect of access to Certifying Authority's X.500 directory service for certificate revocation or status information. Where fees are payable, Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing the fee schedule on a nominated website.

(4) No fee is to be levied for access to Certification Practice Statement via Internet. A fee may be charged by the Certifying Authority for providing printed copies of its Certification Practice Statement.

36. Representations upon issuance of Digital Signature Certificate.

A Certifying Authority while issuing a Digital Signature Certificate shall certify that-

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder;

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(ca) the subscriber holds a private key which is capable of creating a digital signature;⁷²

(cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber;⁷³

(d) the subscriber's public key and private key constitute a functioning key pair;

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

37. Suspension of Digital Signature Certificate.

- (1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,-
 - (a) on receipt of a request to that effect from-

(i) the subscriber listed in the Digital Signature Certificate; or

(ii) any person duly authorised to act on behalf of that subscriber;

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

⁷² Inserted by Information Technology (Amendment) Act, 2008.

⁷³ Inserted by Information Technology (Amendment) Act, 2008.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate.

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it-

(a) where the subscriber or any other person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that-

> (a) a material fact represent in the Digital Signature Certificate is false or has been concealed;

> (b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

> (c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

> (d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

COMMENTS:

Rule 29 of the *Information Technology (Certifying Authorities) Rules,* 2000 is relevant in this regard. It states:

29. Revocation of Digital Signature Certificate.-

(1) Digital Signature Certificate shall be revoked and become invalid for any trusted use, where- (a) there is a compromise of the Digital Signature Certificate owner's private key; (b) there is a misuse of the Digital Signature Certificate; (c) there is a misrepresentation or errors in the Digital Signature Certificate; (d) the Digital Signature Certificate is no longer required.

(2) The revoked Digital Signature Certificate shall be added to the Certificate Revocation List (CRL).

39. Notice of suspension or revocation.⁷⁴

(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2)Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

CHAPTER VIII - DUTIES OF SUBSCRIBERS

40. Generating key pair.

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, the subscriber shall generate that key pair by applying the security procedure.⁷⁵

⁷⁴ Also refer to Circular No. 1/2002 dated 16th December 2002 titled "GUIDELINES FOR SUBMISSION OF CERTIFICATES AND CRLS TO THE CCA FOR PUBLISHING IN NRDC BY CERTIFYING AUTHORITIES" issued by Office of Controller of Certifying Authorities.

⁷⁵ Substituted for "40. Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure." by Information Technology (Removal of Difficulties) Order, 2002.

40A. Duties of subscriber of Electronic Signature Certificate.

In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.⁷⁶

41. Acceptance of Digital Signature Certificate.

(1) A subscriber shall deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate-

- (a) to one or more persons;
- (b) in a repository; or

otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

> (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

> (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

> (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key.

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure.⁷⁷

⁷⁶ Inserted by Information Technology (Amendment) Act, 2008.

⁷⁷ Substituted for "(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber." by Information Technology (Removal of Difficulties) Order, 2002.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation.- For removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the certifying Authority that the private key has been compromised.

CHAPTER IX - PENALITIES, COMPENSATION AND ADJUDICATION ⁷⁸

43. Penalty and compensation⁷⁹ for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-

(a) accesses or secures access to such computer, computer system or computer network or computer resource⁸⁰;

COMMENTS:

The two concepts covered in this provision are "accesses" and "secures access".

According to section 2(1)(a) of the *Information Technology Act*, "access" with its grammatical variations and cognate expressions, means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

⁸⁰ The words "or computer resource" inserted by Information Technology (Amendment) Act, 2008.

⁷⁸ The words "PENALITIES, COMPENSATION AND ADJUDICATION" substituted for "PENALTIES AND ADJUDICATION" by Information Technology (Amendment) Act, 2008.

⁷⁹ The words "and Compensation" inserted by Information Technology (Amendment) Act, 2008.

Essentials of the term "access" are: (A) Gaining entry into a computer, computer system or computer network (B) Instructing the logical, arithmetical, or memory function resources of a computer, computer system or computer network (C) Communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Grammatical variations of access include terms such as accesses, accessed, accessing etc. Cognate expressions are related words and phrases. Depending upon the situation, these could include "log on", "retrieve" etc. Gaining entry into applies to physical access. The terms computer, computer system and computer network have been defined very widely under the *Information Technology Act*. These terms may include the physical box (cabinet) in which a computer is housed. They may also include the physical room in which a computer network or super computer is housed.

Illustration: A massive super computer is housed in particular premises. Sameer breaks open the door and enters the premises. He has gained entry into the computer.

Illustration: A Government computer contains critical information in its hard disk. Sameer unscrews the cabinet of the computer in order to steal the hard disk. He has gained entry into the computer.

Instructing means "to give orders" or "to direct". Instructing is essentially a one way process which does not require two-way communication between the instructor and the instructed.

Illustration: A Government computer contains critical information. Sameer enters the room where the computer is located and keys in some commands into the keyboard. He does not realise that the keyboard is disconnected from the computer. Here, Sameer has not instructed the logical, arithmetic or memory functions of the computer.

Communicating with is essentially a two-way process that involves exchange of information.

Illustration: Sameer is a hacker attempting to steal some information from Sanya's computer. He first remotely scans Sanya's computer using specialised software. The software sends out queries to Sanya's computer which replies to the queries. As a result of this, Sameer obtains details of the operating system installed on Sanya's computer. Sameer has communicated with Sanya's computer.

Secures access is a term that needs to be examined next. The term "secure" means "to make certain". The term "secures access" would mean "to make certain that access can be achieved as and when desired by the person seeking to access".

Illustration: Sanya is the network administrator of a Government department. She stores the passwords of the Government department main server in her personal laptop.

Sameer is Sanya's friend. Without Sanya's permission, he switches on her laptop and notes down the passwords of the Government department main server. He has accessed Sanya's laptop without her permission.

He has "secured access" to the Government server. Although he has not accessed the Government server, he has "secured" access to it. By obtaining the passwords, he has made certain that he can access the server as and when he desires.

This section covers incidents where the "permission" of the owner or other person in charge of the computer is not obtained. Permission is the "authorization granted to do something" e.g. Sanya permits Sameer to switch on her computer.

Permission can be express or implied. Permission can also be complete or partial.

Illustration: Sanya is the network administrator of Noodle Ltd. The employment contract that she has signed with Noodle Ltd states that she is responsible for the "complete maintenance and security of the Noodle Ltd computer systems and networks". Noodle Ltd has given her the express permission to access their systems. This is also complete permission. As the network administrator Sanya would need complete access to all parts of the systems.

Illustration: Tanya is an employee of the marketing department of Noodle Ltd. All the marketing department employees have been allotted usernames and passwords which allows them to log into the Noodle Ltd main server. Noodle Ltd has given Tanya the implied permission to access their systems. This is also a partial permission. As an employee of the marketing department, Tanya would need access only to that part of the system that contains information relevant to the marketing department.

This section also covers acts that exceed permission.

Illustration: Sameer is an employee of the finance department of Noodle Ltd. His username and password entitles him to

access only limited information on the official Noodle server. Tanya is the senior manager of the finance department. One day, while Tanya is abroad on official business, she calls up Sameer and gives him her username and password. She requests Sameer to retrieve some official documents from the Noodle server and email those documents to her. Sameer complies with her request.

Several days later, Sameer again uses Tanya's password to access the Noodle server. Now he has exceeded the scope of his permission. Tanya had given Sameer an implied permission to use her password only on one occasion. The subsequent use of the password by Sameer is unauthorised and amounts to exceeding the scope of his permission.

AUSTRALIA:

The relevant provision is section 476.2 of *The Criminal Code* which is titled "Meaning of unauthorised access, modification or impairment and is quoted below:

(1) In this Part:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer; or

(d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means;

by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

(2) Any such access, modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

(3) For the purposes of an offence under this Part, a person causes any such unauthorised access, modification or impairment if the person's conduct substantially contributes to it.

(4) For the purposes of subsection (1), if:

(a) a person causes any access, modification or impairment of a kind mentioned in that subsection; and

(b) the person does so: (i) under a warrant issued under the law of the Commonwealth, a State or a Territory; or (ii) under an emergency authorisation given to the person under Part 3 of the Surveillance Devices Act 2004 or under a law of a State or Territory that makes provision to similar effect; or (iii) under a tracking device authorisation given to the person under section 39 of that Act;

the person is entitled to cause that access, modification or impairment.

CANADA:

The relevant provision is section 342.1 of the *Criminal Code* which is titled "Unauthorized use of computer", and is quoted below:

342.1 (1) Every one who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service,

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

(2) In this section,

"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device that, or a group of interconnected or related devices one or more of which, (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function; "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof;

"traffic" means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way.

JAPAN:

A relevant provision is Article 3(2) of the *Unauthorized Computer Access Law* which is titled "Prohibition of acts of unauthorized computer access". According to this article, the act of unauthorized computer access means an act that falls under one of the following items:

(1) An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another person's identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code);

(2) An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item); (3) An act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication line, any information or command that can evade the restrictions concerned.

Article 2 of the *Unauthorized Computer Access Law* defines some of the relevant terms. It states-

1. In this law, "access administrator" means a person who administers the operations of a computer (hereafter referred to as "specific computer") which is connected to a telecommunication line, with regard to its use (limited to such use as is conducted through the telecommunication line concerned; hereafter referred to as "specific use").

2. In this Law, "identification code" means a code —that is granted to a person (hereafter referred to as "authorized user") who has been authorized by the access administrator governing a specific use of a specific computer to conduct that specific use, or to that access administrator (hereafter in this paragraph, authorized user and access administrator being referred to as "authorized user, etc.") to enable that access administrator to identify that authorized user, etc.; and that falls under any of the following items or that is a combination of a code which falls under any of the following items and any other code:

(1) A code the content of which the access administrator concerned is required not to make known to a third party wantonly;

(2) A code that is compiled in such ways as are defined by the access administrator concerned using an image of the body, in whole or in part, of the authorized user, etc., concerned, or his or her voice;

(3) A code that is compiled in such ways as are defined by the access administrator concerned using the signature of the authorized user, etc., concerned.

3. In this Law, "access control function" means a function that is added, by the access administrator governing a specific use, to a specific computer or to another specific computer which is connected to that specific computer through a telecommunication line in order to automatically control the specific use concerned of that specific computer, and that removes all or part of restrictions on that specific use after confirming that a code inputted into a specific computer having that function by a person who is going to conduct that specific use is the identification code (to include a code which is a combination of a code compiled in such ways as are defined by the access administrator concerned using an identification code and part of that identification code; the same shall apply in Article 3, paragraph 2, items (1) and (2)) for that specific use.

Another relevant provision is Article 4 of the *Unauthorized Computer* Access Law which is titled "Prohibition of acts of facilitating unauthorized computer access". It states-

No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user.

MALAYSIA:

A relevant provision is section 2(5) of the *Computer Crimes Act* which is quoted below:

(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorized if—

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have the consent or exceeds any right or consent to access by him of the kind in question to the program or data from any person who is so entitled.

SINGAPORE:

A relevant provision is section 2(5) of the *Computer Misuse Act*, which states-

(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if —

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

UNITED KINGDOM:

A relevant provision is section 1 of the Computer Misuse Act, which states-

1. Unauthorised access to computer material

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;

(b) the access he intends to secure , or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

UNITED STATES OF AMERICA:

A relevant provision is section 1030 of the US Code [Title 18 - Crimes and Criminal Procedure, Part I – Crimes, Chapter 47 - Fraud And False Statements] which states-

Sec. 1030. Fraud and related activity in connection with computers (a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access,

and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

(5)

(A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) -

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security; (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if -

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is -

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under

subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if -

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)

(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

(5)

(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and (B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section -

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer -

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means -

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) (!2) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or

alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection may be brought under this subsection of the of the date of the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

US CASE LAW:

The following are extracts from *Prosecuting Computer Crimes*, published by Office of Legal Education Executive Office for United States Attorneys:

Many of the criminal offenses contained within the Computer Fraud and Abuse Act (CFAA) require that an intruder either access a computer without authorization or exceed authorized access. The term "without authorization" is not defined in the Act and one court found its meaning "to be elusive." EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) (dicta); see also SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593 (E.D. Va. 2005) (holding that defendants had authorization to use a computer system even though such access violated the terms of a license agreement binding the user who provided them with access to the system).

The term "exceeds authorized access" is defined by the CFAA to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

The legislative history of the CFAA reflects an expectation by Congress that persons who exceed authorized access are likely to be insiders, whereas persons who act without authorization are likely to be outsiders. As a result, Congress restricted the circumstances under which an insider—a user with authorized access—could be held liable for violating section 1030. "[I]nsiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage.

By contrast, outside intruders who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass." See S. Rep. No. 99-432, at 10 (1986), reprinted in 1986 U.S.C.C.A.N. 2479; see also S. Rep. No. 104-357, at 11 (1996), available at 1996 WL 492169.

According to this view, outsiders are intruders with no rights to use a protected computer system, and, therefore, they should be subject to a wider range of criminal prohibitions. Those who act without authorization can be convicted under any of the access offenses contained in the CFAA, which can be found in 18 U.S.C. § 1030(a)(1)-(5). However, users who exceed authorized access have at least some authority to access the computer system. Such users are therefore subject to criminal liability under more narrow circumstances. The offenses that can be charged based on exceeding authorized access are limited to those set forth in subsections (a)(1), (a)(2), and (a)(4). Table 2 below summarizes the authorization requirements of the CFAA offenses. If both the "without authorization" and "exceeds authorization" boxes are checked, the offense can be proven upon either showing. Note that subsections (a)(6) and (a)(7) are not access offenses and therefore have no authorization requirement.

Traditional insider / outsider cases include *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997), where an Internal Revenue Service employee was found to have exceeded his authorized access to IRS computer systems when he looked at taxpayer records for personal purposes, and United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001), where a Russian intruder broke into an American company's customer databases and was found to have acted without authorization.

While the universe of individuals who lack any authorization to access a computer is relatively easy to define, determining whether individuals who possess some legitimate authorization to access a computer have exceeded that authorized access may be more difficult. The term "exceeds authorized access" is defined as follows:

[T]o access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

18 U.S.C. § 1030(e)(6).

The scope of any authorization hinges upon the facts of each case. In the simplest of prosecutions, a defendant without authorization to access a computer may intentionally bypass a technological barrier (such as password protection or system privileges) that prevented him from obtaining information on a computer network. However, many cases will involve exceeding authorized access, and establishing the scope of authorized access will be more complicated. The extent of authorization may turn upon the contents of an employment agreement or similar document, a terms of service notice, or a log-on banner outlining the permissible purposes for accessing a computer or computer network. See Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435 (N.D. Tex. 2004) (user agreement); EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003) (various site notices); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 253 (S.D.N.Y. 2000) (terms of use notice); America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450-51 (E.D. Va. 1998) (terms of service agreement); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) (employee confidentiality agreement).

In one case, however, an insider (a person with some limited authorization to use a system) strayed so far beyond the bounds of his authorization that the court treated him as having acted without authorization. United States v. Morris, 928 F.2d 504 (2d Cir. 1991). Morris was convicted under a previous version of section 1030(a)(5), which punished "intentionally access[ing] a Federal interest computer without authorization." 18 U.S.C. Ş 1030(a)(5)(A) (1988). Morris created an Internet program known as a "worm," which spread to computers across the country and caused damage. To enable the worm to spread, Morris exploited vulnerabilities in two processes he was in fact authorized to use: "sendmail" (an email program) and "fingerd" (a program used to find out certain information about the users of other computers on the network). Morris, 928 F.2d. at 509-10.

On appeal, Morris argued that because he had authorization to engage in certain activities, such as sending electronic mail, on some university computers, he had merely exceeded authorized access, rather than having gained unauthorized access.

The Second Circuit rejected Morris' argument on three grounds. First, it held that the fact that the defendant had authorization to use certain computers on a network did not insulate his behavior when he gained access to other computers that were beyond his authorization. "Congress did not intend an individual's authorized access to one federal interest computer to protect him from prosecution, no matter what other federal interest computers he accesses." Id. at 511. Rather, "Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorized access to other federal interest computers." Id. at 510. Second, the court held that although Morris may have been authorized to use certain generally available functions—such as the email or user query services—on the systems victimized by the "worm," he misused that access in such a way to support a finding that his access was unauthorized. The court wrote that:

Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers.

Id⁸¹. Finally, the court held that even assuming the defendant's initial insertion of the worm simply exceeded his authorized access, evidence demonstrated that the worm was designed to spread to other computers and gain access to those computers without authorization by guessing their passwords.

"Authorized" is a fluid concept. Even when authorization exists, it can be withdrawn or it can lapse. In some instances, a court may invoke agency law to determine whether a defendant possessed or retained authorization to access a computer. See, e.g., Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124 (W.D. Wash. 2000) (finding that insiders with authorization to use a system can lose that authorization when they act as agents of an outside organization).

In Shurgard, employees were found to have acted "without authorization" when they accessed their employer's computers to appropriate trade secrets for the benefit of a competitor. The court applied principles of agency law, and concluded that the employees' authorized access to the employer's computers ended when they became agents of the competitor. Id. at 1124-25. See International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (holding that an employee's access to data became unauthorized when breach of his duty of loyalty terminated his agency relationship). See also Vi Chip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D.Ca. 2006) (applying the holding of Citrin to an employee who deleted data after being informed that his employment was to be terminated). But see

⁸¹ Gauging whether an individual has exceeded authorized access based upon whether the defendant used the technological features of the computer system as "reasonably expected" was criticized by one court as too vague an approach. EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003) (in a civil case under § 1030(a)(4), involving whether use of a web scraper exceeded authorized access, rejected inferring "reasonable expectations" test in favor of express language on the part of the plaintiff).

Lockheed Martin Corp. v. Speed, 2006 WL 2683058 at *5-7 (M.D. Fla. 2006) (criticizing Citrin).

Notably, Shurgard, Citrin, Vi Chip, and Lockheed all involved employees who were accused of abusing-e.g., selling, transferring, or destroying-data to which they had authorized access as part of their jobs. As a result, the plaintiffs were unable to establish that the defendants exceeded authorized access. Instead, in each of these cases the plaintiffs attempted to argue that access became unauthorized when the employee's purpose was not to benefit the employer. Essentially, each argued by reference to the Restatement (Second) of Agency that when the agent's duty of loyalty to his principal was breached, the relationship was terminated and subsequent access was unauthorized. Shurgard, 119 F. Supp. 2d at 1124-25; Citrin, 440 F.3d at 420-21; Vi Chip, 438 F. Supp. 2d. at 1100; Lockheed, 2006 WL 2683058 at *4. To prevail under this theory, a plaintiff needs to convince the court that the relationship was essentially terminated-i.e., the authorization to access the data was losteven while the employee was still technically in its employ. The courts in Shurgard, Citrin, and Vi Chip agreed with this rationale, but the court in Lockheed did not. Shurgard, 119 F. Supp. 2d at 1124-25; Citrin, 440 F.3d at 420-21; Vi Chip, 438 F. Supp. 2d. at 1100; Lockheed, 2006 WL 2683058 at *5-7. Prosecutors faced with similar facts may want to consider charging an offense that does not contain an authorization requirement, such as section 1030(a)(5)(A)(i).

One court found that insiders acted without authorization when they violated clearly defined computer access policies. See, e.g., America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (holding that AOL members acted without authorization when they used AOL network to send unsolicited bulk emails in violation of AOL's member agreement). But see America Online, Inc. v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255 (N.D. Iowa 2000) (noting that no other published decision contains the same interpretation as America Online, Inc. v. LCGM, Inc. on the issue of unauthorized access).

Typically, however, persons who are employees or licensees of the entity whose computer they used are held liable for exceeding authorized access as opposed to unauthorized access. See EF Cultural Travel, 274 F.3d at 582-84 (holding that a former employee who violated a confidentiality agreement by providing information about accessing a protected computer system could be liable for exceeding authorized access). In SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593 (E.D. Va. 2005), the Court dismissed a claim that defendants, who gained access to a protected computer due to breach of a software license by a licensee, either exceeded authorized access or gained unauthorized access. The court believed that the licensee had given the defendants authority to use the computer system, which undercut the plaintiff's unauthorized use claim. Id. at 608-09. Moreover, since it was the licensee and not the defendants who agreed to the terms of the license, the defendants were not bound to the use limitations, and therefore, had not exceeded authorized access. Id. at 609-10. The court noted, however, that had the licensee-as opposed to the persons who gained access to the system via the licensee-been sued for exceeding authorized use, they may have been found liable under theory set forth in EF Cultural Travel. Id. at 609 (citing EF Cultural Travel BV, 274 F.3d at 582).

The SecureInfo decision is troublesome in that it could arguably be read to support the proposition that users who are granted access to a system by an authorized user cannot be found liable under either an unauthorized use or an in excess of authorization theory. Presumably, however, had the third parties used their authorized access to obtain information unavailable to even licensed users, the court would have held them liable. The better reading of this decision is that courts may be reluctant to predicate civil liability, much less criminal liability, under the CFAA solely upon a violation of a software licensing agreement.

In sum, "without authorization" generally refers to intrusions by outsiders, but some courts have also applied the term to intrusions by insiders who access computers other than the computer they are authorized to use, intrusions by insiders acting as agents for outsiders, and intrusions by insiders who violate clearly defined access policies. Section 1030 imposes greater liability on outsiders because their very presence on the computer or network constitutes trespass. Thus, certain subsections (18 U.S.C. §§ 1030(a)(3), (a)(5)(A)(ii), & (a)(5)(A)(iii)) criminalize actions based upon access without authorization, but do not impose the same liability if the access merely exceeds authorization. In any event, it is clear that courts treat the issue of authority to access as a question of fact under the specific circumstances of each case. Prosecutors should consider not only whether the access breached technical security measures (such as passwords), but also employer policies, banners, user agreements, contracts, licenses, or similar items.

CONVENTION ON CYBERCRIME:

Article 2 of the *Convention on Cybercrime* of the Council of Europe is titled "Illegal access" and states-

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

(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;

COMMENTS:

This section penalises the following unauthorised acts: (1) downloading from a computer, computer system or computer network, (2) copying from a computer, computer system or computer network, (3) extracting data, database or information from a computer, computer system or computer network. Let us examine some of these terms in detail.

The term *download* is generally used for transferring information, software etc -(1) from a remote or distant to a nearby computer (2) from a larger to a smaller computer (3) from a computer to a peripheral device (e.g. floppy or pen-drive).

Illustration: Sameer is browsing the Internet and comes across a useful software program stored on a website. He downloads it from the Internet onto his computer. He then installs it on his computer.

Illustration: Pooja uses her personal laptop to connect to her office server. She then downloads the Office Manual from the server onto her laptop.

Illustration: Pooja makes an online purchase of some songs. After the payment is processed, she downloads the song from the

music company's website onto her cell phone which is connected to her laptop.

Copies means "to duplicate or reproduce or imitate something". The original information is not affected by the copying. It remains unchanged. The copied information may be in a different format as compared to the format of the original information. This can be understood from the following examples.

Illustration: Pooja stores all her important data on her laptop in the "D" drive. In order to prevent accidental deletion of her data, she copies it onto the "E" drive of her laptop.

Illustration: Pooja reads a very funny joke on a website. The website has stored the joke in an image file so that people cannot simply copy the joke and email it to their friends. The website wants users to refer their friends to its webpage in order to read the joke. Pooja reads the joke on the website and then types it in word by word into a text file in her computer. She has copied the joke.

Illustration: Pooja has created an MS Word document on her laptop. She then uses specialised software to convert the document into a PDF (Portable Document Format) file. She has copied the original file and reproduced it in a new format.

Illustration: Pooja has purchased a CD containing dozens of songs in mp3 format. Using her computer, she copies the songs from the CD onto her cell phone.

Extracts means to derive or obtain something. Extracting usually requires some special effort or skill.

Illustration: Pooja has purchased a CD containing songs in "cda" format. Using her computer, she converts the songs into 'mp3' format. She has extracted the mp3 format songs from the audio CD that she had purchased.

Illustration: Pooja obtains the source code files for open source software. She then uses "compiler" software to convert the source code files into the executable file. This executable file can be used to install the software onto a computer. She has extracted the executable file from the source code files.

Illustration: Pooja obtains a software executable file. She then uses "decompiler" software to obtain the source code files that were used to create the executable file. She has extracted the source code file from the executable file. *Data* is a formalised representation of information, knowledge, facts, concepts or instructions. Data undergoes processing by a computer. Data can be in electronic form (e.g. stored in a CD) or physical form (e.g. computer printouts). Examples of data include computerised attendance records of a school, information in the RAM of a computer, printouts of a computerised accounting system etc.

Computer data base is a formalised representation of information. The term includes information produced by a computer and intended for use in a computer. This is best understood through the following illustration.

Illustration: Noodle School has an automated system for student administration. This system is powered by a database that contains detailed student information. One table of this database is titled "basic_info" and contains the following categories of information.

Roll no.	Name	Address	Phone	Email

Another table is titled "student_marks" and contains the following categories of information:

Roll no.	Test 1	Test 2	Test 3	Final

When a student's report card is to be prepared, the system automatically takes the marks from the "student_marks" table and the name and contact information from the "basic_details" table. It then collates the information and prepares the final report card.

Information includes data, text, images, sound, voice, codes, computer programmes, software and databases or microfilm or computer generated micro fiche. Microfilms are processed sheets of plastic (similar to the commonly used photograph rolls) that carry images of documents. These images are usually about 25 times reduced from the original document size. The images cannot be read by the naked eye and special readers are used to project the images on a screen. They are most commonly used in libraries for transmission, storage, reading and printing of books. Microfiche is a type of microfilm which carries several micro images.

Illustration: The following are information: (1) a photo stored on a DVD (2) a song stored on a CD (3) the ebook version of this book (4) a recording of a phone conversation.

Removable storage medium is a storage medium that retains the stored information even after it has been removed from a computer e.g. hard disks, floppies, USB disks, zip drives, CD, VCD, DVD. The RAM of a computer would not be removable storage medium as it loses all stored data as soon as it is removed from the host computer.

It is relevant to note section 81 of the *Information Technology Act*, which states-

81. Act to have overriding effect. –

The provisions of this Act shall have effect notwithstanding anything consistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 or the Patents Act, 1970.

Sub-sections (aa), (ab), (ac) and (ad) of section 52 of the *Copyright Act* are relevant. They state-

(aa) the making of copies or adaptation of a computer programme by the lawful possessor of a copy of such computer programme from such copy- (i) in order to utilise the computer programme for the purpose for which it was supplied; or (ii) to make back-up copies purely as a temporary protection against toss, destruction or damage in order only to utilise the computer programme for the purpose for which it was supplied;

(ab) the doing of any act necessary to obtain information essential for operating inter-operability of an independently created computer programme with other programmes by a lawful possessor of a computer programme provided that such information is not otherwise readily available;

(ac) the observation, study or test of functioning of the computer programme in order to determine the ideas and principles which underline any elements of the programme while performing such acts necessary for the functions for which the computer programme was supplied;

(ad) the making of copies or adaption of the computer programme from a personally legally obtained copy for non-commercial personal use;

Section 47 of the Patent Act is relevant. It states-

Section 47 - Grant of patents to be subject to certain conditions

The grant of patent under this Act shall be subject to the condition that—

(1) any machine, apparatus or other article in respect of which the patent is granted or any article made by using a process in respect of which the patent is granted, may be imported or made by or on behalf of the Government for the purpose merely of its own use;

(2) any process in respect of which the patent is granted may be used by or on behalf of the Government for the purpose merely of its own use;

(3) any machine, apparatus or other article in respect of which the patent is granted or any article made by the use of the process in respect of which the patent is granted, may be made or used, and any process in respect of which the patent is granted may be used, by any person, for the purpose merely of experiment or research including the imparting of instructions to pupils; and

(4) in the case of a patent in respect of any medicine or drug, the medicine or drug may be imported by the Government for the purpose merely of its own use or for distribution in any dispensary, hospital or other medical institution maintained by or on behalf of the Government or any other dispensary, hospital or other medical institution which the Central Government may, having regard to the public service that such dispensary, hospital or medical institution renders, specify in this behalf by notification in the Official Gazette.

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

COMMENTS:

This section penalises two acts namely: (1) introducing a virus or contaminant into a computer, (2) causing the introduction of a virus or contaminant into a computer.

These acts may be directed towards a computer, a computer system or computer network. Let us discuss the important terms:

Computer virus means any computer instruction, information, data or programme that (1) destroys, damages, degrades or adversely affects the performance of a computer resource or (2) attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource. **Illustration:** The Love Bug virus comes as an attachment to an email with the subject "I Love You". When a victim clicks on the attachment, the virus overwrites all files on the victim's computer with junk data thereby destroying and damaging all the data.

Illustration: Macro viruses usually come embedded in Microsoft Word and Excel files. When a user runs the infected file, the macro virus gets activated and damages his data.

Illustration: The Chernobyl virus can lie dormant for the entire year in a victim's computer. Most versions of the virus get activated only on April 26th. The virus which was originally called CIH is referred to as the Chernobyl Virus because it attacks on April 26th which is the date when the Chernobyl nuclear accident took place in Ukraine in 1986.

Computer contaminant means any set of computer instructions that are designed to (1) modify, destroy, record, transmit data or programme residing within a computer, or (2) usurp the normal operation of the computer.

Illustration: Sameer sends an online greeting card to Pooja. The greeting card is an image file that is infected with a "Computer Trojan". When Pooja clicks on the greeting card to view it, the Trojan gets installed on her computer. The Trojan usurps the functioning of Pooja's computer. It gives complete control of the computer to Sameer. He can now remotely alter files on Pooja's computer. This is an example of a computer contaminant.

Illustration: Sameer installs a key logger on a cyber café computer. The key logger automatically records all text entered on the infected computer by users. Every evening at 5 pm the key logger transmits this recorded data to Sameer's email account. This is an example of a computer contaminant.

(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;

COMMENTS:

This section penalises two acts namely (1) damaging and (2) causing to be damaged. These acts may be directed towards a computer, a computer

system, computer network, data, computer database or other programs. Let us discuss the important terms:

Data is a formalised representation of information, knowledge, facts, concepts or instructions. Data undergoes processing by a computer. Data can be in electronic form (e.g. stored in a CD) or physical form (e.g. computer printouts). Examples of data include computerised attendance records of a school, information in the RAM of a computer, printouts of a computerised accounting system etc.

Computer database is a formalised representation of information. The term includes information produced by a computer and intended for use in a computer. This is best understood through the following illustration.

Illustration: Noodle School has an automated system for student administration. This system is powered by a database that contains detailed student information. One table of this database is titled "basic_info" and contains the following categories of information.

Roll no.	Name	Address	Phone	Email

Another table is titled "student_marks" and contains the following categories of information:

Roll no.	Test 1	Test 2	Test 3	Final

When a student's report card is to be prepared, the system automatically takes the marks from the "student_marks" table and the name and contact information from the "basic_details" table. It then collates the information and prepares the final report card.

Damage for the purposes of this section implies to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Illustration: Sameer deletes the "address column" of the "basic_info" table of the Noodle School database from the illustration above. Now, although the final report card can be prepared, the address labels to courier the report cards cannot be prepared. Sameer has damaged the database.

Illustration: Sameer picks up Pooja's laptop with the intention of stealing it. He then accidentally drops it on the floor, thereby destroying it. Sameer has damaged Pooja's laptop.

To cause means to make something happen. Cause can be direct or indirect.

Illustration: Sameer pressed the "delete" button on the keyboard causing the data to be deleted. Sameer's act of pressing the delete button is the direct cause of the data being deleted.

Illustration: Sameer switched off the power connection to the house, thereby causing the computer to switch off. Due to the sudden switch off, Pooja could not save her data and it was lost. Sameer's act of switching off the power to the house was the indirect cause of the data loss. The unexpected switching off of the computer was the direct cause of the data loss.

CONVENTION ON CYBERCRIME:

Article 4 of the *Convention on Cybercrime* of the Council of Europe is titled "Data interference" and states-

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

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

COMMENTS:

This section penalises two acts namely (1) disrupting and (2) causing to be disrupted. These acts may be directed towards a computer, a computer system or computer network. Let us discuss the important terms:

Disrupting means "to prevent the normal continuance of", "to throw into confusion or disorder", "to interrupt or impede the progress of". Disruption can be total or partial.

Illustration: Noodle Ltd has a large computer network that spans 3 continents. Noodle employees around the globe use the network to transfer important data. Sameer creates a computer worm that affects the Noodle network. The worm multiplies and replicates and clogs up all the resources thereby slowing the Noodle network. Sameer has partially disrupted the Noodle network.

Illustration: Sameer is an employee of the Pune office of Noodle Ltd. The office has a dozen computers connected to each other through a wireless access point. This access point creates a wireless network within the office. Sameer deliberately switches

off the access point. The computers are no longer in a network. Sameer has totally disrupted the Noodle network.

Illustration: Sameer is an employee of the Mumbai office of Noodle Ltd. The office has a medium speed Internet connection. Sameer starts downloading several movies from the Internet simultaneously. This slows down the Internet speed available to the other Noodle employees. Sameer has partially disrupted the Noodle network.

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

COMMENTS:

This section penalises two acts namely: (1) denying an authorised person access to a computer (2) causing the denial of access to an authorised person.

These acts may be directed towards a computer, a computer system or computer network. Let us discuss the important terms:

To deny access means "to restrict access" or "to disallow access". This denial can be total or partial.

Illustration: Sameer is the network administrator of the Mumbai office of Noodle Ltd. He is disgruntled that his salary has not been raised. He disables the passwords of the other employees so they are unable to access the Noodle servers. Sameer has totally denied access to the authorised employees.

Illustration: Sameer has created a computer virus that opens up multiple program windows on a victim computer. This virus affects Pooja's computer and opens up hundreds of program windows on her computer. This results in her computer becoming unusable. Sameer has caused total denial of access.

Illustration: A series of more than 125 separate but coordinated denial of service attacks hit the cyber infrastructure of Estonia in early 2007. It is suspected that the attacks were carried out by Russian hackers using sophisticated automated denial of service software. The software made millions of requests to Estonia Government servers. The servers could not handle so many requests and they crashed. This resulted in legitimate users being unable to access the servers. This is a total denial of access.

Illustration: Sameer is the network administrator of the Mumbai office of Noodle Ltd. He is disgruntled that his salary has not been raised. He shuts down one of the Noodle servers. Legitimate users are unable to access that server but can access the other servers. Sameer has caused a partial denial of access.

This section does not penalize instances where an unauthorised person is denied access to a computer.

Illustration: The senior management of Noodle Ltd is suspicious that Sameer is involved in corporate espionage and is selling confidential information to rival companies. They ask the Noodle network administrator to immediately block Sameer's access to the main servers. Although Sameer has not been officially suspended or removed from his job, he cannot claim damages from Noodle Ltd for this denial of access. The computer systems belong to Noodle Ltd and the management can withdraw access permissions at any time and without giving prior notice.

(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, rules or regulations made thereunder;

COMMENTS:

The essential element of this section is that assistance is provided for obtaining access to a computer in contravention of the IT Act and its allied laws. A person who obtains access to a computer in contravention of the IT Act would be liable under the relevant sections (e.g. 43(a) or 66 or 70 etc). What this section specifically covers is providing assistance to such a person. Such assistance must facilitate the unlawful access.

Assistance is the act of helping or aiding.

Facilitate means "to make easier" or "to make less difficult" or to "assist in the progress of".

Let us consider some illustrations to understand this concept.

Illustration: Sameer is planning to gain unauthorised access into the computer systems of Noodle Bank Ltd. Aditi, the manager of Noodle, hands over a list of passwords to Sameer. Using these passwords, Sameer gains the unlawful access. Aditi has provided assistance to Sameer to facilitate his unlawful access. **Illustration:** Sameer is planning to gain unauthorised access into the computer systems of Noodle Bank Ltd. Priyanka, the network security administrator of Noodle, is his good friend. She is monitoring the Intrusion Detection System (IDS) of Noodle at the time when Sameer is launching his attack. The IDS detects the attack and gives a warning. Priyanka deliberately ignores the warning and does not use any measures to stop the attack. Priyanka has provided assistance to Sameer to facilitate his unlawful access.

Illustration: Sameer is planning to gain unauthorised access into the computer systems of Noodle Bank Ltd. Priyanka, the network security administrator of Noodle, is his good friend. She disables the Noodle firewall at the time when Sameer is launching his attack. Priyanka has provided assistance to Sameer to facilitate his unlawful access.

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

COMMENTS:

An illustration to clarify the essential elements of this section is:

(1) Sameer avails of some service e.g. purchases a software

(2) Pooja's account with Noodle Bank is charged for this purchase

(3) This has been done by Sameer's manipulation of the Noodle Bank computers

Let us discuss the key terms in this section.

Tampering implies "meddling so as to misuse".

Illustration: Pooja has put a "BIOS" password on her computer. This means that as soon as her computer is switched on, it asks for a password. It does not boot up the operating system till this password is entered. Sameer removes the CMOS battery of Pooja's computer for a few minutes. He then puts the battery back and starts her computer. The "BIOS" password gets deleted and he is able to obtain unauthorised access to her computer. He has tampered with her computer.

Illustration: Noodle Ltd. has secured its computer network by configuring a firewall. Sameer places a powerful magnet near the computer on which the firewall is configured. Over a few days this magnet corrupts the hard disk and the firewall becomes ineffective. Sameer then remotely secures unauthorised access to

the Noodle network. He has tampered with the Noodle computer.

Manipulating implies "influencing something skilfully in an unfair manner".

Illustration: Pooja is checking her email account with gmail.com. As she is logged in to gmail, the gmail authentication cookie is present on her machine.

She receives an email from Sameer containing a really funny joke. The email contains a link to a site which promises her lots more funny stuff. She clicks on the link and is very happy with the site that opens up.

What she does not realize is that this joke site has forged a request to the gmail "Create Filter" wizard. This creates a filter that forwards a copy of all emails coming into Pooja's account to Sameer!

Gmail accepts the request to create the filter because the genuine gmail account holder (Pooja) is authenticated and logged in at the moment and her session cookie is passed along with the forged request. Sameer has manipulated Pooja's gmail account.

Note: This is a cross-site request forgery (CSRF) attack that transmits unauthorized commands to a website from a trusted user.

Now that we have understood the key terms, let us examine some scenarios where this section would be violated.

Illustration: Pooja regularly uses her computer to log into her online banking account with Noodle Bank. Sameer sends Pooja a spoofed email that appears to come from Noodle Bank. The email contains a link to what appears to be a Noodle Bank webpage. Pooja enters her login details on this webpage (which is actually a forged / phished webpage). Now Sameer has obtained her login information. He then purchases some software online and uses Pooja's online bank account to pay for it. He will be liable under this section.

Illustration: Sameer is a hotel waiter. He secretly notes down credit card information of the hotel customers. He then purchases a software program from a website. In order to pay for the purchase he provides the credit card information of one of the hotel customers. This information is then passed on by the website to the payment gateway (e.g. Master, Visa etc). The automated software at the gateway authenticates the transaction as the credit card information is correct. In reality, the gateway

has been manipulated to allow a fraudulent transaction to go through.

Illustration: Noodle Ltd is a book selling company. Customers can place the orders via phone. They are also required to provide their credit card information on the phone. A Noodle employee enters the order details and the credit card information directly into the Noodle computer systems.

The order is then processed in due course. Sameer has designed the Noodle systems in such a way that every 17^{th} payment is credited to "Noodle" instead of "Noodle". Suppose in a day there are 600 orders. Then the payment for the 17^{th} , 34^{th} , 51^{st} , 68^{th} ... order will be made to a company called "Nooodle" which is owned by Sameer.

In case of these orders the payment is not received by Noodle Ltd but the deliveries are made by them, so the customers never understand the fraud and do not lodge any complaint. Sameer has manipulated the Noodle systems.

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;⁸²

COMMENTS:

The elements of this section are (1) destruction / deletion /alteration of information in a computer, or (2) diminishing value or utility of a computer resource, or (3) injuriously affecting a computer resource

Let us discuss the relevant terms and issues in detail.

Information includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche. Data is a formalised representation of information, knowledge, facts, concepts or instructions. Data undergoes processing by a computer. Data can be in electronic form (e.g. stored in a CD) or physical form (e.g. computer printouts). Examples of data include computerised attendance records of a school, information in the RAM of a computer, printouts of a computerised accounting system etc.

Microfilms are processed sheets of plastic (similar to the commonly used photograph rolls) that carry images of documents. These images are usually about 25 times reduced from the original. The images cannot be

⁸² Inserted by Information Technology (Amendment) Act, 2008.

viewed by the naked eye and special readers are used to project the images on a screen. They are most commonly used in libraries for transmission, storage, reading and printing of books.

Microfiche is a type of microfilm containing several micro images.

Illustration: The following are information: (1) photos stored on a DVD (2) songs stored on a CD (3) the ebook version of this book (4) the recording of a phone conversation.

Computer resource includes computer, computer system, computer network, data, computer data base or software.

Information residing in a computer resource must be construed in a wide manner. It includes information that exists or is present in a computer resource temporarily or permanently. This is best discussed through the following illustrations.

Illustration: A personal computer has a BIOS chip that contains basic instructions needed to boot up a computer. These instructions are in the form of "information permanently residing" on the BIOS (which is a computer resource).

Illustration: Pooja is browsing a website. While she is viewing the website on her monitor, the information is cached in her computer in a folder specially reserved for temporary files. Some of that information is also stored in the RAM of her computer. When the computer is shutdown, the information in the RAM is lost. These are examples of information that is "temporarily residing" in a computer resource.

Illustration: Other illustrations of information residing in a computer resource are: (1) music files stored in an iPod (2) software installed on a computer (3) ebook stored on a CD (4) software installed in a cell phone (5) software embedded in a microwave oven.

Destroy means "to make useless", "cause to cease to exist", "nullify", "to demolish", or "reduce to nothing".

Destroying information also includes acts that render the information useless for the purpose for which it had been created.

Illustration: Noodle Ltd has created a vast database of customer details and buying habits. The Noodle managers can query this database using a sophisticated "query management system".

Sameer has developed this unique and path breaking "query management system" entirely on his own. One day, Sameer quits his job and takes the entire code of the "query management system" with him.

Now the information in the database is still intact but it is no longer usable for the purpose of predicting customer orders. Sameer has, in effect, destroyed the information contained in the database.

Deletes in relation to electronic information means "to remove", "to erase", "to make invisible" etc. Such deletion can be temporary or permanent.

Illustration: Pooja has created a text file containing her resume. Sameer deletes the file from her computer. On deletion, the file gets automatically transferred to the "recycle bin" of Pooja's computer, from where it can be easily retrieved. Here Sameer has temporarily deleted the file. Sameer empties the "recycle bin" of Pooja's computer. The file is still only temporarily deleted as it can be recovered using cyber forensics.

Sameer then uses specialised wiping software so that the file cannot be recovered using forensics. Now he has permanently deleted the file.

Illustration: Pooja is a novice computer user. She has created a text file containing her resume. Sameer changes the properties of the file and makes it a "hidden" file. Although the file still exists on Pooja's computer, she can no longer see it. Sameer has deleted the file.

Alters, in relation to electronic information, means "modifies", "changes", "makes different" etc. This modification or change could be in respect to size, properties, format, value, utility etc. Alteration can be permanent or temporary. It can also be reversible or irreversible.

Illustration: Pooja has created a webpage for her client. A webpage is essentially an HTML (Hyper Text Markup Language) file. Sameer changes the file from HTML to text format. He has altered the file. This is a reversible alteration.

Illustration: Pooja has created a text file. Sameer changes the properties of the file and makes it a "hidden" file. The file retains its original content but it has been altered as its attributes have changed (it is now a hidden file). This is a reversible alteration.

Illustration: Pooja has created a text file named "pooja.txt". Sameer changes the name of this file to "pooja1.txt". Although the file retains its original content, it has been altered. This is a reversible alteration.

Illustration: Pooja is investigating Sameer's computer for suspected cyber pornography. She seizes a word file that contains incriminating evidence against Sameer. As per procedure, she computes the hash value of the file and notes it in her report.

Sameer later manages to access the seized file and adds a "#" symbol to the contents of the file. The hash value of this altered file will be different from the hash value computed earlier by Pooja.

This is a permanent irreversible alteration. Even after the "#" symbol is removed, the hash value of the file will never be the same as the original computed by Pooja.

Illustration: Pooja is a graphics designer. She creates very high resolution images for her clients. A high resolution image can be magnified several times and still look clear.

Sameer is one of her employees. He changes some of the high resolution images into low resolution images. Although the low resolution images look the same as the high resolution ones, they cannot be magnified. The value and utility of the images has been reduced. This is an example of permanent and irreversible alteration.

Value implies monetary worth.

Illustration: Pooja is a graphics designer. She buys a sophisticated computer for Rs 2 lakh. The value of the computer is Rs 2 lakh. She purchases one license of specialised graphics software for Rs 50,000 and installs the software on her computer. The value of the computer is now Rs 2.5 lakh. She then hires a specialist to configure her computer for optimal performance. The specialist charges her Rs 10,000 for his services. The value of the computer is now Rs 2.6 lakh.

Utility means "usefulness".

Illustration: The utility of a high resolution image lies in its ability to be magnified several times. This enables the image to be used for various purposes such as on a website, in a printed catalogue, on a large hoarding etc.

Illustration: The utility of anti-virus software lies in its ability to detect computer viruses and other malicious code.

Illustration: The utility of a sophisticated computer is its ability to render high resolution graphics files in a very short time.

Diminish means "reduce" or "lessen",

Illustration: A computer worm replicates itself and thereby hogs up system resources such as hard disk space, bandwidth etc. This can diminish the performance and speed of the computer network.

Diminishes value means "reduces the monetary worth".

Illustration: Pooja is a graphics designer. She creates very high resolution images for her clients. A high resolution image can be magnified several times and still look clear. She can sell each image for around Rs 5000.

Sameer is one of her employees. He changes some of the high resolution images into low resolution images. Although the low resolution images look the same as the high resolution ones, they cannot be magnified. Now she cannot sell an image for more than Rs 400. Sameer has thus diminished the value of the images.

Diminishes utility means "reduces the usefulness".

Illustration: Pooja has purchased a very sophisticated computer that has 2 GB RAM. This enables the computer to render a large image file in 3 seconds. Sameer steals 1 GB RAM from the computer. Now the computer takes more than 5 seconds to render the image file. Sameer's act of stealing the RAM has diminished the utility of Pooja's computer.

Affects means "influences" or "produces a change in".

Illustration: A computer virus changes the data stored in a computer. The virus affects the data.

Injurious means "harmful", "hurtful", or "detrimental".

Illustration: A computer virus is injurious to the data stored in a computer.

Affects injuriously means produces a "harmful or detrimental change".

Illustration: Placing a powerful magnet close to a floppy disk causes permanent and irreversible damage to the disk. We can say that the magnet affects the disk injuriously.

Illustration: Dropping a laptop on the floor can affect it injuriously.

Illustration: Dropping water on a laptop can affect it injuriously.

(j) steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code

used for a computer resource with an intention to cause damage; $^{\rm 83}$

COMMENTS:

Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. Computer source code need not only be in the electronic form. It can be printed on paper (e.g. printouts of flowcharts for designing a software application).

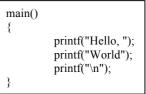
Let us understand this using some illustrations.

Illustration: Pooja has created a simple computer program. When a user double-clicks on the *hello.exe* file created by Pooja, the following small screen opens up:

Hello World

The *hello.exe* file created by Pooja is the executable file that she can give to others. The small screen that opens up is the output of the software program written by Pooja.

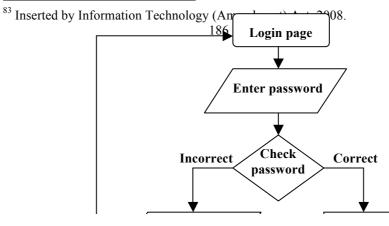
Pooja has created the executable file using the programming language called "C". Using this programming language, she created the following lines of code:



These lines of code are referred to as the source code.

Illustration: Noodle Ltd has created software for viewing and creating image files. The programmers who developed this program used the computer-programming language called Visual C++. Using the syntax of these languages, they wrote thousands of lines of code. This code is then compiled into an executable file and given to end-users. All that the end user has to do is double-click on a file (called setup.exe) and the program gets installed on his computer. The lines of code are known as computer source code.

Illustration: Pooja is creating a simple website. A registered user of the website would have to enter the correct password to access the content of the website. She creates the following



flowchart outlining the functioning of the authentication process of the website.

She takes a printout of the flowchart to discuss it with her client. The printout is source code.

The following acts are prohibited in respect of the source code (1) stealing, concealing, destroying or altering (2) causing another to steal, conceal, destroy or alter.

Let us discuss the relevant terms and issues in detail.

The term steal and "commit theft" are usually used interchangeably. Section 378 of the Indian Penal Code defines theft as "Whoever intending to take dishonestly any moveable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft."

Illustration: Pooja has created a software program. The source code files of the program are contained in a pen-drive. Sameer takes that pen-drive out of Pooja's cupboard without informing her. He has "stolen" the source code.

Conceal simply means "to hide".

Illustration: Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer changes the properties of the folder and makes it a "hidden" folder.

Although the source code folder still exists on Pooja's computer, she can no longer see it. Sameer has concealed the source code.

Destroy means "to make useless", "cause to cease to exist", "nullify", "to demolish", or "reduce to nothing".

Destroying source code also includes acts that render the source code useless for the purpose for which it had been created.

Illustration: Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer deletes the folder. He has destroyed the source code.

Illustration: Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer deletes one of the source code files. Now the source code cannot be compiled into the final product. He has destroyed the source code.

Illustration: Pooja is designing a software program. She draws out the flowchart depicting the outline of the functioning of the program. Sameer tears up the paper on which she had drawn the flowchart. Sameer has destroyed the source code.

Alters, in relation to source code, means "modifies", "changes", "makes different" etc. This modification or change could be in respect to size, properties, format, value, utility etc.

Illustration: Pooja has created a webpage for her client. The source code of the webpage is in HTML (Hyper Text Markup Language) format. Sameer changes the file from HTML to text format. He has altered the source code.

he shall be liable to pay damages by way of compensation to the person so affected. ⁸⁴

COMMENTS:

Compensation is usually the money that the Court orders the offender to pay to the victim. The Court orders this compensation to be paid when the acts of the offender have caused loss or injury to the victim.

Simply put, damages are the compensation for legal injury. Damages can be of various types:

⁸⁴ The words "he shall be liable to pay damages by way of compensation to the person so affected" substituted for "he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."

(1) Compensatory damages are allowed as a recompense for injury actually suffered.

Illustration: Sameer physically damages Pooja's laptop by dropping it on the floor. The Court orders Sameer to pay compensation equal to the cost of the laptop as paid by Pooja.

(2) Consequential damages are consequential upon the act complained of.

Illustration: Sameer physically damages Pooja's laptop by dropping it on the floor. Pooja has to purchase a new laptop. The Court orders Sameer to pay compensation equal to the price of a new laptop.

(3) Exemplary or punitive damages are awarded as a punishment and serve as a warning to others.

Illustration: Sameer is Pooja's business rival. He destroys Pooja's data by physically damaging her laptop. The Court orders Sameer to pay compensation equal to 10 times the price of a new laptop.

(4) General damages are awarded for things such as mental agony, loss of reputation etc. Such things cannot be accurately stated in terms of money.

Illustration: Sameer posts a defamatory post about Pooja on a social networking website. This harms Pooja's reputation and causes her mental agony. The Court orders Sameer to pay her Rs 10 lakh as compensation.

Explanation. - For the purposes of this section,-

(i) "computer contaminant" means any set of computer instructions that are designed –

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.⁸⁵

43 A. Compensation for failure to protect data⁸⁶

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is 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.

Explanation – For the purposes of this section,-

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security

⁸⁵ Inserted by Information Technology (Amendment) Act, 2008.

⁸⁶ Inserted by Information Technology (Amendment) Act, 2008.

practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

COMMENTS:

Relevent provisions are contained in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

These rules relate to information of two primary types: (1) "Personal information" which means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

(2) "Sensitive personal data or information" of a person which means such personal information which consists of information relating to: (a) password; (b) financial information such as Bank account or credit card or debit card or other payment instrument details; (c) physical, physiological and mental health condition; (d) sexual orientation; (e) medical records and history; (f) Biometric information; (g) any detail relating to the above clauses as provided to body corporate for providing service; and h. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

Sensitive personal data or information does not include any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law.

These rules apply to all those who collect, receive, possess, store, deal or handle information of individuals during the course of commercial or professional activities. These include companies, partnerships, associations, sole proprietorships etc. They also include professionals like doctors, lawyers, chartered accountants etc.

An indicative list of those covered by the Data Privacy Rules include:

1. Insurance companies in respect of information relating to their customers and employees.

2. Banks in respect of information relating to their customers and employees.

3. Hospitals in respect of information relating to their patients and employees.

4. All business organizations (manufacturing, trading etc) in respect of information relating to their employees.

5. Doctors, stock brokers and chartered accountants in respect of information relating to their clients.

6. Retails stores, restaurants, ecommerce companies that collect payment through debit cards, credit cards etc.

7. Call centers, BPOs, LPOs etc.

All these entities are required by law to provide a data privacy policy on their website. This policy should provide details relating to:

1. clear and easily accessible statements of its practices and policies,

2. type of information collected,

3. purpose of collection and usage of such information,

4. disclosure of information

5. reasonable security practices and procedures

All these entities must obtain consent from the provider of the information regarding purpose of usage before collection of such information.

44. Penalty for failure to furnish information, return, etc

If any person who is required under this Act or any rules or regulations made thereunder to-

(a) 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;

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

(c) 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.

45. Residuary penalty.

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.

46. Power to adjudicate.

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder which renders him liable to pay penalty or compensation,⁸⁷ the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.⁸⁸

COMMENTS:

Order no. 2(8)/2000-Pers.I dated 25th March 2003 issued by Government of India, Ministry of Communication and Information Technology, Department of Information Technology is relevant and states-

⁸⁷ The words "direction or order made thereunder which renders him liable to pay penalty or compensation," substituted for the words "direction or order made thereunder" by Information Technology (Amendment) Act, 2008.

⁸⁸ Refer to the Order dated 25th March 2003 [G.S.R.240(E)] which states inter alia that "the Secretary of Department of Information Technology of each of the States or of Union Territories is hereby appointed as Adjudicating Officer for the purposes of the Information Technology Act, 2000."

Also refer to "Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003" dated 17th March 2003.

G.S.R.240(E) In exercise of the powers conferred by sub-section (1) of section 46 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following order/appointments viz. -

1. Whereas sub-section (1) of the section 46 makes provision for appointment of one or more Adjudicating Officers not below the rank of Director to the Central Government and subsection (3) requires that such an officer should possess experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government and whereas such experience necessary for appointment as Adjudicating Officer has been notified by the Central Government as per the Gazette Notification for Information Technology Rules 2003 under the short title Qualification and Experience of Adjudicating Officer and Manner of Holding Enquiry vide Gazette Notification GSR dated March, 2003.

2. Further Whereas the Secretary of the Department of Information Technology of each of the States or Union Territories are normally not below the rank of Director and possess the requisite experience in the field of Information Technology and also possess legal/judicial experience as required, therefore the Secretary of Department of Information Technology of each of the States or of Union Territories is hereby appointed as Adjudicating Officer for the purposes of the Information Technology Act, 2000.

3. The Department of Information Technology of each of the States or of Union Territories shall provide the infrastructure and maintain the records of the matters handled by Adjudicating Officer functioning in the States/Union Territories.

(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore: Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crore shall vest with the competent court.⁸⁹

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for

⁸⁹ Inserted by Information Technology (Amendment) Act, 2008.

making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

COMMENTS:

Rules 4, 5, 6, 7, 8, 9, 10, 11 and 12 of the *Information Technology* (*Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry*) Rules, 2003 are relevant. They state-

4. Scope and Manner of holding inquiry: -

(a) The Adjudicating Officers shall exercise jurisdiction in respect of the contraventions in relation to Chapter IX of IT Act 2000 and the matter or matters or places or area or areas in a State or Union Territory of the posting of the person.

(b) The complaint shall be made to the Adjudicating Officer of the State or Union Territory on the basis of location of Computer System, Computer Network as defined in sub-Section 2 of Section 75 of IT Act on a plain paper on the Proforma attached to these Rules together with the fee payable calculated on the basis of damages claimed by way of compensation.

(c) The Adjudicating Officer, shall issue a notice together with all the documents to all the necessary parties to the proceedings, fixing a date and time for further proceedings. The notice shall contain such particulars as far as may be as to the time and place of the alleged contravention, and the person (if any) against whom, or the thing (if any) in respect of which, it was committed.

(d) On the date so fixed, the Adjudicating Officer shall explain to such person or persons to whom notice is issued about the contravention alleged to have been committed in relation to any of the provisions of the Act or of any rule, regulation, direction or order made there under.

(e) If the person in respect of whom notice is issued pleads guilty, the Adjudicating Officer shall record the plea, and may impose penalty or award such compensation as he thinks fit in accordance with the provisions of the Act, rules, regulations, order or directions made there under.

(f) Alternatively on the date fixed the person or persons against whom a matter is filed may show cause why an enquiry should not be held in the alleged contravention or that why the report alleging the contravention should be dismissed.

(g) The Adjudicating Officer on the basis of the report of the matter, investigation report (if any), other documents and on the basis of submissions shall form an opinion that there is sufficient cause for holding an enquiry or that the report into the matter should be dismissed and on that basis shall either by order dismiss the report of the matter, or shall determine to hear the matter.

(h) If any person or persons fails, neglects or refuses to appear, or present himself as required by sub-rule (d), before the Adjudicating Officer, the Adjudicating Officer shall proceed with the inquiry in the absence of such person or persons after recording the reasons for doing so.

(i) At any time or on receipt of a report of contravention from an aggrieved person, or by a Government agency or suo-moto, the Adjudicating Officer, may get the matter or the report investigated from an officer in the Office of Controller or CERT-IND or from the concerned Deputy Superintendent of Police, to ascertain more facts and whether prima facie there is a case for adjudicating on the matter or not.

(j) The Adjudicating Officer, shall fix a date and time for production of documents or evidence and for this purpose may also rely on electronic records or communications and as far as may be, shall use or make available the infrastructure for promoting on-line settlement of enquiry or disputes or for taking evidence including the services of an adjudicating officer and infrastructure in another State.

(k) As far as possible, every application shall be heard and decided in four months and the whole matter in six months.

(l) Adjudicating Officer, when convinced that the scope of the case extends to the Offence(s) (under Chapter XI of IT Act) instead of Contravention, needing appropriate punishment instead of mere financial penalty, should transfer the case to the Magistrate having jurisdiction to try the case, through Presiding Officer.

5. Order of the Adjudicating Officer: -

(a) If, upon consideration of the evidence produced before the Adjudicating Officer and other records and submissions, the Adjudicating Officer is satisfied that the person has become liable

to pay damages by way of compensation or to pay penalty under any of the provisions of the Act or rules, regulations, directions or orders, the Adjudicating Officer may, by order in writing, order payment of damages by way of compensation or impose such penalty, as deemed fit.

(b) While adjudging the quantum of compensation or penalty, the Adjudicating Officer shall have due regard to the following factors, namely:

(i) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(ii) the amount of loss caused to any person as a result of the default;

(iii) the repetitive nature of the default.

6. Copy of the Order: - Adjudicating Officers shall deliver a certified copy of the order to the Complainant & Respondent.

7. Service of notices and orders: -A notice or an order issued under these rules shall be served on the person in any of the following manners, that is to say: -

(a) by delivering or tendering it to that person or the person's authorized agent in an electronic form provided that there is sufficient evidence of actual delivery of the electronic record to the concerned person; or

(b) by sending it to the person by registered post with acknowledgement due to the address of his place of residence or the last known place of residence or business place;

(c) if it cannot be served under clause (a) or (b) above then by affixing it, in the presence of two witnesses, on the outer door or some other conspicuous part of the premises in which that person resides or is known to have last resided, or carried on business or personally works or last worked for gain.

8. Fee: -

Every complaint of a matter to the Adjudicating Officer shall be accompanied by fee, payable by a bank draft drawn in favour of "Adjudicating Officer Information Technology Act" at the place of functioning of Adjudicating Officer in the States or Union Territories, calculated on the basis of the damages claimed by way of compensation from the contraveners on the rates provided below.

Tab	le	of	Fee	

(i) Damages by way of compensation	Fee	
a) Upto Rs.10,000	10% ad valorem rounded of to nearest next hundred	
b) From 10001 to Rs.50000	Rs. 1000 plus 5% of the amount exceeding Rs.10,000 rounded of to nearest next hundred	
c) From Rs.50001 to Rs.100000	Rs. 3000/- plus 4%of the amount exceeding Rs. 50,000 rounded of to nearest next hundred	
d) More than Rs. 100000	Rs.5000/- plus 2% of the amount exceeding Rs. 100,000 rounded of to nearest next hundred	
(ii) Fee for every application	Rs. 50/-	

9. Duplicity Avoided: -

When an adjudication into a matter of contravention is pending before an Adjudicating Officer, same matter shall not be pursued before any court or Tribunal or Authority in any proceeding whatsoever and if there is already filed a report in relation to the same matter, the proceedings before such other court, Tribunal or Authority shall be deemed to be withdrawn.

10. Frivolous complaints: -

If a person files a frivolous report of the matter, the adjudicating officer in his discretion may order the complainant, to make good the cost of the persons against whom the complaint was filed and to pay a damage of not exceeding Rupees Twenty Five Thousand and the adjudicating officer may also order payment of a fine up to an amount not exceeding Rupees Ten Thousand only.

11. Compounding of Contraventions: -

(a) A person, against whom a report of contravention of the Act, Rules or Regulations, directions or orders or conditions has been filed before an Adjudicating Officer, may make an application for compounding the contravention during the adjudicating proceedings to the concerned adjudicating officer.

Provided that an application for compounding may be filed even before the contravention is reported, in which case the contravener himself shall state the contravention undertaken or committed and the likely loss to various parties and the amount of compensatory damages tendered by the contravener.

(b) The applicant desirous of compounding the contravention shall deposit the sum determined by the officer compounding the contravention into the office of Adjudicating Officer.

Provided that sum determined as compounding fee shall not exceed the maximum amount of penalty, which may be imposed under this Act for the contraventions so compounded.

12. Certifying Authorities and other Governmental Agencies to Assist

All the licensed or recognized Certifying Authorities, the Controller and other officers agencies established under the Act and other government agencies like CERTIND shall promptly assist the Adjudicating Officers in any proceedings filed or pending before the Adjudicating Officers.

APPENDIX

PROFORMA FOR COMPLAINT TO ADJUDICATING OFFICER UNDER INFORMATION TECHNOLOGY ACT - 2000

Ι

- 1. Name of the Complainant
- 2. E-mail address
- 3. Telephone No.
- 4. Address for correspondence
- 5. Digital Signature Certificate, if any

II

- 1. Name of the Respondent
- 2. E-mail address
- 3. Telephone No.

4. Address for correspondence

5. Digital Signature Certificate, if any

III

Damages claimed Fee deposited Demand Draft No._____dated _____Branch_____

IV Complaint under Section/Rule/Direction/Order etc.

V Time of Contravention

VI Place of Contravention

VII Cause of action

VIII Brief facts of the case

(Signature of the Complainant)

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

COMMENTS:

Rule 3 of the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 is relevant. It states-

3. Eligibility for Adjudicating Officer: -

Whereas the purpose and intent of Section 46(3) of IT Act is that the Adjudicating Officer should be a person so qualified and experienced to take decisions with a view in relation to Information Technology aspects as well as in a position to determine the complaints keeping in view the legal or judicial mannerism on the principle of compensation of damages of IT Act.

A person shall not be qualified for appointment as Adjudicating Officer unless the person –

(a) Possesses a University graduate Bachelor degree or equivalent, recognized by Central Government / State Government for the purpose of recruitment to grade I Service in a Government Department through Union / State Public Service Commission; (b) Possesses Information Technology experience in the areas of relevance to public interface with Central / State Government functioning and experience obtained though the in-service training imparting competence to operate computer system to send and receive e-mails or other information through the computer network, exposure and awareness about the method of carrying information, data, sound, images or other electronic records through the medium of network including Internet.

(c) Possesses legal or judicial experience to discharge responsibilities connected with the role of Central / State Government in respect of making decisions or orders in relation to administration of laws as a District Magistrate, or Additional District Magistrate or Sub-Divisional Magistrate or an Executive Magistrate or in other administrative or quasi-judicial capacity for a cumulative period of 5 years;

(d) Is working and holding a post in Grade I in Government Department either in State Government/Union Territories to perform functional duty & discharge job responsibility in the field of Information Technology;

(e) Is an in-service officer not below the rank of Director to the Government of India or an equivalent officer of State Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and-

> (a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of section 193 and 228 of the Indian Penal Code;

> (b) shall be deemed to be a civil court for the purpose of section 345 and 346 of the Code of Criminal Procedure, 1973

> (c) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908.⁹⁰

⁹⁰ Inserted by Information Technology (Amendment) Act, 2008.

COMMENTS:

Section 58(2) of the Information Technology Act states-

The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:-

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it ex parte;

(g) any other matter which may be prescribed.

Section 193 of the *Indian Penal Code* is titled "Punishment for false evidence" and states-

Whoever intentionally gives false evidence in any stage of a judicial proceeding, or fabricates false evidence for the purpose of being used in any stage of a judicial proceeding, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine,

and whoever intentionally gives or fabricates false evidence in any other case, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

Explanation 1.--A trial before a Court-martial is a judicial proceeding.

Explanation 2.--An investigation directed by law preliminary to a proceeding before a Court of Justice, is a stage of a judicial proceeding, though that investigation may not take place before a Court of Justice.

Illustration

A, in an enquiry before a Magistrate for the purpose of ascertaining whether Z ought to be committed for trial, makes on

oath a statement which he knows to be false. As this enquiry is a stage of a judicial proceeding, A has given false evidence.

Explanation 3.--An investigation directed by a Court of Justice according to law, and conducted under the authority of a Court of Justice, is a stage of a judicial proceeding, though that investigation may not take place before a Court of Justice.

Illustration

A, in any enquiry before an officer deputed by a Court of Justice to ascertain on the spot the boundaries of land, makes on oath a statement which he knows to be false. As this enquiry is a stage of a judicial proceeding. A has given false evidence.

Section 228 of the *Indian Penal Code* is titled "Intentional insult or interruption to public servant sitting in judicial proceeding" and states-

Whoever intentionally offers any insult, or causes any interruption to any public servant, while such public servant is sitting in any stage of a judicial proceeding, shall be punished with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

Section 345 of the *Code of Criminal Procedure* is titled "Procedure in certain cases of contempt" and states-

(1) When any such offence as is described in section 175, section 178, section 179, section 180 or section 228 of the Indian Penal Code (45 of 1860) is committed in the view or presence of any civil, Criminal or Revenue Court, the Court may cause the offender to be detained in custody and may at any time before the rising of the Court on the same day, take cognizance of the offence and, after giving the offender a reasonable opportunity of showing cause why he should not be punished under this section, sentence the offender to fine not exceeding two hundred rupees, and, in default of payment of fine, to simple imprisonment for a term which may extend to one month, unless such fine be sooner paid.

(2) In every such case the Court shall record the facts constituting the offence, with the statement (if any) made by the offender as well as the finding and sentence.

(3) If the offence is under section 228 of the Indian Penal Code (45 of 1860), the record shall show the nature and stage of the judicial proceeding in which the Court interrupted or insulted was sitting, and the nature of the interruption or insult.

Section 346 of the *Code of Criminal Procedure* is titled "Procedure where Court considers that case should not be dealt with under section 345" and states-

(1) If the Court in any case considers that a person accused of any of the offences referred to in section 345 and committed in its view or presence should be imprisoned otherwise than in default of payment of fine, or that a fine exceeding two hundred rupees should be imposed upon him, or such Court is for any other reason of opinion that the case should not be disposed of under section 345 such Court, after recording the facts constituting the offence and the statement of the accused as hereinbefore provided, may forward the case to a magistrate having jurisdiction to try the same, and may require security to be given for the appearance of such person before such Magistrate, or if sufficient security is not given shall forward such person in custody to such Magistrate.

(2) The Magistrate to whom any case is forwarded under this section shall proceed to deal with, as far as may be, as if it were instituted on a police report.

47. Factors to be taken into account by the adjudicating officer.

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:-

- (a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
- (b) the amount of loss caused to any person as a result of the default;
- (c) the repetitive nature of the default.

CHAPTER X - THE CYBER APPELLATE TRIBUNAL⁹¹

⁹¹ Also refer to Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 and Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003.

48. Establishment of Cyber Appellate Tribunal.

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal.⁹²

(1) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the official Gazette, appoint:

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act, 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008.

(2) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.

(3) Subject to the provisions of this Act –

(a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof;

(b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two Members of such Tribunal as the Chairperson may deem fit;

(c) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the

⁹² Substituted by Information Technology (Amendment) Act, 2008 for "A cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government."

Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify;

(d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.

(4) Notwithstanding anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench.

(5) If at any stage of the hearing of any case or matter it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.

50. Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal.⁹³

(1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court.

(2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having special knowledge of, and professional experience in, information technology, telecommunication, industry, management or consumer affairs:

Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than one year or Joint

⁹³ Substituted by Information Technology (Amendment) Act, 2008 for "A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he- (a) is, or has been, or is qualified to be, a Judge of a High Court; or (b) is, or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

Secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than seven years.

(3) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that Service for a period of not less than five years.

51. Term of office, conditions of service, etc., of Chairperson and Members. $^{\rm 94}$

(1) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

(2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.

(3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member.

⁹⁴ Substituted by Information Technology (Amendment) Act, 2008 for "The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier."

52. Salary, allowances and other terms and conditions of service of Chairperson and Members $^{\rm 95}$

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of the Cyber Appellate Tribunal shall be such as may be prescribed.

COMMENTS:

The Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009 are the relevant provisions.

52A. Powers of superintendence, direction, etc.⁹⁶

The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

52B. Distribution of business among Benches.⁹⁷

Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.

⁹⁵ Substituted by Information Technology (Amendment) Act, 2008 for "The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed: Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officers shall be varied to his disadvantage after appointment."

⁹⁶ Inserted by Information Technology (Amendment) Act, 2008.

⁹⁷ Inserted by Information Technology (Amendment) Act, 2008.

52C. Power of Chairperson to transfer cases.⁹⁸

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or *suo motu* without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.

52D. Decision by majority⁹⁹

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.

53. Filling up of vacancies.

If, for reason other than temporary absence, any vacancy occurs in the office of the Chairperson or Member, as the case may be,¹⁰⁰ of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54. Resignation and removal.

(1) The Chairperson or the Member¹⁰¹ of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

⁹⁸ Inserted by Information Technology (Amendment) Act, 2008.

⁹⁹ Inserted by Information Technology (Amendment) Act, 2008.

¹⁰⁰ The words "Chairperson or Member, as the case may be," substituted for "Presiding Officer" by Information Technology (Amendment) Act, 2008.

¹⁰¹ The words "Chairperson or Member, as the case may be," substituted for "Presiding Officer" by Information Technology (Amendment) Act, 2008.

Provided that the said Chairperson or the Member¹⁰² shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Chairperson or the Member¹⁰³ of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Chairperson or Member.¹⁰⁴

COMMENTS:

The Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009 are the relevant provisions.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.

No order of the Central Government appointing any person as the Chairperson or the Member 105 of a Cyber Appellate

¹⁰² The words "Chairperson or Member, as the case may be," substituted for "Presiding Officer" by Information Technology (Amendment) Act, 2008.

¹⁰³ The words "Chairperson or Member, as the case may be," substituted for "Presiding Officer" by Information Technology (Amendment) Act, 2008.

¹⁰⁴ The words "Chairperson or Member, as the case may be," substituted for "Presiding Officer" by Information Technology (Amendment) Act, 2008.

¹⁰⁵ The words "Chairperson or Member, as the case may be," substituted for "Presiding Officer" by Information Technology (Amendment) Act, 2008.

Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal.

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Chairperson¹⁰⁶.

(3) The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57. Appeal to Cyber Appellate Tribunal.

(1) Save as provided in sub-section (2), any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it

¹⁰⁶ The words "Chairperson" substituted for "Presiding Officer" by Information Technology (Amendment) Act, 2008.

thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

COMMENTS:

The *Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000* provide detailed provisions relating to this issue, as quoted below:

3. Procedure for filing applications.—

(1) An application to the Tribunal shall be presented in Form-1 annexed to these rules by the applicant in person or by an agent or by a duly authorized legal practitioner, to the Registrar or sent by registered post addressed to the Registrar.

(2) The application under sub-rule (1) shall be presented in six complete sets in a paper-book form along with one empty file size envelope bearing full address of the respondent. Where the number of respondents is more than one, sufficient number of extra paper-books together with required number of empty file size envelopes bearing the full address of each respondent shall be furnished by the applicant.

(3) The applicant may attach to and present with his application a receipt slips as in Form No. 1 which shall be signed by the Registrar or the officer receiving the applications on behalf of the Registrar in acknowledgement of the receipt of the application.

(4) Notwithstanding anything contained in sub rules (1), (2) and (3), the Tribunal may permit:— (a) more than one person to join together and file a single application if it is satisfied, having regard to the cause of action and the nature of relief prayed for, that they have the same interest in the service matter; or (b) an Association representing the persons desirous of joining in a single application provided, however, that the application shall disclose the names of all the persons on whose behalf it has been filed.

4. Presentation and scrutiny of applications.—

(1) The Registrar, or the officer authorised by the Registrar shall endorse on every application the date on which it is presented or deemed to have been presented under that rule and shall sign the endorsement.

(2) If, on scrutiny, the application is found to be in order, it shall be duly registered and given a serial number.

(3) If the application, on scrutiny, is found to be defective, and the defect noticed is formal in nature, the Registrar may allow the party to rectify the same in his presence, and if the said defect is not formal in nature, the Registrar may allow the applicant such time to rectify the defect as he may deem fit.

(4) If the applicant fails to rectify the defect within the time allowed under sub rule (3), the Registrar may, by order and for reasons to be recorded in writing, decline to register the application.

(5) An appeal against the order of the Registrar under sub rule (4) shall be made within 15 days of the making of such order to the Tribunal whose decision thereon shall be final.

5. Place of filing application.—

The applicant shall file application with the Registrar.

6. Application fee.—

Every application filed with the Registrar shall be accompanied by a fee of Rs. 2,000/- (rupees two thousand) only which shall be either in the form of a crossed demand draft or a pay order drawn on a Scheduled Bank in favour of the Registrar and payable at New Delhi.

7. Contents of application.—

(1) Every application filed under rule 3 shall set forth concisely under distinct heads, the grounds for such application and such grounds shall be numbered consecutively and typed in double space on one side of the paper.

(2) It shall not be necessary to present a separate application to seek an interim order or direction if the application contains a prayer seeking an interim order or direction pending final disposal of the application.

(3) An application may, subsequent to the filing of application under section 57 of the Act, apply for an interim order or direction. Such an application shall, as far as possible, be in the same form as is prescribed for on application under section 57 and shall be accompanied by a fee of Rs. 5/- (Rupees five only) which shall be payable in court fee stamps affixed on such application.

8. Paper book, etc. to accompany the application.-

(1) Every application shall be accompanied by a paper book containing:—(i) a certified copy of the order against which the application has been filed; (ii) copies of the documents relied upon by the applicant and referred to in the application; and (iii) an index of documents.

(2) The documents referred to in sub rule (I) may be attested by an advocate or by a Gazetted Officer.

(3) Where an Application is filed by an agent, documents authorising him to act as such agent shall also be appended to the application.

Provided that where an application is filed by an advocate it shall be accompanied by a duly executed 'vakalatname'.

9. Plural remedies.-

An application shall be based upon a single cause of action and may seek one or more reliefs provided they are consequential to one another.

10. Service of notice of application on the respondents.---

(1) A copy of the application in the paper-book shall ordinarily be served on each of the respondents by the Registrar in one of the following modes:— (i) hand delivery (dasti) through the applicant or through a process server; or (ii) through registered post with acknowledgement due.

(2) Notwithstanding anything contained in sub rule (1), the Registrar may, taking into account the number of respondents and their places of residence or work and other circumstances direct that notice of the application shall be served upon the respondents in any other manner including any manner of substituted service, as it appear to the Registrar just and convenient.

(3) Every applicant shall pay a fee for the service or execution of processes, in respect of an application where the number of respondents exceeds five, as under:— (i) a sum of Rs. 50 (Rupees fifty) for each respondent in excess of five respondents; or (ii) where the service is in such manner as the Registrar may direct under sub rule (2), a sum not exceeding the actual charges incurred in effecting the service as may be determined by the Registrar.

(4) The fee for the service or execution of processes under 'sub rule (3) shall be remitted by the applicant either in the form of a crossed Demand Draft drawn on a Scheduled Bank in favour of the Registrar and payable at the station where Registrar's office is situated or remitted through a crossed Indian Postal Order drawn in favour of the Registrar and payable in General Post Office of the station where the Tribunal is located.

(5) Notwithstanding anything contained in sub rules (1), (2), (3) and (4), if the Tribunal is satisfied that it is not reasonably practicable to serve notice of application upon all the respondents, if may for reasons to be recorded in writing, direct that the application shall be heard notwithstanding that some of the respondents have not been served with notice of the application, provided that no application shall be heard unless:—(i) notice of the application has been served on the Government, if Government is respondent; (ii) notice of the application has been filed; and (iii) the Tribunal is satisfied that the interests of the respondents on whom notice of the application has been served are adequately and sufficiently represented by the respondents on whom notice of the application has been served.

11. Filing of reply and other documents by the respondent.--

(1) The respondent shall file six complete sets containing the reply to the application alongwith the documents in a paper-book form with the Registrar within one month of the date of service of the notice of the application on him.

(2) The respondent shall also serve a copy of the reply along with copies of documents as mentioned in sub rule (1) to the applicant or his advocate, if any, and file proof of such service with the Registrar. The Tribunal may, on application by the respondent,

allow filing of the reply after the expiry of the period of one month.

12. Date and place of hearing to be notified.-

The Tribunal shall notify to the parties the date and the place of hearing of the application.

14. Decision on applications.—

(1) Tribunal shall draw up a calendar for the hearing of transferred cases and as far as possible hear and decide the cases according to the calendar.

(2) Every application shall be heard and decided, as far as possible, within six months of the date of its presentation.

(3) For purposes of sub-rule (1) and (2), the Tribunal shall have the power to decline an adjournment and to limit the time for oral arguments.

15. Action on application for applicant's default.--

(1) Where on the date fixed for hearing of the application or on any other date to which such hearing may be adjourned, the applicant does not appear when the application is called on for hearing, the Tribunal may, in its discretion, either dismiss the application for default or hear and decide it on merit.

(2) Where an application has been dismissed for default and the applicant appears afterwards and satisfies the Tribunal that there was sufficient cause for his non-appearance when the application was called on for hearing, the Tribunal shall make an order setting aside the order dismissing the application and restore the same.

16. Hearing on application ex-parte.—

(1) Where on the date fixed for hearing the application or on any other date to which hearing is adjourned, the applicant appears and the respondent does not appear when the application is called on for hearing, the Tribunal may, in its discretion, adjourn or hear and decide the application ex-parte.

(2) Where an application has been heard ex-parte against a respondent or respondents, such respondent or respondents may apply to the Tribunal for an order to set it aside and if such respondent or respondents satisfy the Tribunal that the notice was

not duly served, or that he or they were prevented by any sufficient cause from appearing when the application was called on for hearing, the Tribunal may make an order setting aside the exparte hearing as against him or them upon such terms as it thinks fit, and shall appoint a day for proceeding with the application:

Provided that where the ex-parte hearing of the application is of such nature that it cannot be set aside as against one respondent only, it may be set aside as against all or any of the other respondents also:

Provided further that Tribunal shall not set aside ex-parte hearing of an application merely on the ground that there has been an irregularity in the service of notice, if it is satisfied that the respondent had notice of the date of hearing and had sufficient time to appear and answer the applicant's claim.

17. Adjournment of application.-

The Tribunal may on such terms as it deems fit and at any stage of the proceedings adjourn the hearing of the application.

18. Order to be signed and dated—

Every order of the Tribunal shall be in writing and shall be signed and dated by the Presiding Officer.

19. Publication of orders.—

Such of the orders of the Tribunal as are deemed fit for publication in any report or the press may be released for such publication on such terms and conditions as the Tribunal may lay down.

20. Communication of orders to parties.-

Every order passed on an application shall be communicated to the applicant and to the respondent either in person or by registered post free of cost.

21. No fee for inspection of records.-

No fee shall be charged for inspecting the records of a pending application by a party thereto.

22. Orders and directions in certain cases.-

The Tribunal may make such orders or give such directions as may be necessary or expedient to give effect or in relation to its orders or to prevent abuse of its process or to secure the ends of justice.

23. Registration of legal practitioners clerks:-

(1) A clerk employed by a legal practitioner and permitted as such to have access to the records and to obtain copies of the orders of the Tribunal in which the legal practitioner ordinarily practices shall be known as a "registered clerk"

(2) A legal practitioner desirous of registering his clerk shall make an application to the Registrar in Form 2.

(3) A legal practitioner shall have at a time not more than two registered clerks unless the Registrar by general or special order otherwise permits.

(4) A register of all the registered clerks shall, be maintained in the office of the Registrar and after registration of the clerk, the Registrar shall direct the issue of an identity card to him which shall be non transferable and shall be produced by the holder upon request by an officer or any other employee of the Tribunal.

(5) The identity card mentioned in sub-rule (4) shall be issued under the signatures of the Registrar of the Tribunal.

(6) Whenever a legal practitioner ceases to employ a registered clerk, he shall notify the fact at once to the Registrar by means of a letter enclosing therewith the identity card issued to his clerk and on receipt of such letter the name of the said registered clerk shall be struck off from the register.

24. Working hours of the Tribunal-

Except on Saturday, Sundays and other holidays, the offices of the Tribunal shall, subject to any order made by the Presiding Officer, remain open daily from 10.00 a.m. to 5.00 p.m. but no work, unless it is of an urgent nature, shall be admitted after 4.30 p.m. on any working day.

25. Sitting hours of the Tribunal.—

The sitting hours of the Tribunal shall ordinarily be from 10.30. a.m. to 1-00 p.m. and 2.00 p.m. to 5.00 p.m. subject to any order made by the Chairman.

58. Procedure and powers of the Cyber Appellate Tribunal.

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

COMMENTS:

The principles of natural justice have been discussed in detail by the Supreme Court of India in Uma Nath Pandey and Ors. Vs. State of U.P. and Anr. [Criminal Appeal No. 471 of 2009 (Arising out of SLP (Crl.) No. 6382 of 2007), decided On: 16.03.2009], as quoted below:

6. Natural justice is another name for commonsense justice. Rules of natural justice are not codified canons. But they are principles ingrained into the conscience of man. Natural justice is the administration of justice in a commonsense liberal way. Justice is based substantially on natural ideals and human values. The administration of justice is to be freed from the narrow and restricted considerations which are usually associated with a formulated law involving linguistic technicalities and grammatical niceties. It is the substance of justice which has to determine its form.

7. The expressions "natural justice" and "legal justice" do not present a water-tight classification. It is the substance of justice which is to be secured by both, and whenever legal justice fails to achieve this solemn purpose, natural justice is called in aid of legal justice. Natural justice relieves legal justice from unnecessary technicality, grammatical pedantry or logical prevarication. It supplies the omissions of a formulated law. As Lord Buckmaster said, no form or procedure should ever be permitted to exclude the presentation of a litigants' defence.

8. The adherence to principles of natural justice as recognized by all civilized States is of supreme importance when a quasi-judicial body embarks on determining disputes between the parties, or any administrative action involving civil consequences is in issue. These principles are well settled. The first and foremost principle is what is commonly known as audi alteram partem rule. It says that no one should be condemned unheard. Notice is the first limb of this principle. It must be precise and unambiguous. It should appraise the party determinatively the case he has to meet. Time given for the purpose should be adequate so as to enable him to make his representation. In the absence of a notice of the kind and such reasonable opportunity, the order passed becomes wholly vitiated. Thus, it is but essential that a party should be put on notice of the case before any adverse order is passed against him. This is one of the most important principles of natural justice. It is after all an approved rule of fair play. The concept has gained significance and shades with time. When the historic document was made at Runnymede in 1215, the first statutory recognition of this principle found its way into the "Magna Carta". The classic exposition of Sir Edward Coke of natural justice requires to "vocate, interrogate and adjudicate". In the celebrated case of Cooper v. Wandsworth Board of Works (1863) 143 ER 414, the principle was thus stated:

Even God did not pass a sentence upon Adam, before he was called upon to make his defence. "Adam" says God, "where art thou? hast thou not eaten of the tree whereof I commanded thee that thou shouldest not eat.

9. Since then the principle has been chiselled, honed and refined, enriching its content. Judicial treatment has added light and luminosity to the concept, like polishing of a diamond.

10. Principles of natural justice are those rules which have been laid down by the Courts as being the minimum protection of the rights of the individual against the arbitrary procedure that may be adopted by a judicial, quasi-judicial and administrative authority while making an order affecting those rights. These rules are intended to prevent such authority from doing injustice.

11. What is meant by the term 'principles of natural justice' is not easy to determine. Lord Summer (then Hamilton, L.J.) in Ray v. Local Government Board (1914) 1 KB 160 at p.199 : 83 LJKB 86 described the phrase as sadly lacking in precision. In General Council of Medical Education & Registration of U.K. v. Sanckman (1943 AC 627: (1948) 2 All ER 337, Lord Wright observed that it was not desirable to attempt 'to force it into any procusteam bed' and mentioned that one essential requirement was that the Tribunal should be impartial and have no personal interest in the controversy, and further that it should give `a full and fair opportunity' to every party of being heard.

12. Lord Wright referred to the leading cases on the subject. The most important of them is the Board of Education v. Rice, where Lord Loreburn, L.C. observed as follows:

Comparatively recent statutes have extended, if they have originated, the practice of imposing upon departments or offices of State the duty of deciding or determining questions of various kinds. It will, I suppose usually be of an administrative kind, but sometimes, it will involve matter of law as well as matter of fact, or even depend upon matter of law alone. In such cases, the Board of Education will have to ascertain the law and also to ascertain the facts. I need not and that in doing either they must act in good faith and fairly listen to both sides for that is a duty lying upon everyone who decides anything. But I do not think they are bound to treat such a question as though it were a trial.... The Board is in the nature of the arbitral tribunal, and a Court of law has no jurisdiction to hear appeals from the determination either upon law or upon fact. But if the Court is satisfied either that the Board have not acted judicially in the way I have described, or have not determined the question which they are required by the Act to determine, then there is a remedy by mandamus and certiorari.

13. Lord Wright also emphasized from the same decision the observation of the Lord Chancellor that the Board can obtain information in any way they think best, always giving a fair opportunity to those who are parties to the controversy for correcting or contradicting any relevant statement prejudicial to their view". To the same effect are the observations of Earl of Selbourne, LO in Spackman v. Plumstead District Board of Works, where the learned and noble Lord Chancellor observed as follows:

No doubt, in the absence of special provisions as to how the person who is to decide is to proceed, law will imply no more than that the substantial requirements of justice shall not be violated. He is not a judge in the proper sense of the word; but he must give the parties an opportunity of being heard before him and stating their case and their view. He must give notice when he will proceed with the matter and he must act honestly and impartially and not under the dictation of some other person or persons to whom the authority is not given by law. There must be no malversation of any kind. There would be no decision within the meaning of the statute if there were anything of that sort done contrary to the essence of justice.

14. Lord Selbourne also added that the essence of justice consisted in requiring that all parties should have an opportunity of submitting to the person by whose decision they are to be bound, such considerations as in their judgment ought to be brought before him. All these cases lay down the very important rule of natural justice contained in the oft-quoted phrase `justice should not only be done, but should be seen to be done'.

15. Concept of natural justice has undergone a great deal of change in recent years. Rules of natural justice are not rules embodied always expressly in a statute or in rules framed thereunder. They may be implied from the nature of the duty to be performed under a statute. What particular rule of natural justice should be implied and what its context should be in a given case must depend to a great extent on the fact and circumstances of that case, the frame-work of the statute under which the enquiry is held. The old distinction between a judicial act and an administrative act has withered away. Even an administrative order which involves civil consequences must be consistent with the rules of natural justice. Expression 'civil consequences' encompasses infraction of not merely property or personal rights but of civil liberties, material deprivations, and non-pecuniary damages. In its wide umbrella comes everything that affects a citizen in his civil life.

16. Natural justice has been variously defined by different Judges. A few instances will suffice. In Drew v. Drew and Lebura (1855(2) Macg. 18, Lord Cranworth defined it as `universal justice'. In James Dunber Smith v. Her Majesty the Queen 1877-78(3) App.Case 614, 623 JC Sir Robort P. Collier, speaking for the judicial committee of Privy council, used the phrase `the requirements of substantial justice', while in Arthur John Specman v. Plumstead District Board of Works 1884-85(10) App.Case 229, 240, Earl of Selbourne, S.C. preferred the phrase `the substantial requirement of justice'. In Vionet v. Barrett 1885(55) LJRD 39, 41, Lord Esher, MR defined natural justice as `the natural sense of what is right and wrong'. While, however, deciding Hookings v. Smethwick Local Board of Health 1890(24) QBD 712, Lord Fasher, M.R. instead of using the definition given earlier by him in Vionet's case (supra) chose to define natural justice as 'fundamental justice'. In Ridge v. Baldwin 1963(1) WB 569, 578, Harman LJ, in the Court of Appeal countered natural justice with 'fair-play in action' a phrase favoured by Bhagawati, J. in Maneka India Gandhi v. Union of MANU/SC/0133/1978 [1978]2SCR621 . In re R.N. (An Infant) 1967(2) B617, 530, Lord Parker, CJ, preferred to describe natural justice as `a duty to act fairly'. In Fairmount Investments Ltd. v. Secretary to State for Environment 1976 WLR 1255 Lord Russell of Willowan somewhat picturesquely described natural justice as `a fair crack of the whip' while Geoffrey Lane, LJ. In Regina v. Secretary of State for Home Affairs Ex Parte Hosenball MANU/AG/0472/1977 preferred the homely phrase `common fairness'.

17. How then have the principles of natural justice been interpreted in the Courts and within what limits are they to be confined? Over the years by a process of judicial interpretation two rules have been evolved as representing the principles of natural justice in judicial process, including therein quasi-judicial and administrative process. They constitute the basic elements of a fair hearing, having their roots in the innate sense of man for fairplay and justice which is not the preserve of any particular race or country but is shared in common by all men. The first rule is 'nemo judex in causa sua' or 'nemo debet esse judex in propria causa sua' as stated in (1605) 12 Co.Rep.114 that is, `no man shall be a judge in his own cause'. Coke used the form `aliquis non debet esse judex in propria causa quia non potest esse judex at pars' (Co.Litt. 1418), that is, 'no man ought to be a judge in his own case, because he cannot act as Judge and at the same time be a party'. The form `nemo potest esse simul actor et judex', that is, 'no one can be at once suitor and judge' is also at times used. The second rule is `audi alteram partem', that is, `hear the other side'. At times and particularly in continental countries, the form 'audietur at altera pars' is used, meaning very much the same thing. A corollary has been deduced from the above two rules and particularly the audi alteram partem rule, namely 'qui aliquid statuerit parte inaudita alteram actguam licet dixerit, haud acquum facerit' that is, 'he who shall decide anything without the other side having been heard, although he may have said what is right, will not have been what is right' (See Bosewell's case (1605) 6 Co.Rep. 48-b, 52-a) or in other words, as it is now expressed,

'justice should not only be done but should manifestly be seen to be done'. Whenever an order is struck down as invalid being in violation of principles of natural justice, there is no final decision of the case and fresh proceedings are left upon. All that is done is to vacate the order assailed by virtue of its inherent defect, but the proceedings are not terminated.

18. What is known as `useless formality theory' has received consideration of this Court in M.C. Mehta v. Union of India [1999]3SCR1173. It was observed as under:

Before we go into the final aspect of this contention, we would like to state that case relating to breach of natural justice do also occur where all facts are not admitted or are not all beyond dispute. In the context of those cases there is a considerable case-law and literature as to whether relief can be refused even if the court thinks that the case of the applicant is not one of 'real substance' or that there is no substantial possibility of his success or that the result will not be different, even if natural justice is followed (See Malloch v. Aberdeen Corporation (1971)2 All ER 1278, HL) (per Lord Reid and Lord Wilberforce), Glynn v. Keele University (1971) 2 All ER 89; Cinnamond v. British Airports Authority MANU/AG/0471/1980, CA) and other cases where such a view has been held. The latest addition to this view is R v. Ealing Magistrates' Court, ex p. Fannaran 1996 (8) ALR 351, 358 (See de Smith, Suppl. P.89 (1998) where Straughton, L.J. held that there must be 'demonstrable beyond doubt' that the result would have been different. Lord Woolf in Lloyd v. McMohan 1987 (1) All ER 1118, CA has also not disfavoured refusal of discretion in certain cases of breach of natural justice. The New Zealand Court in McCarthy v. Grant 1959 NZLR 1014 however goes halfway when it says that (as in the case of bias), it is sufficient for the applicant to show that there is 'real likelihood-not certainty- of prejudice'. On the other hand, Garner Administrative Law (8th Edn. 1996. pp.271-72) says that slight proof that the result would have been different is sufficient. On the other side of the argument, we have apart from Ridge v. Baldwin 1964 AC 40 : (1963) 2 All ER 66, HL, Megarry, J. in John v. Rees 1969 (2) All ER 274 stating that there are always `open and shut cases' and no absolute rule of proof of prejudice can be laid down. Merits are not for the court but for the authority to consider.

Ackner, J has said that the 'useless formality theory' is a dangerous one and, however inconvenient, natural justice must be followed. His Lordship observed that 'convenience and justice are often not on speaking terms'. More recently, Lord Bingham has deprecated the 'useless formality theory' in R. v. Chief Constable of the Thames Valley Police Forces, ex p. Cotton 1990 IRLR 344 by giving six reasons (see also his article 'Should Public Law Remedies be Discretionary?" 1991 PL. p.64). A detailed and emphatic criticism of the 'useless formality theory' has been made much earlier in 'Natural Justice, Substance or Shadow' by Prof. D.H. Clark of Canada (see 1975 PL.pp.27-63) contending that Malloch (supra) and Glynn (supra) were wrongly decided. Foulkes (Administrative Law, 8th Edn. 1996, p.323), Craig (Administrative Law, 3rd Edn. P.596) and others say that the court cannot prejudge what is to be decided by the decision-making authority. De Smith (5th Edn. 1994, paras 10.031 to 10.036) says courts have not yet committed themselves to any one view though discretion is always with the court. Wade (Administrative Law, 5th Edn. 1994, pp.526-530) says that while futile writs may not be issued, a distinction has to be made according to the nature of the decision. Thus, in relation to cases other than those relating to admitted or indisputable facts, there is a considerable divergence of opinion whether the applicant can be compelled to prove that the outcome will be in his favour or he has to prove a case of substance or if he can prove a 'real likelihood' of success or if he is entitled to relief even if there is some remote chance of success. We may, however, point out that even in cases where the facts are not all admitted or beyond dispute, there is a considerable unanimity that the courts can, in exercise of their 'discretion', refuse certiorari, prohibition, mandamus or injunction even though natural justice is not followed. We may also state that there is yet another line of cases as in State Bank of Patiala v. S.K. Sharma MANU/SC/0438/1996 : (1996)IILLJ296SC , Rajendra State of M.P. MANU/SC/0690/1996 Singh v. AIR1996SC2736 that even in relation to statutory provisions requiring notice, a distinction is to be made between cases where the provision is intended for individual benefit and where a provision is intended to

protect public interest. In the former case, it can be waived while in the case of the latter, it cannot be waived.

We do not propose to express any opinion on the correctness or otherwise of the 'useless formality theory' and leave the matter for decision in an appropriate case, inasmuch as the case before us, 'admitted and indisputable' facts show that grant of a writ will be in vain as pointed by Chinnappa Reddy, J.

19. Natural justice is the essence of fair adjudication, deeply rooted in tradition and conscience, to be ranked as fundamental. The purpose of following the principles of natural justice is the prevention of miscarriage of justice.

The sole purpose of rules of procedure which are referred to as rules of natural justice is to ensure fairplay. [AIR 1967 SC 408]

"No one, I think, disputes that three features of natural justice stand out. (i) The right to be heard by an unbiased Tribunal (ii) The right to have notice of charges of misconduct (iii) The right to be heard in answer to that charge." [Lord Hudson in Ridge vs. Baldwin (1963) 2AER66 (HL)]

Rule 13 of the *Cyber Regulations Appellate Tribunal (Procedure) Rules,* 2000 is relevant in relation to the sittings of the Tribunal. It states:

The Tribunal shall ordinarily hold its sittings at New Delhi:

Provided that, if at any time, the Presiding Officer of the Tribunal is satisfied that circumstances exist which render it necessary to have sittings of the Tribunal at any place other than New Delhi the Presiding Officer may direct to hold the sittings at any such appropriate place.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:-

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it *ex parte*;

(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

COMMENTS:

Section 193 of the *Indian Penal Code* is titled "Punishment for false evidence" and states-

Whoever intentionally gives false evidence in any stage of a judicial proceeding, or fabricates false evidence for the purpose of being used in any stage of a judicial proceeding, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine,

and whoever intentionally gives or fabricates false evidence in any other case, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

Explanation 1.--A trial before a Court-martial is a judicial proceeding.

Explanation 2.--An investigation directed by law preliminary to a proceeding before a Court of Justice, is a stage of a judicial proceeding, though that investigation may not take place before a Court of Justice.

Illustration

A, in an enquiry before a Magistrate for the purpose of ascertaining whether Z ought to be committed for trial, makes on oath a statement which he knows to be false. As this enquiry is a stage of a judicial proceeding, A has given false evidence.

Explanation 3.--An investigation directed by a Court of Justice according to law, and conducted under the authority of a Court of Justice, is a stage of a judicial proceeding, though that investigation may not take place before a Court of Justice.

Illustration

A, in any enquiry before an officer deputed by a Court of Justice to ascertain on the spot the boundaries of land, makes on oath a statement which he knows to be false. As this enquiry is a stage of a judicial proceeding, A has given false evidence.

Section 196 of the *Indian Penal Code* is titled "Using evidence known to be false" and states-

Whoever corruptly uses or attempts to use as true or genuine evidence any evidence which he knows to be false or fabricated, shall be punished in the same manner as if he gave or fabricated false evidence.

Section 195 of the *Code of Criminal Procedure* is titled "Prosecution for contempt of lawful authority of public servants, for offences against public justice and for offences relating to documents given in evidence" and states-

Section 195 - Prosecution for contempt of lawful authority of public servants, for offences against public justice and for offences relating to documents given in evidence

(1) No Court shall take cognizance-

(a) (i) of any offence punishable under sections 172 to 188 (both inclusive) of the Indian Penal Code (45 of 1860), or (ii) of any abetment of, or attempt to commit, such offence, or (iii) of any criminal conspiracy to commit, such offence,

except on the complaint in writing of the public servant concerned or of some other public servant to whom he is administratively subordinate;

(b) (i) of any offence punishable under any of the following sections of the Indian Penal Code (45 of 1860), namely, sections 193 to 196 (both inclusive), 199, 200, 205 to 211 (both inclusive) and 228, when such offence is alleged to have been committed in, or in relation to, any proceeding in any Court, or (ii) of any offence described in section 463, or punishable under section 471, section 475 or section 476, of the said Code, when such offence is alleged to have been committed in respect of a document produced or given in evidence in a proceeding in any Court, or (iii) of any criminal conspiracy to commit, or attempt to commit, or the

abetment of, any offence specified in sub-clause (i) or sub-clause (ii),1[except on the complaint in writing of that Court or by such officer of the Court as that Court may authorise in writing in this behalf, or of some other Court to which that Court is subordinate].

(2) Where a complaint has been made by a public servant under clause (a) of sub-section (1) any authority to which he is administratively subordinate may order the withdrawal of the complaint and send a copy of such order to the Court; and upon its receipt by the Court, no further proceedings shall be taken on the complaint:

Provided that no such withdrawal shall be ordered if the trial in the Court of first instance has been concluded.

(3) In clause (b) of sub-section (1), the term "Court" means a Civil, Revenue or Criminal Court, and includes a tribunal constituted by or under a Central, provincial or State Act if declared by that Act to be a Court for the purposes of this section.

(4) For the purposes of clause (b) of sub-section (1), a Court shall be deemed to be subordinate to the Court to which appeals ordinarily lie from appealable decrees or sentences of such former Court, or in the case of a civil Court from whose decrees no appeal ordinarily lies, to the principal Court having ordinary original civil jurisdiction within whose local jurisdiction such Civil Court is situate:

Provided that-

(a) where appeals lie to more than one Court, the Appellate Court of inferior jurisdiction shall be the Court to which such Court shall be deemed to be subordinate;

(b) where appeals lie to a civil and also to a Revenue Court, such Court shall be deemed to be subordinate to the civil or Revenue Court according to the nature of the case or proceeding in connection with which the offence is alleged to have been committed.

59. Right to legal representation.

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

60. Limitation.

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

61. Civil court not to have jurisdiction.

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.

62. Appeal to High Court.

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to filed within a further period not exceeding sixty days.

63. Compounding of contraventions.

(1) Any contravention under this Act¹⁰⁷ may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

¹⁰⁷ The word "Chapter" has been substituted by the word "Act" by Information Technology (Removal of Difficulties) Order, 2002.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years form the date on which the first contravention, committed by him, was compounded.

Explanation.- For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (I), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

COMMENTS:

Simply put, compounding an offence means condoning the offence in return for money. The accused pays a sum of money and in return he is not prosecuted for the offence.

The amended *Information Technology Act* contains another provision for compounding under section 77A.

Under section 63 of the *Information Technology Act*, the following can compound a contravention under sec: (1) the Controller or (2) officer specially authorised by the Controller in this behalf or (3) the adjudicating officer.

The compounding can be done either (1) before the institution of adjudication proceedings or (2) after the institution of adjudication proceedings.

Illustration 1: Sameer obtains / copies some information from Pooja's computer without her permission. Pooja files a complaint with the Adjudicating Officer (AO) u/s 43(b) of the IT Act. The AO can compound the case and stop all further proceeding.

Illustration 2:

Presume that in illustration 1 above, the offence was compounded in January 2008. Sameer again contravenes section 43(b) of the IT Act in March 2009. This time the offence cannot be compounded.

Illustration 3: Presume that in illustration 1 above the offence was compounded in January 2008. Sameer again contravenes section 43(b) of the IT Act in March 2011. This time the offence can be compounded.

64. Recovery of penalty or compensation.

A penalty imposed or compensation awarded¹⁰⁸ under this Act, if it is not paid shall be recovered as an arrear of land revenue and the licence or the Electronic Signature¹⁰⁹ Certificate, as the case may be, shall be suspended till the penalty is paid.

COMMENTS:

Land revenue and the process of recovery of land revenue is covered by the law of the specific state or Union Territory.

In Maharashtra, the relevant law is the *Maharashtra Land Revenue Code*, 1966. Section 2(19) of this Code states:

(19) "land revenue" means all sums and payments, in money received or legally claimable by or on behalf of the State Government from any person on account of any land or interest in or right exercisable over land held by or vested in him, under whatever designation such sum may be payable and any cess or rate authorised by the State Government under the provisions of any law for the time being in force; and includes premium, rent, lease money, quit, rent, judi payable by a inamdar or any other payment provided under any Act, rule, contract or deed on account of any land;

Section 173 of the *Maharashtra Land Revenue Code, 1966* is titled "'Arrear", "defaulter" and states:

Any land revenue due and not paid on or before the prescribed dates becomes there from an arrear, and the persons responsible for it under the provision of Section 168 or otherwise become defaulters.

¹⁰⁸ The words "or compensation awarded" inserted by Information Technology (Amendment) Act, 2008.

¹⁰⁹ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

Section 176 of the *Maharashtra Land Revenue Code, 1966* is titled "Process of recovery of arrears" and states:

An arrear of land revenue may be recovered by any or more of the following processes, that is to say,-

(a) by serving a written notice of demand on the defaulter under Section 178;

(b) by forfeiture of the occupancy or alienated holding in respect of which the arrear is due under Section 179;

(c) by distraint and sale of the defaulter's movable property under Section 180;

(d) by attachment and sale of the defaulter's immovable property under Section 181;

(e) by attachment of the defaulter's immovable property under Section 182;

(f) by arrest and imprisonment of the defaulter under Sections 183 and 184.

(g) in the case of alienated holding consisting of entire villages, or shares of village, by attachment of the said villages or shares of villages under Sections 185 to 190 (both inclusive):

Provided that, the processes specified in clauses (c), (d) and (e) shall not permit the attachment and sale of the following, namely:-

(i) the necessary wearing apparel, cooking vessels, beds and bedding of the defaulter, his wife and children, and such personal ornaments as, in accordance with the religious usage, cannot be parted with by any woman;

(ii) tools of artisans and, if the defaulter is an agriculturist, his implements of husbandry, except an implement driven by mechanical power and such cattle and seed as may, in the opinion of the Collector, be necessary to enable him to earn his livelihood as such and also such portion of the agricultural produce as in the opinion of the Collector is necessary for the purpose of providing, until the next harvest, for the due cultivation of the land and for support of the holder and his family;

(iii) articles set aside exclusively for the use of religious endowments;

(iv) houses and other buildings (with the materials and sites thereof and the land immediately appurtenant thereto and necessary for their enjoyment) belonging to an agriculturist and occupied by him.

CHAPTER XI - OFFENCES

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 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 listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

COMMENTS:

Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. Computer source code need not only be in the electronic form. It can be printed on paper (e.g. printouts of flowcharts for designing a software application). Let us understand this using some illustrations.

> **Illustration:** Pooja has created a simple computer program. When a user double-clicks on the hello.exe file created by Pooja, the following small screen opens up:

Hello World

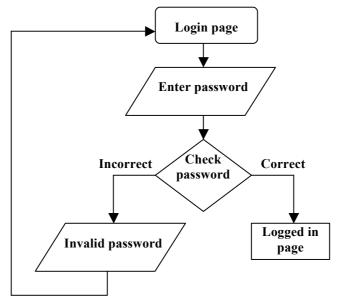
The hello.exe file created by Pooja is the executable file that she can give to others. The small screen that opens up is the output of the software program written by Pooja. Pooja has created the executable file using the programming language called "C". Using this programming language, she created the following lines of code:

main() {	printf("Hello, "); printf("World");
}	

These lines of code are referred to as the source code.

Illustration: Noodle Ltd has created software for viewing and creating image files. The programmers who developed this program used the computer-programming language called Visual C++. Using the syntax of these languages, they wrote thousands of lines of code. This code is then compiled into an executable file and given to end-users. All that the end user has to do is double-click on a file (called setup.exe) and the program gets installed on his computer. The lines of code are known as computer source code.

Illustration: Pooja is creating a simple website. A registered user of the website would have to enter the correct password to access the content of the website. She creates the following flowchart outlining the functioning of the authentication process of the website.



She takes a printout of the flowchart to discuss it with her client. The printout is source code.

This section relates to computer source code that is either: (1) required to be kept (e.g. in a cell phone, hard disk, server etc), or (2) required to be maintained by law.

The following acts are prohibited in respect of the source code (1) knowingly concealing or destroying or altering (2) intentionally concealing or destroying or altering (3) knowingly causing another to conceal or destroy or alter (4) intentionally causing another to conceal or destroy or alter. Let us discuss the relevant terms and issues in detail.

Conceal simply means "to hide".

Illustration: Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer changes the properties of the folder and makes it a "hidden" folder. Although the source code folder still exists on Pooja's computer, she can no longer see it. Sameer has concealed the source code.

Destroy means "to make useless", "cause to cease to exist", "nullify", "to demolish", or "reduce to nothing".

Destroying source code also includes acts that render the source code useless for the purpose for which it had been created.

Illustration: Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer deletes the folder. He has destroyed the source code.

Illustration: Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer deletes one of the source code files. Now the source code cannot be compiled into the final product. He has destroyed the source code.

Illustration: Pooja is designing a software program. She draws out the flowchart depicting the outline of the functioning of the program. Sameer tears up the paper on which she had drawn the flowchart. Sameer has destroyed the source code.

Alters, in relation to source code, means "modifies", "changes", "makes different" etc. This modification or change could be in respect to size, properties, format, value, utility etc.

Illustration: Pooja has created a webpage for her client. The source code of the webpage is in HTML (Hyper Text Markup Language) format. Sameer changes the file from HTML to text format. He has altered the source code.

CASE LAW: Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh & Anr. [2005CriLJ4314]

Summary of the case:

Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm. The court held that such manipulation amounted to tampering with computer source code as envisaged by section 65 of the Information Technology Act, 2000.

Background of the case:

Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500 as well as service bundle for 3 years with an initial payment of Rs. 3350 and monthly outflow of Rs. 600. The subscriber was also provided a 1 year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically "unlocked" so that the exclusive Reliance handsets could be used for the Tata Indicom service.

Reliance officials came to know about this "unlocking" by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Teleservices Limited officials for reprogramming the Reliance handsets.

These arrested persons approached the High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

Issues raised by the Defence:

(1) Subscribers always had an option to change from one service provider to another.

(2) The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.

(3) The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.

(4) A telephone handset is neither a computer nor a computer system containing a computer programme.

(5) There is no law in force which requires the maintenance of "computer source code". Hence section 65 of the Information Technology Act does not apply.

Findings of the court

(1) As per section 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

(2) The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. This is known as source code in computer parlance.

(3) A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.

(4) When the person moves from one cell to another cell in the same city, the system i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.

(5) All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.

(6) System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.

(7) Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.

(8) Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.

(9) When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.

(10) If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.

(11) When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring.

(12) So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

(13) This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

(14) When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If someone manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

Conclusions of the court

(1) A cell phone is a computer as envisaged under the Information Technology Act.

(2) ESN and SID come within the definition of "computer source code" under section 65 of the Information Technology Act.

(3) When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.

(4) Whether a cell phone operator is maintaining computer source code, is a matter of evidence.

(5) In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases -(a) "when the computer source code is required to be kept" (b) "maintained by law for the time being in force".

SUMMARY:

Acts penalized	(1) knowingly or intentionally concealing,
	destroying or altering computer source code
	(2) knowingly or intentionally causing another to
	conceal, destroy or alter computer source code
Punishment	Imprisonment upto 3 years and / or fine upto Rs 2 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 2 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 2 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) Accused has concealed or destroyed or altered computer source code or caused another to do so
	(2) Accused did such act(s) with knowledge and / or intention
	(3) Accused does not have the legal rights with respect to the source code to do such act(s)
Points for defence	(1) Acts committed by the accused did not result in the source code being concealed, destroyed or altered
	(2) The acts of the accused were not done with knowledge or intention
	(3) Accused had the legal rights with respect to the source code to do such act(s)

66. Computer related offences.¹¹⁰

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 purposes 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.

COMMENTS:

The acts referred to in section 43 of the Information Technology Act are:

(a) accessing or securing access to a computer, computer system, computer network or computer resource without the permission of the owner or person in-charge;

(b) downloading, copying or extracting any data, computer data base or information from a computer, computer system or computer network or removable storage medium without the permission of the owner or person in-charge;

(c) introducing or caused to be introduced any computer contaminant or computer virus into any computer, computer system or computer network without the permission of the owner or person in-charge;

(d) damaging or causing 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 without the permission of the owner or person in-charge;

(e) disrupting or causing disruption of any computer, computer system or computer network;

¹¹⁰ Substituted by Information Technology (Amendment) Act, 2008 for "(1) Whoever with the intent of cause or knowing that is likely to cause wrongful loss or damage 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 up to three years, or with fine which may extend up to two lakh rupees, or with both."

(f) denying or causing the denial of access to any person authorised to access any computer, computer system or computer network by any means without the permission of the owner or person in-charge;

(g) providing any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder without the permission of the owner or person in-charge;

(h) charging the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network without the permission of the owner or person in-charge;

(i) destroying, deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means without the permission of the owner or person in-charge;

(j) stealing, concealing, destroying or altering or causing any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage without the permission of the owner or person in-charge;

Section 24 of Indian Penal Code states-

Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

Section 25 of Indian Penal Code states-

A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

Another relevant provision is Section 23 of *Indian Penal Code* which defines some of the words discussed above, as under:

"Wrongful gain" is gain by unlawful means of property to which the person gaining is not legally entitled.

"Wrongful loss".--"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.

Gaining wrongfully, losing wrongfully.--A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property, as well as when such person is wrongfully deprived of property.

SUMMARY:

Acts penalized	 dishonestly or fraudulently accessing or securing access to a computer, computer system, computer network or computer resource without the permission of the owner or person in-charge; dishonestly or fraudulently downloading,
	copying or extracting any data, computer data base or information from a computer, computer system or computer network or removable storage medium without the permission of the owner or person in-charge;
	(3) dishonestly or fraudulently introducing or caused to be introduced any computer contaminant or computer virus into any computer, computer system or computer network without the permission of the owner or person in-charge;
	(4) dishonestly or fraudulently damaging or causing 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 without the permission of the owner or person in- charge;
	(5) dishonestly or fraudulently disrupting or causing disruption of any computer, computer system or computer network;
	(6) dishonestly or fraudulently denying or causing the denial of access to any person authorised to access any computer, computer system or computer network by any means without the permission of the owner or person in-charge;
	(7) dishonestly or fraudulently providing any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder without the permission of the owner or person in-charge;
	(8) dishonestly or fraudulently charging the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network without the permission of the owner or person in-charge;

	 (9) dishonestly or fraudulently destroying, deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means without the permission of the owner or person incharge; (10) dishonestly or fraudulently stealing, concealing, destroying or altering or causing any person to steal, conceal, destroy or alter any
	computer source code used for a computer resource with an intention to cause damage without the permission of the owner or person in- charge;
Punishment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 5 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	 Police officer not below the rank of Inspector Controller Officer authorised by Controller under section of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	 (1) The accused committed one or more act prohibited by this section (2) The accused committed these acts dishonestly and / or fraudulently or has the relevant (3) The accused committed these acts without the permission of the owner or person in-charge
Points for defence	(1) The accused acted with the permission of the owner or person in-charge(2) The accused was the owner or person in-charge

(3) The accused did not have the relevant intention or knowledge
(4) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise

AUSTRALIA:

Section 477.1 of *The Criminal Code* which is titled "Unauthorised access, modification or impairment with intent to commit a serious offence" and is quoted below:

Intention to commit a serious Commonwealth, State or Territory offence

(1) A person is guilty of an offence if:

(a) the person causes: (i) any unauthorised access to data held in a computer; or (ii) any unauthorised modification of data held in a computer; or (iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the unauthorised access, modification or impairment is caused by means of a carriage service; and

(c) the person knows the access, modification or impairment is unauthorised; and

(d) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment.

(2) Absolute liability applies to paragraph (1)(b).

(3) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the offence was:(a) an offence against a law of the Commonwealth, a State or a Territory; or (b) a serious offence.

Intention to commit a serious Commonwealth offence

(4) A person is guilty of an offence if:

(a) the person causes: (i) any unauthorised access to data held in a computer; or (ii) any unauthorised modification of data held in a computer; or (iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the person knows the access, modification or impairment is unauthorised; and

(c) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth (whether by that person or another person) by the access, modification or impairment.

(5) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the offence was:

- (a) an offence against a law of the Commonwealth; or
- (b) a serious offence.

Penalty

(6) A person who is guilty of an offence against this section is punishable, on conviction, by a penalty not exceeding the penalty applicable to the serious offence.

Impossibility

(7) A person may be found guilty of an offence against this section even if committing the serious offence is impossible.

No offence of attempt

(8) It is not an offence to attempt to commit an offence against this section.

Meaning of serious offence

(9) In this section:

serious offence means an offence that is punishable by imprisonment for life or a period of 5 or more years.

Section 477.2 of *The Criminal Code* which is titled "Unauthorised modification of data to cause impairment" and is quoted below:

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised modification of data held in a computer; and

(b) the person knows the modification is unauthorised; and

(c) the person is reckless as to whether the modification impairs or will impair: (i) access to that or any other data held in any computer; or (ii) the reliability, security or operation, of any such data; and

(d) one or more of the following applies: (i) the data that is modified is held in a Commonwealth computer; (ii) the data that is modified is held on behalf of the Commonwealth in a computer; (iii) the modification of the data is caused by means of a carriage service; (iv) the modification of the data is caused by means of a Commonwealth computer; (v) the modification of the data impairs access to, or the reliability, security or operation of, other data held in a Commonwealth computer; (vi) the modification of the data impairs access to, or the reliability, security or operation of, other data held on behalf of the Commonwealth in a computer; (vii) the modification of the data impairs access to, or the reliability, security or operation of, other data by means of a carriage service.

Penalty: 10 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) A person may be guilty of an offence against this section even if there is or will be no actual impairment to:

(a) access to data held in a computer; or

(b) the reliability, security or operation, of any such data.

(4) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.3

Section 478.1 of *The Criminal Code* which is titled "Unauthorised access to, or modification of, restricted data" and is quoted below:

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised access to, or modification of, restricted data; and

(b) the person intends to cause the access or modification; and

(c) the person knows that the access or modification is unauthorised; and

(d) one or more of the following applies:

(i) the restricted data is held in a Commonwealth computer;

(ii) the restricted data is held on behalf of the Commonwealth;

(iii) the access to, or modification of, the restricted data is caused by means of a carriage service.

Penalty: 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

(3) In this section:

restricted data means data:

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer.

Section 478.2 of *The Criminal Code* which is titled "Unauthorised impairment of data held on a computer disk etc." and is quoted below:

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised impairment of the reliability, security or operation of data held on:

- (i) a computer disk; or
- (ii) a credit card; or
- (iii) another device used to store data by electronic means; and

(b) the person intends to cause the impairment; and

(c) the person knows that the impairment is unauthorised; and

(d) the computer disk, credit card or other device is owned or leased by a Commonwealth entity.

Penalty: 2 years imprisonment.

(2) Absolute liability applies to paragraph (1)(d).

Section 478.3 of *The Criminal Code* which is titled "Possession or control of data with intent to commit a computer offence" and is quoted below:

(1) A person is guilty of an offence if:

(a) the person has possession or control of data; and

(b) the person has that possession or control with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or

(ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

(3) It is not an offence to attempt to commit an offence against this section.

Meaning of possession or control of data

(4) In this section, a reference to a person having possession or control of data includes a reference to the person:

(a) having possession of a computer or data storage device that holds or contains the data; or

(b) having possession of a document in which the data is recorded; or

(c) having control of data held in a computer that is in the possession of another person (whether inside or outside Australia).

Section 478.4 of *The Criminal Code* which is titled "Producing, supplying or obtaining data with intent to commit a computer offence and is quoted below:

(1) A person is guilty of an offence if:

(a) the person produces, supplies or obtains data; and

(b) the person does so with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or

(ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

(3) It is not an offence to attempt to commit an offence against this section.

Meaning of producing, supplying or obtaining data

(4) In this section, a reference to a person producing, supplying or obtaining data includes a reference to the person:

(a) producing, supplying or obtaining data held or contained in a computer or data storage device; or

(b) producing, supplying or obtaining a document in which the data is recorded.

MALAYSIA:

A relevant provision is section (4) of the *Computer Crimes Act*, titled "Unauthorized access with intent to commit or facilitate commission of further offence", which states-

(1) A person shall be guilty of an offence under this section if he commits an offence referred to in section 3 with intent—

(a) to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code [Act 574]; or

(b) to facilitate the commission of such an offence whether by himself or by any other person.

(2) For the purposes of this section, it is immaterial whether the offence to which this section applies is to be committed at the same time when the unauthorized access is secured or on any future occasion.

(3) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

Another relevant provision is section (5) of the *Computer Crimes Act*, titled "Unauthorized modification of the contents of any computer", which states-

(1) A person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer.

(2) For the purposes of this section, it is immaterial that the act in question is not directed at—

- (a) any particular program or data;
- (b) a program or data of any kind; or
- (c) a program or data held in any particular computer.

(3) For the purposes of this section, it is immaterial whether an unauthorized modification is, or is intended to be, permanent or merely temporary.

(4) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both; or be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both, if the act is done with the intention of causing injury as defined in the Penal Code.

SINGAPORE:

A relevant provision is section 4 of the *Computer Misuse Act*, titled "Access with intent to commit or facilitate commission of offence", which states-

(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

(2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 10 years or to both.

(4) For the purposes of this section, it is immaterial whether —

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

Another relevant provision is section 5 of the *Computer Misuse Act*, titled "Unauthorised modification of computer material", which states-

(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

Another relevant provision is section 6 of the *Computer Misuse Act*, titled "Unauthorised use or interception of computer service", which states-

(1) Subject to subsection (2), any person who knowingly ----

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

Another relevant provision is section 7 of the *Computer Misuse Act*, titled "Unauthorised obstruction of use of computer", which states-

(1) Any person who, knowingly and without authority or lawful excuse —

(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not

exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

UNITED KINGDOM:

A relevant provision is section 2 of the *Computer Misuse Act*, titled "Unauthorised access with intent to commit or facilitate commission of further offences" which states-

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

- (a) to commit an offence to which this section applies; or
- (b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Another relevant provision is section 3 of the *Computer Misuse Act*, titled "Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc" which states-

(1) A person is guilty of an offence if—

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer;

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

CONVENTION ON CYBERCRIME:

Article 8 of the *Convention on Cybercrime* of the Council of Europe is titled "Computer-related fraud" and states-

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

(a) any input, alteration, deletion or suppression of computer data;

(b) any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

66A. Punishment for sending offensive messages through communication service, etc.¹¹¹

Any person who sends, by means of a computer resource or a communication device, -

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

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with

¹¹¹ Inserted by Information Technology (Amendment) Act, 2008

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.

COMMENTS:

Section 66A penalises the following being sent through email, sms etc:

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

(2) false information sent for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will.

Illustration: Pooja is Sameer's ex-girlfriend. After their breakup, Pooja married Tapan, who is unaware of Pooja's past relationship with Sameer. Angry over this issue, Sameer sends an email to Pooja, in which he threatens that unless Pooja gives him Rs 1 lakh, he will spread the news that Pooja had been pregnant before marriage.

Pooja does not give him the money. Sameer sends emails to all of Pooja's friends and relatives telling them that Pooja had been pregnant before marriage.

If the information about Pooja's pregnancy is true then Sameer will not be liable under this section. If this information is false, then Sameer will be liable under this section.

This section also penalises the sending of emails (this would include attachments in text, image, audio, video as well as any additional electronic record transmitted with the message.) for the following purposes: (1) causing annoyance, or (2) causing inconvenience, or (3) to deceive or to mislead about the origin of the messages.

Illustration: Sameer sends emails to thousands of customers of the NatCash Bank. These emails request the recipient to click on a link and enter their online banking username and password at a website that appears to be that of the Bank but in reality is a fake. Sameer has spoofed the emails in such a way that they appear to have originated from the NatCash Bank official email address. He would be liable under this section.

Acts penalized	 (1) sending grossly offensive or menacing information by email, sms, mms etc (2) sending false information by email, sms, mms etc for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will
	(3) sending email, sms, mms etc for the purpose of causing annoyance or inconvenience
	(4) sending email, sms, mms etc to deceive or to mislead the addressee or recipient about the origin of such messages
Punishment	Imprisonment upto 3 years and fine
Punishment for attempt	Imprisonment upto 18 months and fine
Punishment for abetment	Imprisonment upto 3 years and fine
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	 (1) The accused sent grossly offensive or menacing information by email, sms, mms etc (2) The accused sent false information by email, sms, mms etc for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will (3) The accused sent email, sms, mms etc for the purpose of causing annoyance or inconvenience (4) The accused sent email, sms, mms etc to deceive or to mislead the addressee or recipient

	about the origin of such messages
Points for defence	(1) The nature of the information was such that it would generally not be considered grossly offensive or menacing
	(2) The accused had reason to believe that the information was true and did not send it for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will
	(3) The accused did not send the information for the purpose of causing annoyance or inconvenience
	(4) The accused did not have reason to believe that the addressee or recipient would be deceived or misled the about the origin of such messages(5) The accused did not have the relevant
	intention or knowledge(6) The acts were committed accidentally or by
	(b) The acts were committed accidentary of by mistake as the accused did not have the relevant technical expertise

CONVENTION ON CYBERCRIME:

Article 7 of the *Convention on Cybercrime* of the Council of Europe is titled "Computer-related forgery" and states-

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

66B. Punishment for dishonestly receiving stolen computer resource or communication device¹¹²

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason

¹¹² Inserted by Information Technology (Amendment) Act, 2008

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.

COMMENTS:

This section addresses the issue of dishonestly receiving stolen computer resource or communication device. This section applies to a person who dishonestly receives or retains (1) any stolen computer resource (computer, computer system, computer network, data, computer data base or software), or (2) any stolen communication device (cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image).

Section 24 of Indian Penal Code states-

Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

This section applies only if the person knows or has reason to believe that the computer resource or communication device is stolen.

> **Illustration:** Sameer has been arrested several times in the past for offences relating to theft. One day, he approaches Parag with 15 cell phones and offers to sell them for half their market value. Parag buys the cell phones from Sameer and then sells them in his shop for the full market value. Parag would be liable under this section.

Acts penalized	 (1) dishonestly receiving any stolen computer resource or communication device knowing or having reason to believe the same to be stolen (2) dishonestly retaining any stolen computer resource or communication device knowing or having reason to believe the same to be stolen
Punishment	Imprisonment upto 3 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto

	Rs 1 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 1 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector(2) Controller
	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	 (1) The accused dishonestly received / retained stolen computer resource or communication device (2) The accused knew or having reason to believe the same to be stolen
Points for defence	 (1) The accused did not have reason to believe that the computer resource or communication device was stolen (2) The accused received / retained the computer resource or communication device for the purpose of handing it over to the police or the rightful owner (3) The accused received / retained the computer resource or communication device for the purpose of tracing the rightful owner (4) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise to ascertain that the said were stolen

66C. Punishment for identity theft.¹¹³

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished

¹¹³ Inserted by Information Technology (Amendment) Act, 2008 260

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.

COMMENTS:

This section penalises identity theft. This section applies to cases where someone who dishonestly or fraudulently does the following: (1) makes use of the electronic signature of any other person, or (2) makes use of the password of any other person, or (3) makes use of any other unique identification feature of any other person.

Illustration: Sameer is a junior employee in a bank. He oversees his senior Pooja typing her password into her official computer. One day, Sameer logs into the banks system using Pooja's password and transfers some money into his account. He will be liable under this section.

Section 24 of Indian Penal Code states-

Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

Section 25 of Indian Penal Code states-

A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

Acts penalized	 (1) fraudulently making use of the electronic signature, password or any other unique identification feature of any other person (2) dishonestly making use of the electronic signature, password or any other unique identification feature of any other person
Punishment	Imprisonment upto 3 years and fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 18 months and fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 3 years and fine upto Rs 1 lakh
Whether cognizable?	Yes
Whether bailable?	Yes

[1
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime
	affects the socio economic conditions of the
	country or has been committed against a child
	below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section
	28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused made use of the electronic
	signature, password etc of any other person
	(2) The accused did this act fraudulently and / or
	dishonestly
	(3) The accused did not have any permission or
	legal right to use the said electronic signature,
	password etc
Points for defence	(1) The accused did not have reason to believe
	that the electronic signature, password etc
	belonged to some other person
	(2) The accused had permission, express or
	implied, to use the said electronic signature,
	password etc
	(3) The acts were committed accidentally or by
	mistake as the accused did not have the relevant
	technical expertise

CANADA:

A relevant provision is section 342.1 of the *Criminal Code* which is titled "Unauthorized use of computer", which states-

(1) Every one who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service,

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or

(b) or an offence under section 430 in relation to data or a computer system, or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

(2) In this section,

"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(a) contains computer programs or other data, and

(b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof;

"traffic" means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way.

MALAYSIA:

A relevant provision is section 6 of the *Computer Crimes Act*, titled "Wrongful communication" which states-

(1) A person shall be guilty of an offence if he communicates directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorized to communicate.

(2) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding twenty five thousand ringgit or to imprisonment for a term not exceeding three years or to both.

SINGAPORE:

A relevant provision is section 8 of the *Computer Misuse Act*, titled "Unauthorised disclosure of access code" which states-

(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so —

- (a) for any wrongful gain;
- (b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

66D. Punishment for cheating by personation by using computer resource¹¹⁴

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished

¹¹⁴ Inserted by Information Technology (Amendment) Act, 2008

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.

COMMENTS:

The term "cheating" is defined in section 415 of the *Indian Penal Code*, which states:

Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

Explanation,--A dishonest concealment of facts is a deception within the meaning of this section.

Illustrations

(a) A, by falsely pretending to be in the Civil Service, intentionally deceives Z, and thus dishonestly induces Z to let him have on credit goods for which he does not mean to pay. A cheats.

(b) A, by putting a counterfeit mark on an article, intentionally deceives Z into a belief that this article was made by a certain celebrated manufacturer, and thus dishonestly induces Z to buy and pay for the article. A cheats.

(c) A, by exhibiting to Z a false sample of an article, intentionally deceives Z into believing that the article corresponds with the sample, and thereby, dishonestly induces Z to buy and pay for the article. A cheats.

(d) A, by tendering in payment for an article a bill on a house with which A keeps no money, and by which A expects that the bill will be dishonoured, intentionally deceives Z, and thereby dishonestly induces Z to deliver the article, intending not to pay for it. A cheats.

(e) A, by pledging as diamonds article which he knows are not diamonds, intentionally deceives Z, and thereby dishonestly induces Z to lend money. A cheats.

(f) A intentionally deceives Z into a belief that A means to repay any money that Z may lend him and thereby dishonestly induces Z to lend him money. A does not intend to repay it. A cheats.

(g) A intentionally deceives Z into a belief that A means to deliver to Z a certain quantity of indigo plant which he does not intend to deliver, and thereby dishonestly induces Z to advance money upon the faith of such delivery. A cheats; but if A, at the time of obtaining the money, intends to deliver the indigo plant, and afterwards breaks his contract and does not deliver it, he does not cheat, but is liable only to a civil action for breach of contract.

(h) A intentionally deceives Z into a belief that A has performed A's part of a contract made with Z, which he has not performed, and thereby dishonestly induces Z to pay money. A cheats.

(i) A sells and conveys an estate to B. A, knowing that in consequence of such sale he has no right to the property, sells or mortgages the same to Z, without disclosing the fact of the previous sale and conveyance to B, and receives the purchase or mortgage money from Z. A cheats.

The term "cheating by personation" is defined in section 416 of the *Indian Penal Code*, which states:

A person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

Explanation.--The offence is committed whether the individual personated is a real or imaginary person.

Illustration

(a) A cheats by pretending to be a certain rich banker of the same name. A cheats by personation.

(b) A cheats by pretending to be B, a person who is deceased. A cheats by personation.

Section 66D of the *Information Technology Act* penalises cheating by personation by using a computer resource or any communication device.

Illustration: Pooja receives an email that appears to have been sent from her bank. The email urges her to click on the link in the email. When she does so, she is taken to "a secure page on the bank's website".

She believes the web page to be authentic and enters her username, password and other information. In reality, the website is a fake and Pooja's information is stolen and misused. The fake email and fake website had been created by Sameer. He would be liable under this section.

Acts penalized	(1) Cheating by personation using a computer
	resource
	(2) Cheating by personation using a cell phone or
	other communication device
Punishment	Imprisonment upto 3 years and fine upto Rs 1
	lakh
Punishment for attempt	Imprisonment upto 18 months and fine upto Rs 1
	lakh
Punishment for abetment	Imprisonment upto 3 years and fine upto Rs 1
	lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime
	affects the socio economic conditions of the
	country or has been committed against a child
	below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section
	28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused cheated someone
	(2) The said cheating was done by personation
	using a computer / communication device
Points for defence	(1) The accused did not have the relevant
	intention or knowledge
	(4) The acts were committed accidentally or by
	mistake as the accused did not have the relevant
	technical expertise
	1

66E. Punishment for violation of privacy.¹¹⁵

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, public 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.

COMMENTS:

This section penalizes intentionally or knowingly doing the following in respect of the image of a private area of any person without consent: (1) capturing, or (2) publishing, or (3) transmitting. The above is penalized if it is done under circumstances violating the privacy of that person.

Illustration: Pooja is trying out a new dress in the changing room of a clothing store. Sameer, an employee of the store has hidden a camera that records Pooja while she is changing her clothes. Sameer will be liable under this section.

Illustration: Pooja is a model for a company selling ladies undergarments. As part of her modelling assignment, she poses

¹¹⁵ Inserted by Information Technology (Amendment) Act, 2008.

in underwear. Siddharth is the photographer for that assignment. He takes several photographs of Pooja while she is wearing the underwear. Siddharth will not be liable under this section.

Acts penalized	 (1) Intentionally capturing, publishing or transmitting the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person (2) Intentionally capturing, publishing or transmitting the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person
Punishment	Imprisonment upto 3 years and / or fine upto Rs 2- lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 2 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 2 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	 Police officer not below the rank of Inspector Controller Officer authorised by Controller under section of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	 (1) The accused intentionally or knowingly captured, published or transmitted the image of a private area of any person (2) The accused did so without the consent of the victim (3) The accused did so under circumstances violating the privacy of the victim
Points for defence	(1) The accused had obtained the consent of the

victim, either expressly or impliedly
(2) The circumstances were such that they did not violate the privacy of the victim
(3) The accused did not have the relevant intention or knowledge
(4) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise

CANADA:

The relevant provision is section 162 of the *Criminal Code* titled "Voyeurism", which states-

(1) Every one commits an offence who, surreptitiously, observes — including by mechanical or electronic means — or makes a visual recording of a person who is in circumstances that give rise to a reasonable expectation of privacy, if

(*a*) the person is in a place in which a person can reasonably be expected to be nude, to expose his or her genital organs or anal region or her breasts, or to be engaged in explicit sexual activity;

(b) the person is nude, is exposing his or her genital organs or anal region or her breasts, or is engaged in explicit sexual activity, and the observation or recording is done for the purpose of observing or recording a person in such a state or engaged in such an activity; or

(c) the observation or recording is done for a sexual purpose.

(2) In this section, "visual recording" includes a photographic, film or video recording made by any means.

(3) Paragraphs (1)(a) and (b) do not apply to a peace officer who, under the authority of a warrant issued under section 487.01, is carrying out any activity referred to in those paragraphs.

(4) Every one commits an offence who, knowing that a recording was obtained by the commission of an offence under subsection (1), prints, copies, publishes, distributes, circulates, sells, advertises or makes available the recording, or has the recording in his or her possession for the purpose of printing, copying, publishing, distributing, circulating, selling or advertising it or making it available.

(5) Every one who commits an offence under subsection (1) or (4)

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or

(b) is guilty of an offence punishable on summary conviction.

(6) No person shall be convicted of an offence under this section if the acts that are alleged to constitute the offence serve the public good and do not extend beyond what serves the public good.

(7) For the purposes of subsection (6),

(*a*) it is a question of law whether an act serves the public good and whether there is evidence that the act alleged goes beyond what serves the public good, but it is a question of fact whether the act does or does not extend beyond what serves the public good; and

(b) the motives of an accused are irrelevant.

66F. Punishment for cyber terrorism.¹¹⁶

(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 authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised 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 authorised access, and by means of such conduct obtains

¹¹⁶ Inserted by Information Technology (Amendment) Act, 2008.

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.

COMMENTS:

Section 55 of the *Indian Penal Code* is titled "Commutation of sentence of imprisonment for life" and states-

In every case in which sentence of imprisonment for life shall have been passed, the appropriate Government may, without the consent of the offender, commute the punishment for imprisonment of either description for a term not exceeding fourteen years.

Acts penalized	(1) Doing the following 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:
	(i) causing denial of access to computer resource;(ii) attempting to unauthorizedly penetrate or access a computer resource; or
	(iii) introducing any computer contaminant,(2) Acts in (1) above are penalized if by means of such conduct, the accused causes or is likely to cause the following:
	(i) death or injuries to persons, or(ii) damage to property, or

	(iii) destruction of property, or
	(iv) disruption of supplies or services essential to
	the life of the community, or
	(v) adverse affect to the critical information
	infrastructure specified under section 70.
	(3) Unauthorizedly and knowingly / intentionally
	penetrating or accessing a computer resource and
	obtaining access to:
	(i) information that is restricted for reasons of the
	security of the State or foreign relations;
	(ii) restricted information, with reasons to believe
	that such information may be used to cause or
	likely to cause injury to: (a) the interests of the sovereignty and integrity of India (b) the security
	of the State (c) friendly relations with foreign
	States (d) public order, decency or morality,
	(iii) restricted information, with reasons to
	believe that such information may be used: (a) in
	relation to contempt of court (b) defamation (c)
	incitement to an offence (d) to the advantage of
	any foreign nation, group of individuals or otherwise.
Punishment	Imprisonment upto life imprisonment
Punishment for attempt Punishment for abetment	Imprisonment upto 10 years
	Imprisonment upto life imprisonment
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No.
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section
Relevant court	28 of Information Technology Act Court of Session
First appeal lies to	High Court
Points for prosecution	(1) The accused either had no authorization, or exceeded the authorization granted to him
	(2) The accused committed one or more of the
	acts penalized by this section
Points for defence	(1) The accused had authorization, whether
	express or implied
	(2) The accused did not have the relevant
	intention or knowledge

(3) The acts were committed accidentally or by
mistake as the accused did not have the relevant
technical expertise

UNITED KINGDOM:

A relevant provision is section 1 of the *Terrorism Act, 2000*, which defines terrorism. It states-

1.—(1) In this Act "terrorism" means the use or threat of action Terrorism: where— interpretation.

- (a) the action falls within subsection (2),
- (b) the use or threat is designed to influence the government or to intimidate the public or a section of the public, and

(c) the use or threat is made for the purpose of advancing a political, religious or ideological cause.

- (2) Action falls within this subsection if it-
 - (a) involves serious violence against a person,

(b) involves serious damage to property,

(c) endangers a person's life, other than that of the person committing the action,

(d) creates a serious risk to the health or safety of the public or a section of the public, or

(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

(3) The use or threat of action falling within subsection (2) which involves the use of firearms or explosives is terrorism whether or not subsection (1)(b) is satisfied.

67. Punishment for publishing or transmitting obscene material in electronic form.¹¹⁷

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

¹¹⁷ Also refer to the Order dated 27th February, 2003 [G.S.R. 181(E)] that prescribes the procedure for blocking of websites.

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 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.¹¹⁸

COMMENTS:

There is no settled definition of pornography or obscenity. What is considered simply sexually explicit but not obscene in USA may well be considered obscene in India. There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect.

Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive.

Other than the *Information Technology Act*, other Indian laws that deal with pornography include the *Indecent Representation of Women* (*Prohibition*) *Act* and the *Indian Penal Code*.

This section explains what is considered to be obscene and also lists the acts in relation to such obscenity that are illegal. To understand what constitutes obscenity in the electronic form, let us analyse the relevant terms.

¹¹⁸ Substituted by Information Technology (Amendment) Act, 2008 for "Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeal 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."

Any material in the context of this section would include video files, audio files, text files, images, animations etc. These may be stored on CDs, websites, computers, cell phones etc.

Lascivious is something that tends to excite lust.

Appeals to, in this context, means "arouses interest".

Prurient interest is characterized by lustful thoughts.

Effect means to produce or cause some change or event.

Tend to deprave and corrupt in the context of this section means "to lead someone to become morally bad".

Persons here refers to natural persons (men, women, children) and not artificial persons (such as companies, societies etc).

Having understood these terms, let us analyse what constitutes obscenity. To be considered obscene for the purpose of this section, the matter must satisfy at least one of the following conditions: (1) it must tend to excite lust, or (2) it must arouse interest in lustful thoughts, or (3) it must cause a person to become morally bad.

The above conditions must be satisfied in respect of a person who is the likely target of the material. This can be understood from the following illustration:

Illustration: Sameer launches a website that contains information on sex education. The website is targeted at higher secondary school students. Pooja is one such student who is browsing the said website. Her illiterate young maid servant happens to see some explicit photographs on the website and is filled with lustful thoughts.

This website would not be considered obscene. This is because it is most likely to be seen by educated youngsters who appreciate the knowledge sought to be imparted through the photographs. It is under very rare circumstances that an illiterate person would see these explicit images.

To understand the acts that are punishable in respect of obscenity in the electronic form, let us analyse the relevant terms.

Publishes means "to make known to others". It is essential that at least one natural person (man, woman or child) becomes aware or understands the information that is published. Simply putting up a website that is never visited by any person does not amount to publishing.

Illustration: Sameer has just hosted a website containing his articles written in English. Sameer has not published the articles. An automated software released by an Internet search engine

indexes Sameer's website. Sameer has still not published the articles. A Chinese man, who does not understand a word of English, accidentally visits Sameer's website. Sameer has still not published the articles. Pooja, who understands English, visits Sameer's website and reads some of his articles. Now, Sameer has published his articles.

Transmits means to pass along, convey or spread. It is not necessary that the "transmitter" actually understands the information being transmitted.

Illustration: Sameer has just hosted a website containing his articles. Pooja uses an Internet connection provided by Noodle Ltd to visit Sameer's website. Noodle Ltd has transmitted Sameer's articles to Pooja. However, Noodle employees are not actually aware of the information being transmitted by their computers.

Causes to be published means "to bring about the publishing of something". It is essential that the actual publishing must take place.

Illustration: Sameer has just hosted a website containing his articles. An automated software released by Noodle Internet search engine indexes Sameer's website. But no human being has still used that index to read these articles. Noodle has not caused Sameer's articles to be published. Based upon the index created by Noodle, Pooja reaches Sameer's website and reads some of his articles. Now, Noodle has caused Sameer's articles to be published.

Information in the electronic form includes websites, songs on a CD, movies on a DVD, jokes on a cell phone, photo sent as an email attachment etc.

CASE LAW: Avnish Bajaj vs. State (N.C.T.) of Delhi [(2005)3CompLJ364(Del), 116(2005)DLT427, 2005(79)DRJ576]

Summary of the case

Avnish Bajaj, CEO of Baazee.com, an online auction website, was arrested for distributing cyber pornography. The charges stemmed from the fact that someone had sold copies of a pornographic CD through the Baazee.com website. The court granted him bail in the case.

The major factors considered by the court were:

(1) There was no prima facie evidence that Mr. Bajaj directly or indirectly published pornography,

(2) The actual obscene recording/clip could not be viewed on Baazee.com,

(3) Mr. Bajaj was of Indian origin and had family ties in India.

Background

Avnish Bajaj is the CEO of Baazee.com, a customer-to-customer website, which facilitates the online sale of property. Baazee.com receives commission from such sales and also generates revenue from advertisements carried on its web pages.

An obscene MMS clipping was listed for sale on Baazee.com on 27th November, 2004 in the name of "DPS Girl having fun". Some copies of the clipping were sold through Baazee.com and the seller received the money for the sale. Avnish Bajaj was arrested under section 67 of the Information Technology Act, 2000 and his bail application was rejected by the trial court. He then approached the Delhi High Court for bail.

Issues raised by the Prosecution

(1) The accused did not stop payment through banking channels after learning of the illegal nature of the transaction.

(2) The item description "DPS Girl having fun" should have raised an alarm.

Issues raised by the Defence

(1) Section 67 of the Information Technology Act relates to publication of obscene material. It does not relate to transmission of such material.

(2) On coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend.

Findings of the court

(1) It has not been established that publication took place by the accused, directly or indirectly.

(2) The actual obscene recording/clip could not be viewed on the portal of Baazee.com.

(3) The sale consideration was not routed through the accused.

(4) Prima facie Baazee.com had endeavored to plug the loophole.

(5) The accused had actively participated in the investigations.

(6) The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof.

(7) Even though the accused is a foreign citizen, he is of Indian origin with family roots in India.

(8) The evidence that has been collected indicates only that the obscene material may have been unwittingly offered for sale on the website.

(9) The evidence that has been collected indicates that the heinous nature of the alleged crime may be attributable to some other person.

Decision of the court

(1) The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1 lakh each.

(2) The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the Court.

(3) The court also ordered Mr. Bajaj to participate and assist in the investigation.

Acts penalized	(1) Publishing or transmitting obscene electronic
	material
	(2) Causing to be published or transmitted obscene electronic material
Punishment	On first conviction: Imprisonment of either description upto 3 years and fine upto Rs 5 lakh
	On subsequent conviction: Imprisonment of either description upto 5 years and fine upto Rs 10 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 5 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	On first conviction: Yes
	However, it shall not be compounded if the crime
	affects the socio economic conditions of the country or has been committed against a child
	below the age of 18 years or against a woman
	On subsequent conviction: No
Investigation authorities	(1) Police officer not below the rank of Inspector
-	(2) Controller
	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused published or transmitted obscene
	electronic material
	(2) The accused caused obscene electronic

	material to be published or transmitted
Points for defence	(1) The electronic material was of such nature that it would not be considered obscene by the intended recipient
	(2) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise
	(3) The electronic material was for the public good (e.g. in the interest of science, literature, art, learning etc)
	(4) The electronic material was kept or used for bona fide heritage or religious purposes.

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.¹¹⁹

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.

COMMENTS:

This section penalises publishing or transmitting of material containing sexually explicit act in the electronic form.

> Illustration: Sameer and Pooja are engaged in the act of sexual intercourse in their hotel room. Siddharth, an employee of the hotel uses a hidden video camera to record this act. He then copies this video recording onto a CD and gives a copy to his friend. Siddharth is liable under this section.

This section does not apply to material justified as being for the public good (e.g. in the interest of science, literature, art, learning etc) or which is kept or used for bona fide heritage or religious purposes.

¹¹⁹ Inserted by Information Technology (Amendment) Act, 2008. 280

r	
Acts penalized	(1) Publishing or transmitting electronic material containing sexually explicit act or conduct
	(2) Causing to be published or transmitted electronic material containing sexually explicit act or conduct
Punishment	On first conviction: Imprisonment of either description upto 5 years and fine upto Rs 10 lakh On subsequent conviction: Imprisonment of either description upto 7 years and fine upto Rs 10 lakh
Punishment for attempt	Imprisonment upto 30 months and / or fine upto Rs 10 lakh
Punishment for abetment	Imprisonment upto 5 years and / or fine upto Rs 10 lakh
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	 (1) The accused published or transmitted electronic material containing sexually explicit act or conduct (2) The accused caused such material to be published or transmitted
Points for defence	 published or transmitted (1) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise (2) The electronic material was for the public good (e.g. in the interest of science, literature, art, learning etc) (3) The electronic material was kept or used for
	bona fide heritage or religious purposes.

67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.¹²⁰

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 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 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 *bona fide* heritage or religious purposes.

¹²⁰ Inserted by Information Technology (Amendment) Act, 2008.

Explanation – For the purposes of this section, "children" means a person who has not completed the age of 18 years.

COMMENTS:

This section penalises acts relating to obscene electronic material involving persons below the age of 18 years. The following acts are punishable under this section:

(1) Publishing or transmitting electronic material which depicts children engaged in sexually explicit act or conduct;

(2) Causing to be published or transmitted electronic material which depicts children engaged in sexually explicit act or conduct;

(3) Creating text or digital images depicting children in obscene or indecent or sexually explicit manner;

(4) Collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing electronic material depicting children in obscene or indecent or sexually explicit manner;

(5) Enticing or inducing children for online relationships for sexually explicit acts;

(6) Facilitating the online abuse of children;

(7) Recording in any electronic form sexually explicit acts with children.

This section does not apply to material justified as being for the public good (e.g. in the interest of science, literature, art, learning etc) or which is kept or used for bona fide heritage or religious purposes.

Acts penalized	(1) Publishing or transmitting electronic material which depicts children engaged in sexually
	explicit act or conduct (2) Causing to be published or transmitted electronic material which depicts children
	engaged in sexually explicit act or conduct (3) Creating text or digital images depicting children in obscene or indecent or sexually explicit manner
	(4) Collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing electronic material depicting children in obscene or indecent or sexually explicit

	(5) Cultivating, enticing or inducing children to
	online relationship with one or more children for sexually explicit act
	 (6) Cultivating, enticing or inducing children to online relationship with one or more children in a manner that may offend a reasonable adult (7) Facilitating abusing children online (8) Recording in any electronic form abuse pertaining to sexually explicit act with children
Punishment	On first conviction: Imprisonment of either
	description upto 5 years and fine upto Rs 10 lakh
	On subsequent conviction: Imprisonment of either description upto 7 years and fine upto Rs 10 lakh
Punishment for attempt	Imprisonment upto 30 months and / or fine upto Rs 10 lakh
Punishment for abetment	Imprisonment upto 5 years and / or fine upto Rs 10 lakh
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	The accused committed one or more of the acts penalized by this section
Points for prosecution Points for defence	
	penalized by this section(1) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise
	 penalized by this section (1) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise (2) The electronic material was for the public good (e.g. in the interest of science, literature, art,

CANADA:

A relevant provision is section 163.1 of the *Criminal Code* which is quoted as under-

163.1 (1) Definition of child pornography

In this section, "child pornography" means

(a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means, (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years;

(b) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act;

(c) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or

(d) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act.

163.1 (2) Making child pornography

Every person who makes, prints, publishes or possesses for the purpose of publication any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding ten years and to a minimum punishment of imprisonment for a term of one year; or

(b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of ninety days.

163.1 (3) Distribution, etc. of child pornography

Every person who transmits, makes available, distributes, sells, advertises, imports, exports or possesses for the purpose of

transmission, making available, distribution, sale, advertising or exportation any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding ten years and to a minimum punishment of imprisonment for a term of one year; or

(b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of ninety days.

163.1 (4) Possession of child pornography

Every person who possesses any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding five years and to a minimum punishment of imprisonment for a term of forty-five days; or

(b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of fourteen days.

163.1 (4.1) Accessing child pornography

Every person who accesses any child pornography is guilty of

(a) an indictable offence and liable to imprisonment for a term not exceeding five years and to a minimum punishment of imprisonment for a term of forty-five days; or

(b) an offence punishable on summary conviction and liable to imprisonment for a term not exceeding eighteen months and to a minimum punishment of imprisonment for a term of fourteen days.

163.1 (4.2) Interpretation

For the purposes of subsection (4.1), a person accesses child pornography who knowingly causes child pornography to be viewed by, or transmitted to, himself or herself.

163.1 (4.3) Aggravating factor

If a person is convicted of an offence under this section, the court that imposes the sentence shall consider as an aggravating factor the fact that the person committed the offence with intent to make a profit.

163.1 (5) Defence

It is not a defence to a charge under subsection (2) in respect of a visual representation that the accused believed that a person

shown in the representation that is alleged to constitute child pornography was or was depicted as being eighteen years of age or more unless the accused took all reasonable steps to ascertain the age of that person and took all reasonable steps to ensure that, where the person was eighteen years of age or more, the representation did not depict that person as being under the age of eighteen years.

163.1 (6) Defence

No person shall be convicted of an offence under this section if the act that is alleged to constitute the offence

(a) has a legitimate purpose related to the administration of justice or to science, medicine, education or art; and

(b) does not pose an undue risk of harm to persons under the age of eighteen years.

163.1 (7) Question of law

For greater certainty, for the purposes of this section, it is a question of law whether any written material, visual representation or audio recording advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act.

CONVENTION ON CYBERCRIME:

Article 9 of the *Convention on Cybercrime* of the Council of Europe is titled "Offences related to child pornography" and states-

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

(a) producing child pornography for the purpose of its distribution through a computer system;

(b) offering or making available child pornography through a computer system;

(c) distributing or transmitting child pornography through a computer system;

(d) procuring child pornography through a computer system for oneself or for another person;

(e) possessing child pornography in a computer system or on a computer-data storage medium.

(2) For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct;

(c) realistic images representing a minor engaged in sexually explicit conduct.

(3) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

(4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

67C. Preservation and retention of information by intermediaries¹²¹

(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.

Acts penalized	 (1) Intentionally or knowingly failing to preserve and retain information specified by the Central Government (2) Intentionally or knowingly failing to preserve and retain such information for such duration and in such manner and format as prescribed.
Punishment	Imprisonment upto 3 years and fine
Punishment for attempt	Imprisonment upto 18 months and fine
Punishment for abetment	Imprisonment upto 3 years and fine
Whether cognizable?	Yes

¹²¹ Inserted by Information Technology (Amendment) Act, 2008.

Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	 (1) The intermediary intentionally or knowingly failed to preserve and retain information specified by the Central Government (2) The intermediary intentionally or knowingly failed to preserve and retain such information for
	such duration and in such manner and format as prescribed.
Points for defence	 (1) The said information was destroyed for reasons beyond the control of the intermediary e.g. a virus attack, hard-disk failure etc (2) Prescribed information was never available to
	the intermediary.
	(3) The failure to retain / preserve the information was on account of mistake or reasons beyond the control of the intermediary
	(4) There was no knowledge or intention behind the failure to retain / preserve the information

68. Power of the Controller to give directions.

(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 thereunder.

(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 a fine not exceeding one lakh rupees or with both.¹²²

COMMENTS:

This is a simple section that empowers the Controller to order a Certifying Authority and its employees to comply with the *Information Technology Act* and allied laws. If they do not comply with the order to take suitable measures or cease certain activities, then they are liable for punishment under this section.

Illustration: The Controller orders Siddharth, a director of Noodle Certifying Authority to provide information about Sameer. Noodle had issued a digital signature certificate to Sameer. This information is needed in the adjudication of a case involving Sameer. If Noodle does not provide this information, it will be liable under this section.

Illustration: Noodle Certifying Authority is making statements in the media against other Certifying Authorities. Such statements are affecting the public confidence in the use of digital signatures and e-governance. The Controller orders Siddharth, a director of Noodle Certifying Authority to stop making such statements. If Siddharth does not stop such activities, he will be liable under this section.

Acts penalized	Intentionally or knowingly failing to comply with the order of the Controller
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh

¹²² Substituted by Information Technology (Amendment) Act, 2008 for "Any person who 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 three years or to a fine not exceeding two lakh rupees or to both."

Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1
i unisiment for abetinent	lakh
Whether cognizable?	No
whether cognizable.	
Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime
	affects the socio economic conditions of the
	country or has been committed against a child
	below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section
	28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The Controller directed a Certifying Authority
	or its employee to take specified measures or
	cease carrying on specified measures.
	(2) The order was issued to ensure compliance
	with the provisions of the Information Technology Act and allied rules or regulations.
	(3) The Certifying Authority or its employee
	knowingly and intentionally failed to comply
	with the order of the Controller
Points for defence	(1) The non-compliance was for reasons beyond
	the control of the certifying authority or its
	employee
	(2) The non-compliance was on account of mistake or reasons beyond the control of the
	mistake or reasons beyond the control of the certifying authority or its employee
	(3) There was no knowledge or intention behind
	the non-compliance
	(4) The order of the Controller was not issued to

Information regulations (5) Comply	npliance with the provisions of the n Technology Act and allied rules or ing with the order would have resulted of the law for the time being in force
--	---

69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.¹²³

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or 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 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 generated, transmitted, received or stored in any computer resource.

COMMENTS:

Under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009,

¹²³ Substituted by Information Technology (Amendment) Act, 2008 for 69. Directions of Controller to a subscriber to extend facilities to decrypt information. – (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber 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 decrypt the information. (3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

the competent authority is Secretary in the Department of Home Affairs (in case of the Central Government) and Secretary in charge of the Home Department (in case of State Government or Union Territory).

Some of the important terms defined under Rule 2 of the *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009* are:

(c) "Decryption" means the process of conversion of information in non-intelligible form to an intelligible information via a mathematical formula, code, password or algorithm or a combination thereof;

(d) "Decryption assistance" means to - (i) allow access, to the extent possible, to encrypted information; or (ii) facilitate conversion of encrypted information into an intelligible form;

(e) "Decryption direction" means a direction issued under Rule (3) in terms of which a decryption key holder is directed to - (i) disclose a decryption key; or (ii) provide decryption assistance in respect of encrypted information

(f) "Decryption key" means any key, mathematical formula, code, password, algorithm or any other data which is used to - (i) allow access to encrypted information: or (ii) facilitate the conversion of encrypted information into an intelligible form;

(g) "Decryption key holder" means any person who deploys the decryption mechanism and who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to direct or indirect communications;

(i) "Intercept" with its grammatical variations and cognate expressions, means the aural or other acquisition of the contents of any information through the use of any means, including an interception device, so as to make some or all of the contents of a information available to a person other than the sender or recipient or intended recipient of that communication, and includes the - (a) monitoring of any such communication by means of a monitoring device; (b) viewing, examination or inspection of the contents of any direct or indirect information; and (c) diversion of any direct or indirect information from its intended destination to any other destination;

(j) "Interception device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used

whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept any information;

and a reference to an "interception device" includes, where applicable, a reference to a "monitoring device";

(l) "Monitor" with its grammatical variations and cognate expressions, includes, to view or to inspect or listen to or record information by means of a monitoring device;

(m) "Monitoring device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or to inspect or to listen to or record any information;

(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.

COMMENTS:

The procedure and safeguards have been detailed under the *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.*

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to -

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, 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 imprisonment for a term which may extend to seven years and shall also be liable to fine.

COMMENTS:

Section 69 is a very important section that gives wide powers to the Government to intercept, monitor and decrypt information under special circumstances. The outline of this section is:

(1) The Government can direct any agency (e.g. police, CBI etc) to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource.

(2) The reasons for this order are to be recorded in writing.

(3) The Government must be satisfied that this order is necessary: (a) in the interest of the sovereignty or integrity or defence of India, or (b) in the interest of the security of the State, or (c) in the interest of friendly relations with foreign States, or (d) in the interest of public order, or (d) for preventing incitement to the commission of any cognizable offence relating to the above, or (e) for investigation of any offence.

(4) The Government agency can call upon any person for assistance to monitor, provide access to, intercept or decrypt information.

(5) If such a person does not provide such assistance then he is liable for imprisonment up to 7 years and fine.

Illustration: It is suspected that some terrorists are using the Noodle Ltd email services to plan a terrorist attack in India. The Government directs the police to intercept these emails.

The police request Sameer, the Director of Noodle Ltd for assistance in obtaining these emails. Sameer refuses to cooperate. He would be liable under this section.

Illustration: The Controller suspects that Parag and Siddharth are planning a major hacking attempt on Indian Government websites. The Government directs the police to intercept information being transmitted by them on the Internet.

The suspects are using the Internet services provided by Noodle Ltd. The police request Sameer, the Director of Noodle Ltd for assistance in obtaining this information. Sameer refuses to cooperate. He would be liable under this section.

Acts penalized	(1) Not providing access to the relevant computer
	resource
	(2) Not providing assistance to intercept, monitor,

	or decrypt the relevant information
	(3) Not providing assistance to provide relevant
	information
Punishment	Imprisonment upto 7 years and fine
Punishment for attempt	Imprisonment upto 3.5 years and fine
Punishment for abetment	Imprisonment upto 7 years and fine
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section
	28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused did not extend all facilities and technical assistance to provide access to the relevant computer resource
	(2) The accused did not extend all facilities and technical assistance to intercept, monitor, or decrypt the information
	(3) The accused did not extend all facilities and technical assistance to provide information stored in the relevant computer resource
Points for defence	(1) The order was not issued by the authorized agency or official
	(2) The reasons for the order were not recorded(3) The prescribed procedures and safeguards were not carried out by the authorized agency or
	official
	(4) The accused did not have the technical capabilities to comply with the order
	(5) The accused was unable to comply with the order due to reasons outside its control

UNITED KINGDOM:

Some relevant provisions are sections 49, 53 and 56 of the *Regulation of Investigatory Powers Act 2000,* which state-

Part III Investigation of electronic data protected by encryption etc. Power to require disclosure

49.—(1) This section applies where any protected information—

(a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;

(b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications, or is likely to do so;

(c) has come into the possession of any person by means of the exercise of any power conferred by an authorisation under section 22(3) or under Part II, or as a result of the giving of a notice under section 22(4), or is likely to do so;

(d) has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or

(e) has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police or the customs and excise, or is likely so to come into the possession of any of those services, the police or the customs and excise.

(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds—

(a) that a key to the protected information is in the possession of any person,

(b) that the imposition of a disclosure requirement in respect of the protected information is—

(i) necessary on grounds falling within subsection (3), or

(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,

(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and

(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected

information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime; or

(c) in the interests of the economic well-being of the United Kingdom.

(4) A notice under this section imposing a disclosure requirement in respect of any protected information—

(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;

(b) must describe the protected information to which the notice relates;

(c) must specify the matters falling within subsection (2)(b)(i) or (ii) by reference to which the notice is given;

(d) must specify the office, rank or position held by the person giving it;

(e) must specify the office, rank or position of the person who for the purposes of Schedule 2 granted permission for the giving of the notice or (if the person giving the notice was entitled to give it without another person's permission) must set out the circumstances in which that entitlement arose;

(f) must specify the time by which the notice is to be complied with; and

(g) must set out the disclosure that is required by the notice and the form and manner in which it is to be made; and the time specified for the purposes of paragraph (f) must allow a period for compliance which is reasonable in all the circumstances.

(5) Where it appears to a person with the appropriate permission—

(a) that more than one person is in possession of the key to any protected information,

(b) that any of those persons is in possession of that key in his capacity as an officer or employee of any body corporate, and

(c) that another of those persons is the body corporate itself or another officer or employee of the body corporate, a notice under this section shall not be given, by reference to his possession of the key, to any officer or employee of the body corporate unless he is a senior officer of the body corporate or it appears to the person giving the notice that there is no senior officer of the body corporate and (in the case of an employee) no more senior employee of the body corporate to whom it is reasonably practicable to give the notice.

(6) Where it appears to a person with the appropriate permission—

(a) that more than one person is in possession of the key to any protected information,

(b) that any of those persons is in possession of that key in his capacity as an employee of a firm, and

(c) that another of those persons is the firm itself or a partner of the firm, a notice under this section shall not be given, by reference to his possession of the key, to any employee of the firm unless it appears to the person giving the notice that there is neither a partner of the firm nor a more senior employee of the firm to whom it is reasonably practicable to give the notice.

(7) Subsections (5) and (6) shall not apply to the extent that there are special circumstances of the case that mean that the purposes for which the notice is given would be defeated, in whole or in part, if the notice were given to the person to whom it would otherwise be required to be given by those subsections.

(8) A notice under this section shall not require the making of any disclosure to any person other than—

(a) the person giving the notice; or

(b) such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice.

(9) A notice under this section shall not require the disclosure of any key which—

(a) is intended to be used for the purpose only of generating electronic signatures; and

(b) has not in fact been used for any other purpose.

(10) In this section "senior officer", in relation to a body corporate, means a director, manager, secretary or other similar officer of the body corporate; and for this purpose "director", in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate.

(11) Schedule 2 (definition of the appropriate permission) shall have effect.

53.—(1) A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice.

(2) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.

(3) For the purposes of this section a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if—

(a) sufficient evidence of that fact is adduced to raise an issue with respect to it; and

(b) the contrary is not proved beyond a reasonable doubt.

(4) In proceedings against any person for an offence under this section it shall be a defence for that person to show—

(a) that it was not reasonably practicable for him to make the disclosure required by virtue of the giving of the section 49 notice before the time by which he was required, in accordance with that notice, to make it; but

(b) that he did make that disclosure as soon after that time as it was reasonably practicable for him to do so.

(5) A person guilty of an offence under this section shall be liable—

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;

(b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

56.—(1) In this Part—

"chief officer of police" means any of the following-

(a) the chief constable of a police force maintained under or by virtue of section 2 of the Police Act 1996 or section 1 of the Police (Scotland) Act 1967;

(b) the Commissioner of Police of the Metropolis;

(c) the Commissioner of Police for the City of London;

(d) the Chief Constable of the Royal Ulster Constabulary;

(e) the Chief Constable of the Ministry of Defence Police;

(f) the Provost Marshal of the Royal Navy Regulating Branch;

(g) the Provost Marshal of the Royal Military Police;

(h) the Provost Marshal of the Royal Air Force Police;

(i) the Chief Constable of the British Transport Police;

(j) the Director General of the National Criminal Intelligence Service;

(k) the Director General of the National Crime Squad;

"the customs and excise" means the Commissioners of Customs and Excise or any customs officer;

"electronic signature" means anything in electronic form which-

(a) is incorporated into, or otherwise logically associated with, any electronic communication or other electronic data;

(b) is generated by the signatory or other source of the communication or data; and

(c) is used for the purpose of facilitating, by means of a link between the signatory or other source and the communication or data, the establishment of the authenticity of the communication or data, the establishment of its integrity, or both;

"key", in relation to any electronic data, means any key, code, password, algorithm or other data the use of which (with or without other keys)—

(a) allows access to the electronic data, or

(b) facilitates the putting of the data into an intelligible form;

"the police" means—

(a) any constable;

(b) the Commissioner of Police of the Metropolis or any Assistant Commissioner of Police of the Metropolis; or

(c) the Commissioner of Police for the City of London;

"protected information" means any electronic data which, without the key to the data—

(a) cannot, or cannot readily, be accessed, or

(b) cannot, or cannot readily, be put into an intelligible form;

"section 49 notice" means a notice under section 49;

"warrant" includes any authorisation, notice or other instrument (however described) conferring a power of the same description as may, in other cases, be conferred by a warrant.

69A. Power to issue directions for blocking for public access of any information through any computer resource.¹²⁴

(1) Where the Central Government or any of its officers 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 or cause to be blocked for access by the 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 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.

¹²⁴ Inserted by Information Technology (Amendment) Act, 2008.

COMMENTS:

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 contain detailed provisions relating to the procedure and safeguards for blocking for access of information by public.

Section 69A gives powers to the Government to block access to information under special circumstances. The outline of this section is:

(1) The Government can direct any Government agency or intermediary to block for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The reasons for this order are to be recorded in writing.

(3) The Government must be satisfied that this order is necessary: (a) in the interest of the sovereignty or integrity or defence of India, or (b) in the interest of the security of the State, or (c) in the interest of friendly relations with foreign States, or (d) in the interest of public order, or (e) for preventing incitement to the commission of any cognizable offence relating to the above.

(4) If the intermediary does not comply, it will be liable for imprisonment up to 7 years and fine.

Acts penalized	Not blocking for access, by the public, specified information
Punishment	Imprisonment upto 7 years and fine
Punishment for attempt	Imprisonment upto 3.5 years and fine
Punishment for abetment	Imprisonment upto 7 years and fine
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	 Police officer not below the rank of Inspector Controller Officer authorised by Controller under section of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused did not block for access by the public any information generated, transmitted, received, stored or hosted in any computer

	resource (2) The accused did not cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource
Points for defence	 (1) The order was not issued by the authorized agency or official (2) The reasons for the order were not recorded (3) The prescribed procedures and safeguards were not carried out by the authorized agency or official (4) The accused did not have the technical capabilities to comply with the order (5) The accused was unable to comply with the order due to reasons outside its control

69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.¹²⁵

(1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise 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 or the computer resource shall, when called upon by the agency which has been authorised 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.

(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

¹²⁵ Inserted by Information Technology (Amendment) Act, 2008.

punished with an imprisonment for a term which any 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 and any other information.

COMMENTS:

The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 contain detailed provisions for the procedure and safeguard for monitoring and collecting traffic data or information. Some of the important terms defined in rule 2 include:

(f) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service/ disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization;

(g) "Cyber security breaches" means unauthorized acquisition or unauthorized use by a person of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource;

(i) "Information security practices" means implementation of security policies and standards in order to minimize the cyber security incidents and breaches;

(k) "Monitor" with its grammatical variations and cognate expressions, includes to view or inspect or record or collect traffic data or information by means of a monitoring device;

(l) "Monitoring device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument,

device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or inspect or record or collect traffic data or information;

(m) "Port" or "Application Port" means a set of software rules which identifies and permits communication between application to application, network to network, computer to computer, computer system to computer system;

(o) security policy means documented business rules and processes for protecting information and the computer resource;

Section 69B gives powers to the Government to monitor and collect traffic data or information for cyber security. The outline of this section is:

(1) The Central Government can authorise any Government agency to monitor and collect traffic data or other electronic information.

(2) Such an authorization can be made under the following circumstances: (a) to enhance cyber security in the country (b) for identification, analysis and prevention of intrusion in the country, or (c) for identification, analysis and prevention of spread of computer contaminant in the country.

(3) Such an authorization must be made by a notification in the Official Gazette.

Acts penalized	(1) Not providing technical assistance to the authorized agency(2) Not extending all relevant facilities to the authorized agency
Punishment	Imprisonment upto 3 years and fine
Punishment for attempt	Imprisonment upto 18 months and fine
Punishment for abetment	Imprisonment upto 3 years and fine
Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman

T /• /• /• /•	
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section
	28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused did not provide technical
	assistance to the authorized agency
	(2) The accused did not extend all relevant
	facilities to the authorized agency
Points for defence	(1) The order was not issued by the authorized agency or official
	(2) The prescribed procedures and safeguards
	were not carried out by the authorized agency or
	official
	(3) The accused did not have the technical
	capabilities to comply with the order
	(4) The accused was unable to comply with the
	order due to reasons outside its control

CONVENTION ON CYBERCRIME:

According to article 1(d) of the *Convention on Cybercrime* of the Council of Europe, "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

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.¹²⁶

¹²⁶ Also refer to Executive Order dated 12th September, 2002 which states inter alia that "For the purpose of sub-section 1 of Section 70 of the Act, details of every protected computer, computer system or computer network so notified by appropriate government may be informed to the Controller of Certifying Authorities, Department of Information Technology, 6 CGO Complex, New Delhi for the purpose of records and exercising powers under the said Act".

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;¹²⁷

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised 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.

COMMENTS:

There are three elements to this section-

(1) Gazette notification by the appropriate Government for declaring a computer resource as a protected system¹²⁹.

(2) Government order authorizing persons to access protected systems.

(3) Punishment for securing access or attempting to secure access to protected systems by unauthorised persons.

Let us discuss the relevant terms and issues in detail.

Appropriate government is determined as per Schedule VII of the Constitution of India. Schedule VII of the Constitution of India contains three lists – Union, State and Concurrent. Parliament has the exclusive

¹²⁸ Inserted by Information Technology (Amendment) Act, 2008.

¹²⁹ To be declared as a Protected System, a computer resource must be such that it directly or indirectly affects the facility of Critical Information Infrastructure. "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.

¹²⁷ Substituted by Information Technology (Amendment) Act, 2008 for "The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system."

right to make laws on items covered in the Union List e.g. defence, Reserve Bank of India etc. State Governments have the exclusive right to make laws on items covered in the State List e.g. police, prisons etc. Parliament as well as the State Governments can make laws on matters in the Concurrent List e.g. forests, electricity etc.

Illustration: If the computer network of the Indian Army is to be declared as a protected system, the Central Government would be the appropriate Government.

Illustration: If the computer network of the Mumbai police is to be declared as a protected system, the Government of Maharashtra would be the appropriate Government.

Illustration: If the computer network of the Forest Department in Maharashtra is to be declared as a protected system, the Central Government as well as the Government of Maharashtra would be the appropriate Government.

All the acts, rules, regulations etc passed by the Central and State Government are notified in the Official Gazette. The Official Gazette in the electronic form is called the Electronic Gazette. A notification becomes effective on the date of its publication in the Gazette.

The Government order may specify the authorised persons by name or by designation (e.g. all officers of rank of Inspector and above deputed in a particular department).

The term "securing access" in this section is a grammatical variation of the term "secures access" as discussed earlier.

Attempt to secure access is a very wide term and can best be understood through the following illustrations.

Illustration: Sameer runs a password cracking software to crack the password of a protected system. Irrespective of whether he succeeds in cracking the password, he is guilty of attempting to secure access.

Illustration: Sameer runs automated denial of service software to bring down the firewall securing a protected system. Irrespective of whether he succeeds in bringing down the firewall, he is guilty of attempting to secure access.

Illustration: Sameer sends a Trojan by email to Pooja, who is the network administrator of a protected system. He plans to Trojanize Pooja's computer and thereby gain unauthorised access to the protected system. Irrespective of whether he succeeds in finally accessing the protected system, he is guilty of attempting to secure access. As per Executive Order dated 12th September, 2002, issued by Ministry of Communications & Information Technology, details of every protected system should be provided to the Controller of Certifying Authorities.

Acts penalized	(1) Securing access to a protected system
	(2) Attempting to secure access to a protected system
Punishment	Imprisonment upto 10 years and fine
Punishment for attempt	Imprisonment upto 10 years and fine
Punishment for abetment	Imprisonment upto 10 years and fine
Whether cognizable?	Yes
Whether bailable?	No
Whether compoundable?	No
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Court of Session
First appeal lies to	High Court
Points for prosecution	(1) The accused secured access to a protected system
	(2) The accused attempted to secure access to a protected system
Points for defence	(1) The accused was authorised to access the protected system
	(2) The accused did not have the relevant intention or knowledge
	(3) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise

SUMMARY:

SINGAPORE:

A relevant provision is section 9 of the *Computer Misuse Act*, titled "Enhanced punishment for offences involving protected computers" which states-

(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 20 years or to both.

(2) For the purposes of subsection (1), a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —

(a) the security, defence or international relations of Singapore;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

70A. National Nodal Agency¹³⁰

(1) The Central Government may, by notification published in the Official Gazette, designate any organisation of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

¹³⁰ Inserted by Information Technology (Amendment) Act, 2008.

(2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

70B. Indian Computer Emergency Response Team to serve as national agency for incident response¹³¹

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director-General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,-

(a) collection, analysis and dissemination of information on cyber incidents;

(b) forecast and alerts of cyber security incidents;

(c) emergency measures for handling cyber security incidents;

(d) coordination of cyber incidents response activities;

(e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, preventation, response and reporting of cyber incidents;

(f) such other functions relating to cyber security as may be prescribed.

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

¹³¹ Inserted by Information Technology (Amendment) Act, 2008.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.

(7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1)."

Acts penalized	 (1) The accused did not provide the information called for by the Indian Computer Emergency Response Team (2) The accused did not comply with a direction of Indian Computer Emergency Response Team
Punishment	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 6 months and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes. However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	 Police officer not below the rank of Inspector Controller Officer authorised by Controller under section of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session

Points for prosecution	(1) The accused did not provide the information called for by the Indian Computer Emergency Response Team(2) The accused did not comply with a direction of Indian Computer Emergency Response Team
Points for defence	 (1) The accused did not have the technical capabilities to provide the information (2) The accused did not have the technical capabilities to comply with the direction (3) The accused was unable to comply with the direction due to reasons outside its control (4) The accused was unable to comply with the direction due to reasons outside its control

71. Penalty for misrepresentation.

Whoever makes any misrepresentation, to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Electronic Signature¹³² Certificate, as the case may be, shall be punished with imprisonment for a terms which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

COMMENTS:

This section applies to:

(1) a person, who, for obtaining an electronic signature certificate (a) makes a misrepresentation to the Certifying Authority or (b) suppresses any material fact from the Certifying Authority.

(2) a person obtaining a license to operate as a Certifying Authority (a) makes a misrepresentation to the Controller or (b) suppresses any material fact from the Controller.

Let us examine the essential terms of this section.

Misrepresentation implies "presenting information incorrectly, improperly or falsely". There must be a deliberate intention to deceive.

Illustration: Sameer is applying for a digital signature certificate. He fills in his name as "Siddharth" and also submits photocopies of Siddharth's passport as proof of identity. Sameer

¹³² The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

is liable for misrepresenting information to the Certifying Authority.

Suppress implies "to withhold from disclosure".

Illustration: Noodle Ltd is applying for a licence to become a Certifying Authority. One of the questions in the application form is "In case any of the company directors been convicted for a criminal offence, then please mention relevant details."

One of the Noodle directors has been convicted in the past. But, Noodle officials submit the filled in form with the answer to this question being left blank. The officials will be liable for suppressing information from the Controller.

Material fact implies something that is "relevant, pertinent or essential".

Acts penalized	(1) Misrepresentation to the Controller for obtaining any licence
	(2) Suppression of any material fact from the Controller for obtaining any licence
	(3) Misrepresentation to the Certifying Authority for obtaining any Electronic Signature Certificate
	(4) Suppression of any material fact from the Certifying Authority for obtaining any Electronic Signature Certificate
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector(2) Controller
	(3) Officer authorised by Controller under section

	28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused made a misrepresentation to the Controller for obtaining any licence
	(2) The accused suppressed a material fact from the Controller for obtaining any licence
	(3) The accused made a misrepresentation to the Certifying Authority for obtaining any Electronic Signature Certificate
	(4) The accused suppressed a material fact from the Certifying Authority for obtaining any Electronic Signature Certificate
Points for defence	(1) The act was a result of a mistake or negligence and was not done with knowledge or intention
	(2) The alleged misrepresentation or suppression was due to incorrect information provided to the accused by others
	(3) The acts were committed accidentally or by mistake as the accused did not have the relevant technical expertise

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, if any person who, in pursuance 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.

COMMENTS:

The essential elements of this section are:

(1) It applies to persons who have secured access to some information in pursuance of a power granted under the IT Act or its allied laws (e.g. police, adjudicating officers, Controller etc).

(2) Such persons must disclose this information to a third person without authorisation.

(3) There must be no law which permits such disclosure of information.

Illustration: Pooja is a Deputy Superintendent of Police and is investigating an alleged violation of the IT Act. She raids the premises of one of the suspects, Sameer.

During the raid, she seizes several documents and CDs containing incriminating evidence. She later discloses this information to the Magistrate trying the case. Even though Sameer's permission is not taken, Pooja would not be liable under this section. This is because the Code of Criminal Procedure permits such information and evidence to be disclosed to the Court. However, if Pooja discloses such information to the press without Sameer's permission, then she will be liable under this section.

Acts penalized	(1) Disclosure of records without consent
	(2) Person who discloses records must have obtained the same in pursuance of powers conferred under the Information Technology Act or allied rules, regulations etc
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller

	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused disclosed records without consent
	(2) The accused had obtained the records in pursuance of powers conferred under the Information Technology Act or allied rules, regulations etc
Points for defence	(1) The accused had not obtained the records in pursuance of powers conferred under the Information Technology Act or allied rules, regulations etc
	(2) The disclosure was a result of a mistake or negligence and was not done with knowledge or intention
	(3) The disclosure was committed accidentally or by mistake as the accused did not have the relevant technical expertise
	(4) The accused had obtained consent for the disclosure
	(5) The accused was acting in the discharge of his duties under the law

72A. Punishment for disclosure of information in breach of lawful contract.¹³³

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 fine which may extend to five lakh rupees, or with both.

¹³³ Inserted by Information Technology (Amendment) Act, 2008.

COMMENTS:

This section applies to: 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. This person will be penalised if he discloses such material:

(1) without the consent of the person concerned, or in breach of a lawful contract, and

(2) with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

This section does not apply if the person reveals this information in compliance with any law.

Illustration: Sameer works in a call-centre for a large bank. He has access to the financial records of all the customers of the bank. He comes to know that Pooja has fixed deposits worth Rs 2 crore. He passes on this information to his friend Siddharth, who starts threatening Pooja in order to extort money from her. Sameer would be liable under this section.

Illustration: Sameer works in a call-centre for a large bank. He has access to the financial records of all the customers of the bank. One day, he is approached by the police who are seeking information about a suspected terrorist who happens to be a customer of the bank. Sameer hands over the banking records of this suspect to the police. He would not be liable under this section as he is acting in conformance with the law which requires everyone to assist the police.

Acts penalized	(1) Disclosure of personal information about some other person
	(2) The disclosure must either be without consent or in breach of contract
	(3) There must be intention to cause wrongful loss or wrongful gain or knowledge that wrongful loss or wrongful gain may be caused
Punishment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh
Punishment for attempt	Imprisonment upto 18 months and / or fine upto Rs 5 lakh
Punishment for abetment	Imprisonment upto 3 years and / or fine upto Rs 5 lakh

Whether cognizable?	Yes
Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	 (1) The accused disclosed personal information about some other person (2) The accused made the disclosure either without consent or in breach of contract (3) The accused had the intention to cause wrongful loss or wrongful gain or knowledge that wrongful loss or wrongful gain may be caused
Points for defence	(1) The act was a result of a mistake or negligence and was not done with knowledge or intention
	(2) The disclosure was committed accidentally or by mistake as the accused did not have the relevant technical expertise
	(3) The accused had obtained consent for the disclosure
	(4) The accused was acting in the discharge of his duties under the law
	(5) The accused did not breach the terms of any contract

73. Penalty for publishing Electronic Signature Certificate false in certain particulars.¹³⁴

(1) No person shall publish a Electronic Signature¹³⁵ 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 purposes of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of subsection (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.

COMMENTS:

Let us examine this section through some illustrations.

Illustration: Sameer has created a fake digital signature certificate purporting to have been issued by Noodle Certifying Authority. Sameer plans to use this certificate to carry out some financial frauds. He posts this certificate on his website. He is liable under this section.

Illustration: Pooja has applied to Noodle Certifying Authority for a digital signature certificate. Noodle in due course issues the certificate to Pooja. She, however, does not accept it as some of the details are incorrect in the certificate. In the meanwhile, Noodle Ltd publishes her certificate in their online repository. In this case, Noodle Ltd will be liable under this section.

Illustration: Pooja is employed with Noodle Ltd. She has obtained a digital signature certificate for official purposes on 1st

¹³⁴ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

¹³⁵ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

January. She quits her job on 1^{st} July and her certificate is revoked on that day. Noodle Ltd continues to keep Pooja's revoked certificate in its online repository even after 1^{st} July. Noodle Ltd will be liable under this section. They will not be liable if the purpose behind keeping Pooja's certificate in their repository is to verify documents signed by Pooja between 1^{st} January and 1^{st} July.

Acts penalized	(1) Publishing an Electronic Signature Certificate with the knowledge that the Certifying Authority listed in it has not issued it
	(2) Publishing an Electronic Signature Certificate with the knowledge that the subscriber listed in it has not accepted it
	(3) Publishing an Electronic Signature Certificate with the knowledge that the certificate has been revoked or suspended
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh
Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh
Whether cognizable?	No
Whether bailable?	Yes
Whether compoundable?	Yes.
	However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman
Investigation authorities	(1) Police officer not below the rank of Inspector
	(2) Controller
	(3) Officer authorised by Controller under section28 of Information Technology Act
Relevant court	Magistrate of the first class
First appeal lies to	Court of Session
Points for prosecution	(1) The accused published an Electronic Signature Certificate with the knowledge that the Certifying Authority listed in it has not issued it

	 (2) The accused published an Electronic Signature Certificate with the knowledge that the subscriber listed in it has not accepted it (3) The accused published an Electronic Signature Certificate with the knowledge that the certificate has been revoked or suspended 			
Points for defence	 (1) The act was a result of a mistake or negligence and was not done with knowledge or intention (2) The disclosure was committed accidentally or by mistake as the accused did not have the relevant technical expertise (3) The publication was for the purposes of verifying a digital signature created prior to such suspension or revocation. (4) The accused was acting in the discharge of his duties under the law 			

74. Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature¹³⁶ 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.

SUMMARY:

Acts penalized	Knowingly creating, publishing or making available an Electronic Signature Certificate for any fraudulent or unlawful purpose		
Punishment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh		
Punishment for attempt	Imprisonment upto 1 year and / or fine upto Rs 1 lakh		
Punishment for abetment	Imprisonment upto 2 years and / or fine upto Rs 1 lakh		

¹³⁶ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

Whether cognizable?	No		
Whether bailable?	Yes		
Whether compoundable?	Yes.		
	However, it shall not be compounded if the crime affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or against a woman		
Investigation authorities	(1) Police officer not below the rank of Inspector		
	(2) Controller		
	(3) Officer authorised by Controller under section28 of Information Technology Act		
Relevant court	Magistrate of the first class		
First appeal lies to	Court of Session		
Points for prosecution	 (1) The accused knowingly created, published or made available an Electronic Signature Certificate for any fraudulent purpose (2) The accused knowingly created, published or made available an Electronic Signature Certificate for any unlawful purpose 		
Points for defence	(1) The act was a result of a mistake or negligence and was not done with knowledge or intention		
	(2) The disclosure was committed accidentally or by mistake as the accused did not have the relevant technical expertise		
	(3) The act was not for any fraudulent purpose		
	(4) The act was not for any unlawful purpose		

75. Act to apply for offence or contravention committed outside India.

(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.

(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.

COMMENTS:

Extradition is the delivery of a person accused of a crime in one country by the other country where he has sought refuge.

Illustration: Sameer has committed a crime in India and then escaped to USA. The US government could extradite Sameer to India so that he can face trial for his crime.

The delivery takes place pursuant to an existing treaty or an ad hoc arrangement. Extradition is based on the broad principle that it is in the interest of civilized communities that crimes should not go unpunished.

The domestic law of the nation from whom the extradition of the person is sought plays a crucial role in determining whether the State seeking the extradition would be granted its request or not.

Extradition Act, 1962 is the relevant law in India¹³⁷.

Following are relevant extracts from the Central Bureau of Investigation website [http://www.cbi.gov.in/interpol/extradition.php]:

Extradition may be briefly described as the surrender of an alleged or convicted criminal by one State to another. More precisely, extradition may be defined as the process by which one State upon the request of another surrenders to the latter a person found within its jurisdiction for trial and punishment or, if he has been already convicted, only for punishment, on account of a crime punishable by the laws of the requesting State and committed outside the territory of the requested State.

Extradition plays an important role in the international battle against crime. It owes its existence to the so-called principle of territoriality of criminal law, according to which a State will not apply its penal statutes to acts committed outside its own boundaries except where the protection of special national

¹³⁷ India has entered into extradition treaties with Belgium (1958), Bhutan (1997), Canada (1987), Hong Kong (1997), Nepal(old Treaty) (1963), Netherlands (1989), Russia (2000), Switzerland (1996), UAE (2000), U.K. (1993), USA (1999), Uzbekistan (2002), Spain (2003), Mongolia (2004), Turkey (2003), Germany (2004), Tunisia (2004), Oman (2005), France (2005), Poland (2005), Korea(ROK) (2004), Bahrain (2005), Bulgaria (2006), Ukraine (2006), South Africa (2005), Belarus (2008), Kuwait (2007) and Mauritius (2008). Additionally India has extradition agreements with Australia (1971), Fiji (1979), Italy (2003), Papua New Guinea (1978), Singapore (1972), Sri Lanka (1978), Sweden (1963), Tanzania (1966), Thailand (1982) and Portugal (2002). Source: Central Bureau of Investigation website accessed on 15th October 2009: http://www.cbi.gov.in/interpol/extradition.php

interests is at stake. In view of the solidarity of nations in the repression of criminality, however, a State, though refusing to impose direct penal sanctions to offences committed abroad, is usually willing to cooperate otherwise in bringing the perpetrator to justice lest he goes unpunished.

ICPO-Interpol has been a forerunner in international efforts to improve and accelerate existing procedure of extradition. Apart from attempts by academic bodies such as the Harvard Research Draft Convention on Extradition, the ICPO-Interpol was the first international organization to recommend to member countries a Draft General Agreement for the Extradition of Offenders, which unfortunately has remained a dead letter since it was adopted by the General Assembly of the Organization (then known as the International Criminal Police Commission) in 1948.

Interpol's interest in finding ways of improving the extradition process did not end with the failure of the Draft General Agreement. Since the early fifties, the General Secretariat of the ICPO-Interpol has undertaken on behalf of the member countries two new activities intended to facilitate international police cooperation in matters relating to extradition.

The first of these initiatives concerns the publication of a series of circulars on a country basis, setting out the provisional measures that the police in each country may take when complying with a request from the police of another member country for quick action with a view to identification and arrest of a person wanted on a warrant of arrest. The second initiative taken by the ICPO-Interpol consists in the dissemination of national extradition laws. This activity is based on a resolution of the General Assembly passed in 1967 in Tokyo (Japan) inviting member countries to forward the texts of their extradition laws to the General Secretariat so that the latter may send them to other member countries for their information. The pre-extradition circulars and the texts of extradition laws of the member countries received from the General Secretariat are being maintained in the Interpol Wing.

Position in India

In India the extradition of a fugitive from India to a foreign country or vice-versa is governed by the provisions of Indian Extradition Act, 1962. The basis of extradition could be a treaty between India and a foreign country. Under section 3 of this Act, a notification could be issued by the Government of India extending the provisions of the Act to the country/countries notified.

Information regarding the fugitive criminals wanted in foreign countries is received directly from the concerned country or through the General Secretariat of the ICPO-Interpol in the form of red notices. The Interpol Wing of the Central Bureau of Investigation immediately passes it on to the concerned police organizations. The red notices received from the General Secretariat are circulated to all the State Police authorities and immigration authorities.

The question arises that what action, if any, can be taken by the Police on receipt of an information regarding a fugitive criminal wanted in a foreign country. In this connection the following provisions of law are relevant:

- Action can be taken under the Indian Extradition Act Article No. 34 (b) of 1962. This act provides procedure for the arrest and extradition of fugitive criminals under certain conditions which includes receipt of the request through diplomatic channels ONLY and under the warrant issued by a Magistrate having a competent jurisdiction.

- Action can also be taken under the provisions of Section 41 (1) (g) of the Cr.P.C., 1973 which authorizes the police to arrest a fugitive criminal without a warrant. However, they must immediately refer the matter to Interpol Wing for onward transmission to the Government of India for taking a decision on extradition or otherwise.

In case the fugitive criminal is an Indian national, action can also be taken under Section 188 Cr.P.C., 1973 as if the offence has been committed at any place in India at which he may be found. The trial of such a fugitive criminal can only take place with the previous sanction of the Central Government.

MEA Guidelines

Extradition request for an accused/ fugitive can be initiated after chargesheet has been filed before an appropriate Court and said court having taken cognizance of the case has issued orders/directions justifying accused/fugitive's committal for trial on the basis of evidence made available in the charge sheet and has sought presence of the accused/fugitive to face trial in the case. All extradition requests should be supported by documents and information enumerated below. Note: If an extradition treaty exists between India and the requested country, the extradition request and documents connected therewith should be prepared on the basis of provisions of Extradition Treaty.

(1) It should be in spiral bound and contain an index with page numbers.

(2) The request should be supported by a self-contained affidavit executed by the Court by whom the fugitive is wanted or by a Senior Officer in charge of the case (not below the rank of Superintendent of Police of the concerned investigating agency) sworn before a judicial Magistrate (of the court by which the fugitive is wanted for prosecution). The affidavit should contain brief facts and history of the case, referring at the appropriate places the statements of witnesses and other documentary evidences. Criminal's description establishing his identity; provision of the law invoked etc. so that a prima facie case is made out against the fugitive criminal.

(3) Paragraph 1 of the affidavit should indicate the basis/capacity in which the affidavit is executed.

(4) The affidavit should indicate that the offences for which the accused is charged in India.

(5) The affidavit should also indicate that the law in question was in force at the time of Commission of offences and it is still in force, including the penalty provisions.

(6) The evidence made available should be admissible under Indian laws. Accordingly, the affidavit should indicate whether the statements of witness are admissible as evidence in India in a criminal trial/prosecution. Statements of witnesses should be sworn before the Court.

(7) The affidavit should also indicate that if the accused were extradited to India, he would be tried in India only for those offences for which his/her extradition is sought.

(8) Copy of First Information Report (FIR), duly countersigned by the competent judicial authority, should be enclosed with the request.

(9) Competent authority should countersign copy of charge sheet, which is enclosed with the documents.

(10) A letter/order from the concerned court justifying accused person's committal for trial on the basis of evidence made available in the Charge sheet, with a direction seeking accused person's presence in court to stand trial in said court from the country of present stay.

(11) Warrant of arrest should be in original and open dated indicating clearly only those offences for which the accused is charged and Court has taken cognizance with relevant sections thereof.

(12) Nationality, identity and address of the accused including his photograph should be made available with the request.

(13) Copy of the relevant provisions under which the accused is charged along with the provisions of the relevant laws indicating that the maximum sentence prescribed for the offence for which the accused is charged or convicted.

(14) The extradition request is to be made in quadruplet (four copies). All original and copies should be attested /authenticated by the concerned court.

(15) All the documents should be very clear, legible and in presentable form as they are to be presented to the soverign Governments of Foreign Countries.

(16) Original documents in national languages should be sent along with certified English translation of each such document from authorized translators.

(17) Extradition requests/documents to the country where English is not first language should be submitted along with duly translated copy in host country's local language. The Court issuing warrant should certify such translated copy.

After completion of necessary formalities, the request for extradition should contain a letter/note from a Senior Official (not below the rank of Joint Secretary) or the concerned State Government indicating the correctness of the case/material with a request to the Central Executive to forward it to the Government of the concerned foreign country.

N.B.: If the concerned court is requesting for extradition of a person, the request in the form of an affidavit should be in first person, i.e. by the Hon'ble Magistrate/ Judge himself/herself. (Such requests are usually received from Court Masters or other court officials writing in third person on behalf of the Court. Requested States object to it)

NOTE: The request for extradition and the documents thereof should be prepared as per the requirements of the extradition

treaty between India and the country concerned from which the fugitive is to be extradited to India.

76. Confiscation.

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rule, orders or regulations made thereunder 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, 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 thereunder, 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 authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

77. Compensation, penalties or confiscation not to interfere with other punishment.¹³⁸

No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77A. Compounding of offences¹³⁹

A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or

¹³⁸ Substituted by Information Technology (Amendment) Act, 2008 for 77. Penalties or confiscation not to interfere with other punishments. – No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

¹³⁹ Inserted by Information Technology (Amendment) Act, 2008.

imprisonment for a term exceeding three years has been provided, under this Act:

Provided that the court shall not compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind:

Provided further that the court shall not compound any offence where such offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this Act may file an application for compounding in the court in which offence is pending for trial and the provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 shall apply.

COMMENTS:

A *ready-reference guide* of offences under the Information Technology Act and whether they are compoundable or not is provided below:

Offence	Punishment	Compoundable	
Section 65. Tampering with computer source documents	Imprisonment upto 3 years and / or fine upto Rs 2 lakh	Compoundable	
Section 66. Computer related offences	Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Compoundable	
Section 66A. Punishment for sending offensive messages through communication service, etc	Imprisonment upto 3 years and fine	Compoundable	
Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment upto 3 years and / or fine upto Rs 1 lakh	Compoundable	
Section 66C. Punishment for identity theft	Imprisonment of either description upto 3 years and / or fine upto Rs 1 lakh	Compoundable	
Section 66D. Punishment for cheating by personation by using	Imprisonment of either description upto 3 years and / or fine upto Rs 1 lakh	Compoundable	

computer resource			
Section 66E. Punishment for violation of privacy	Imprisonment upto 3 years and / or fine upto Rs 2 lakh	Compoundable	
Section 66F. Punishment for cyber terrorism	Imprisonment extend to imprisonment for life	Not Compoundable	
Section 67. Punishment for publishing or transmitting obscene	On first conviction: Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Compoundable	
material in electronic form	On subsequent conviction: Imprisonment upto 5 years and / or fine upto Rs 10 lakh	Not Compoundable	
Section 67A. Punishment for publishing or transmitting of material containing sexually explicit	On first conviction: Imprisonment of either description upto 5 years and / or fine upto Rs 10 lakh	Not Compoundable	
act, etc., in electronic form	On subsequent conviction: Imprisonment of either description upto 7 years and / or fine upto Rs 10 lakh	Not Compoundable	
Section 67B. Punishment for publishing or transmitting of material depicting children in	On first conviction: Imprisonment of either description upto 5 years and / or fine upto Rs 10 lakh	Not Compoundable	
sexually explicit act, etc., in electronic form	On subsequent conviction: Imprisonment of either description upto 7 years and / or fine upto Rs 10 lakh	Not Compoundable	
Section 67C. Preservation and retention of information by intermediaries	Imprisonment upto 3 years and fine	Compoundable	
Section 68. Power of the Controller to give directions	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Compoundable	
Section 69. Power to issue directions for interception or monitoring or decryption of	Imprisonment upto 7 years and fine	Not Compoundable	

any information through			
any computer resource			
Section 69A.	Imprisonment unto 7 years	Not	
Power to issue directions	Imprisonment upto 7 years and fine	Not Compoundable	
		Compoundable	
for blocking public access of any information through			
any computer resource			
Section 69B.	Imprisonment upto 3 years	Compoundable	
	and fine	Compoundable	
Power to authorise to monitor and collect traffic			
data or information through			
any computer resource for			
cyber security			
Section 70.	Imprisonment of either	Not	
Protected system	description upto 10 years and	Compoundable	
	fine	_	
Section 70B.	Imprisonment upto 1 year and	Compoundable	
Indian Computer	/ or fine upto Rs 1 lakh		
Emergency Response			
Team to serve as national			
agency for incident			
response			
Section 71.	Imprisonment upto 2 years	Compoundable	
Penalty for	and / or fine upto Rs 1 lakh		
misrepresentation			
Section 72.	Imprisonment upto 2 years	Compoundable	
Breach of confidentiality	and / or fine upto Rs 1 lakh		
and privacy			
Section 72A.	Imprisonment upto 3 years	Compoundable	
Punishment for disclosure	and / or fine upto Rs 5 lakh		
of information in breach of			
lawful contract			
Section 73.	Imprisonment upto 2 years	Compoundable	
Penalty for publishing	and / or fine upto Rs 1 lakh		
Electronic Signature			
Certificate false in certain			
particulars			
Section 74.	Imprisonment upto 2 years	Compoundable	
Publication for fraudulent	and / or fine upto Rs 1 lakh		
purpose			

Section 265B of the *Code of Criminal Procedure* is titled "Application for plea bargaining" and states:

(1) A person accused of an offence may file an application for plea bargaining in the Court in which such offence is pending for trial.

(2) The application under sub-section (1) shall contain a brief description of the case relating to which the application is filed including the offence to which the case relates and shall be accompanied by an affidavit sworn by the accused stating therein that he has voluntarily preferred, after understanding the nature and extent of punishment provided under the law for the offence, the plea bargaining in his case and that he has not previously been convicted by a Court in a case in which he had been charged with the same offence.

(3) After receiving the application under sub-section (1), the Court shall issue notice to the Public Prosecutor or the complainant of the case, as the case may be, and to the accused to appear on the date fixed for the case.

(4) When the Public Prosecutor or the complainant of the case, as the case may be, and the accused appear on the date fixed under sub-section (3), the Court shall examine the accused in camera, where the other party in the case shall not be present, to satisfy itself that the accused has filed the application voluntarily and where--

(a) the Court is satisfied that the application has been filed by the accused voluntarily, it shall provide time to the Public Prosecutor or the complainant of the case, as the case may be, and the accused to work out a mutually satisfactory disposition of the case which may include giving to the victim by the accused the compensation and other expenses during the case and thereafter fix the date for further hearing of the case;

(b) the Court finds that the application has been filed involuntarily by the accused or he has previously been convicted by a Court in a case in which he had been charged with the same offence, it shall proceed further in accordance with the provisions of this Code from the stage such application has been filed under sub-section (1).

Section 265C of the *Code of Criminal Procedure* is titled "Guidelines for mutually satisfactory disposition" and states:

In working out a mutually satisfactory disposition under clause (a) of sub-section (4) of section 265B, the Court shall follow the following procedure, namely:

(a) in a case instituted on a police report, the Court shall issue notice to the Public Prosecutor, the police officer who has investigated the case, the accused and the victim of the case to participate in the meeting to work out a satisfactory disposition of the case:

Provided that throughout such process of working out a satisfactory disposition of the case, it shall be the duty of the Court to ensure that the entire process is completed voluntarily by the parties participating in the meeting:

Provided further that the accused may, if he so desires, participate in such meeting with his pleader, if any, engaged in the case;

(b) in a case instituted otherwise than on police report, the Court shall issue notice to the accused and the victim of the case to participate in a meeting to work out a satisfactory disposition of the case:

Provided that it shall be the duty of the Court to ensure, throughout such process of working out a satisfactory disposition of the case, that it is completed voluntarily by the parties participating in the meeting:

Provided further that if the victim of the case or the accused, as the case may be, so desires, he may participate in such meeting with his pleader engaged in the case.

77B. Offences with three years imprisonment to be bailable¹⁴⁰

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

COMMENTS:

A *ready-reference guide* of offences under the Information Technology Act and whether they are cognizable / bailable or not is provided below:

¹⁴⁰ Inserted by Information Technology (Amendment) Act, 2008.

Offence	Punishment	Cognizable / Bailable	
Section 65. Tampering with computer source documents	Imprisonment upto 3 years and / or fine upto Rs 2 lakh	Cognizable Bailable	
Section 66. Computer related offences	Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Cognizable Bailable	
Section 66A. Punishment for sending offensive messages through communication service, etc	Imprisonment upto 3 years and fine	Cognizable Bailable	
Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment upto 3 years and / or fine upto Rs 1 lakh	Cognizable Bailable	
Section 66C. Punishment for identity theft	Imprisonment of either description upto 3 years and / or fine upto Rs 1 lakh	Cognizable Bailable	
Section 66D. Punishment for cheating by personation by using computer resource	Imprisonment of either description upto 3 years and / or fine upto Rs 1 lakh	Cognizable Bailable	
Section 66E. Punishment for violation of privacy	Imprisonment upto 3 years and / or fine upto Rs 2 lakh	Cognizable Bailable	
Section 66F. Punishment for cyber terrorism	Imprisonment extend to imprisonment for life	Cognizable Non-bailable	
Section 67. Punishment for publishing or transmitting obscene	On first conviction: Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Cognizable Bailable	
material in electronic form	On subsequent conviction: Imprisonment upto 5 years and / or fine upto Rs 10 lakh	Cognizable Non-bailable	

Section 67A. Punishment for publishing or transmitting of material containing sexually explicit	On first conviction:CognizableImprisonment of either description upto 5 years and / or fine upto Rs 10 lakhNon-bailable	
act, etc., in electronic form	On subsequent conviction: Imprisonment of either description upto 7 years and / or fine upto Rs 10 lakh	Cognizable Non-bailable
Section 67B. Punishment for publishing or transmitting of material depicting children in	On first conviction: Imprisonment of either description upto 5 years and / or fine upto Rs 10 lakh	Cognizable Non-bailable
sexually explicit act, etc., in electronic form	On subsequent conviction: Imprisonment of either description upto 7 years and / or fine upto Rs 10 lakh	Cognizable Non-bailable
Section 67C. Preservation and retention of information by intermediaries	Imprisonment upto 3 years and fine	Cognizable Bailable
Section 68. Power of the Controller to give directions	Imprisonment upto 2 years and / or fine upto Rs 1 lakh	Non-cognizable Bailable
Section 69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource	Imprisonment upto 7 years and fine	Cognizable Non-bailable
Section 69A. Power to issue directions for blocking public access of any information through any computer resource	Imprisonment upto 7 years and fine	Cognizable Non-bailable
Section 69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security	Imprisonment upto 3 years and fine	Cognizable Bailable

Section 70. Protected system Section 70B. Indian Computer Emergency Response Team to serve as national agency for incident	Imprisonment of either description upto 10 years and fine Imprisonment upto 1 year and / or fine upto Rs 1 lakh	Cognizable Non-bailable Non-cognizable Bailable	
response Section 71. Penalty for misrepresentation Section 72. Breach of confidentiality and privacy Section 72A. Punishment for disclosure	Imprisonment upto 2 years and / or fine upto Rs 1 lakh Imprisonment upto 2 years and / or fine upto Rs 1 lakh Imprisonment upto 3 years and / or fine upto Rs 5 lakh	Non-cognizable Bailable Non-cognizable Bailable Cognizable Bailable	
of information in breach of lawful contract Section 73. Penalty for publishing Electronic Signature Certificate false in certain particulars Section 74.	Imprisonment upto 2 years and / or fine upto Rs 1 lakh Imprisonment upto 2 years	Non-cognizable Bailable Non-cognizable	
Publication for fraudulent purpose	and / or fine upto Rs 1 lakh	Bailable	

Some relevant provisions of the *Code of Criminal Procedure* are quoted below for reference:

Section 436 - In what cases bail to be taken

(1) When any person other than a person accused of a non-bailable offence is arrested or detained without warrant by an officer in charge of a police station, or appears or is brought before a Court, and is prepared at any time while in the custody of such officer or at any stage of the proceeding before such Court to give bail, such person shall be released on bail:

Provided that such officer or Court, if he or it thinks fit, may, and shall, if such person is indigent and is unable to furnish surety, instead of taking bail from such person, discharge him on his executing a bond without sureties for his appearance as hereinafter provided:

Provided further that nothing in this section shall be deemed to affect the provisions of sub-section (3) of section 1161 or section 446A.

Explanation.-- Where a person is unable to give bail within a week of the date of his arrest, it shall be a sufficient ground for the officer or the Court to presume that he is an indigent person for the purposes of this proviso.

(2) Notwithstanding anything contained in sub-section (1), where a person has failed to comply with the conditions of the bail-bond as regards the time and place of attendance, the Court may refuse to release him on bail, when on a subsequent occasion in the same case he appears before the Court or is brought in custody and any such refusal shall be without prejudice to the powers of the Court to call upon any person bound by such bond to pay the penalty thereof under section 446.

Section 436A - Maximum period for which an undertrial prisoner can be detained

Where a person has, during the period of investigation, inquiry or trial under this Code of an offence under any law (not being an offence for which the punishment of death has been specified as one of the punishments under that law) undergone detention for a period extending up to one-half of the maximum period of imprisonment specified for that offence under that law, he shall be released by the Court on his personal bond with or without sureties:

Provided that the Court may, after hearing the Public Prosecutor and for reasons to be recorded by it in writing, order the continued detention of such person for a period longer than one-half of the said period or release him on bail instead of the personal bond with or without sureties:

Provided further that no such person shall in any case be detained during the period of investigation inquiry or trial for more than the maximum period of imprisonment provided for the said offence under that law.

Explanation.--In computing the period of detention under this section for granting bail the period of detention passed due to delay in proceeding caused by the accused shall be excluded.

Section 437 - When bail may be taken in case of non-bailable offence

(1) When any person accused of, or suspected of, the commission of any non-bailable offence is arrested or detained without warrant by an officer in charge of a police station or appears or is brought before a Court other than the High Court or Court of Session, he may be released on bail, but-

(i) such person shall not be so released if there appear reasonable grounds for believing that he has been guilty of an offence punishable with death or imprisonment for life;

(ii) such person shall not be so released if such offence is a cognizable offence and he had been previously convicted of an offence punishable with death, imprisonment for life or imprisonment for seven years or more, or he had been previously convicted on two or more occasions of a cognizable offence punishable with imprisonment for three years or more but not less than seven years:

Provided that the Court may direct that a person referred to in clause (i) or clause (ii) be released on bail if such person is under the age of sixteen years or is a woman or is sick or infirm:

Provided further that the Court may also direct "that a person referred to in clause (ii) be released on bail if it is satisfied that it is just and proper so to do for any other special reason:

Provided also that the mere fact that an accused person may be required for being identified by witnesses during investigation shall not be sufficient ground for refusing to grant bail if he is otherwise entitled to be released on bail and gives an undertaking that the shall comply with such directions as may be given by the Court.

Provided also that no person shall, if the offence alleged to have been committed by him is punishable with death, imprisonment for life, or imprisonment for seven years or more be released on bail by the Court under this sub-section without giving an opportunity of hearing to the Public Prosecutor.

(2) If it appears to such officer or Court at any stage of the investigation, inquiry or trial as the case may be, that there are not reasonable grounds for believing that the accused has committed a non-bailable offence, but that there are sufficient grounds for further inquiry into his guilt, the accused shall, subject to the provisions of section 446A and pending such inquiry, be released

on bail], or, at the discretion of such officer or Court on the execution by him of a bond without sureties for his appearance as hereinafter provided.

(3) When a person accused or suspected of the commission of an offence punishable with imprisonment which may extend to seven years or more or of an offence under Chapter VI, Chapter XVI or Chapter XVII of the Indian Penal Code (45 of 1860) or abetment of, or conspiracy or attempt to commit, any such offence, is released on bail under sub-section (1) the Court shall impose the conditions,--

(a) that such person shall attend in accordance with the conditions of the bond executed under this Chapter,

(b) that such person shall not commit an offence similar to the offence of which he is accused, or suspected, of the commission of which he is suspected, and

(c) that such person shall not directly or indirectly make any inducement, threat or promise to any person acquainted with the facts of the case so as to dissuade him from disclosing such facts to the Court or to any police officer or tamper with the evidence.

and may also impose, in the interests of justice, such other conditions as it considers necessary.]

(4) An officer or a Court releasing any person on bail under subsection (1), or sub-section (2), shall record in writing his or its reasons or special reasons for so doing.

(5) Any Court which has released a person on bail under subsection (1), or sub-section (2), may, if it considers it necessary so to do, direct that such person be arrested and commit him to custody.

(6) If, in any case triable by a Magistrate, the trial of a person accused of any non-bailable offence is not concluded within a period of sixty days from the first date fixed for taking evidence in the case, such person shall, if he is in custody during the whole of the said period, be released on bail to the satisfaction of the Magistrate, unless for reasons to be recorded in writing, the Magistrate otherwise directs.

(7) If, at any time after the conclusion of the trial of a person accused of a non-bailable offence and before judgment is delivered the Court is of opinion that there are reasonable grounds for believing that the accused is not guilty of any such offence, it shall release the accused, if he is in custody, on the execution by him of a bond without sureties for his appearance to hear judgment delivered.

Section 438 - Direction for grant of bail to person apprehending arrest

(1) Where any person has reason to believe that he may be arrested on accusation of having committed a non-bailable offence, he may apply to the High Court or the Court of Session for a direction under this section that in the event of such arrest he shall be released on bail; and that Court may, after taking into consideration, inter alia, the following factors, namely:--

(i) the nature and gravity of the accusation;

(ii) the antecedents of the applicant including the fact as to whether he has previously undergone imprisonment on conviction by a Court in respect of any cognizable offence;

(iii) the possibility of the applicant to flee from justice; and.

(iv) where the accusation has been made with the object of injuring or humiliating the applicant by having him so arrested, either reject the application forthwith or issue an interim order for the grant of anticipatory bail:

Provided that, where the High Court or, as the case may be, the Court of Session, has not passed any interim order under this subsection or has rejected the application for grant of anticipatory bail, it shall be open to an officer in-charge of a police station to arrest, without warrant the applicant on the basis of the accusation apprehended in such application.

(1A) Where the Court grants an interim order under sub-section (1), it shall forthwith cause a notice being not less than seven days notice, together with a copy of such order to be served on the Public Prosecutor and the Superintendent of Police, with a view to give the Public Prosecutor a reasonable opportunity of being heard when the application shall be finally heard by the Court,

(1B) The presence of the applicant seeking anticipatory bail shall be obligatory at the time of final hearing of the application and passing of final order by the Court, if on an application made to it by the Public Prosecutor, the Court considers such presence necessary in the interest of justice.

(2) When the High Court or the Court of Session makes a direction under subsection (1), it may include such conditions in

such directions in the light of the facts of the particular case, as it may thinks fit, including-

(i) a condition that the person shall make himself available for interrogation by a police officer as and when required;

(ii) a condition that the person shall not, directly or indirectly, make any inducement, threat or promise to any person acquainted with the facts of the case so as to dissuade him from disclosing such facts to the Court or to any police officer;

(iii) a condition that the person shall not leave India without the previous permission of the Court;

(iv) such other condition as may be imposed under subsection (3) of section 437, as if the bail were granted under that section.

(3) If such person is thereafter arrested without warrant by an officer in charge of a police station on such accusation, and is prepared either at the time of arrest or at any time while in the custody of such officer to give bail, he shall be released on bail, and if a Magistrate taking cognizance of such offence decides that a warrant should issue in the first instance against that person, he shall issue a bailable warrant in conformity with the direction of the Court under sub-section (1).

Section 439 - Special powers of High Court or Court of Session regarding bail

(1) A High Court or Court of Session may direct-

(a) that any person accused of an offence and in custody be released on bail, and if the offence is of the nature specified in sub-section (3) of section 437, may impose any condition which it considers necessary for the purposes mentioned in that sub-section;

(b) that any condition imposed by a Magistrate when releasing any person on bail be set aside or modified:

Provided that the High Court or the Court of Session shall, before granting bail to a person who is accused of an offence which is triable exclusively by the Court of Session or which, though not so triable, is punishable with imprisonment for life, give notice of the application for bail to the Public Prosecutor unless it is, for reasons to be recorded in writing, of opinion that it is not practicable to give such notice. (2) A High Court or Court of Session may direct that any person who has been released on bail under this Chapter be arrested and commit him to custody.

Section 440 - Amount of bond and reduction thereof

(1) The amount of every bond executed under this chapter shall be fixed with due regard to the circumstances of the case and shall not be excessive.

(2) The High Court or Court of Session may direct that the bail required by a police officer or Magistrate be reduced.

Section 441 - Bond of accused and sureties

(1) Before any person is released on bail or released on his own bond, a bond for such sum of money as the police officer or Court, as the case may be, thinks sufficient shall be executed by such person, and, when he is released on bail, by one or more sufficient sureties conditioned that such person shall attend at the time and place mentioned in the bond, and shall continue so to attend until otherwise directed by the police officer or Court, as the case may be.

(2) Where any condition is imposed for the release of any person on bail, the bond shall also contain that condition.

(3) If the case so requires, the bond shall also bind the person released on bail to appear when called upon at the High Court, Court of Session or other Court to answer the charge.

(4) For the purpose of determining whether the sureties are fit or sufficient, the Court may accept affidavits in proof of the facts contained therein relating to the sufficiency or fitness of the sureties, or, if it considers necessary, may either hold an inquiry itself or cause an inquiry to be made by a Magistrate subordinate to the Court, as to such sufficiency or fitness.

Section 442 - Discharge from custody

(1) As soon as the bond has been executed, the person for whose appearance it has been executed shall be released; and when he is in jail the Court admitting him to bail shall issue an order of release to the officer in charge of the jail, and such officer on receipt of the orders shall release him. (2) Nothing in this section, section 436 or section 437 shall be deemed to require the release of any person liable to be detained for some matter other than that in respect of which the bond was executed.

Section 443 - Power to order sufficient bail when that first taken is insufficient

If, through mistake, fraud, or otherwise, insufficient sureties have been accepted, or if they afterwards become insufficient, the Court may issue a warrant of arrest directing that the person released on bail be brought before it and may order him to find sufficient sureties, and on his failing so to do, may commit him to jail.

78. Power to investigate offence.

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector¹⁴¹ shall investigate any offence under this Act.

COMMENT:

According to section 2(h) of the *Code of Criminal Procedure*, "investigation" includes all the proceedings under this Code for the collection of evidence conducted by a police officer or by any person (other than a Magistrate) who is authorised by a Magistrate in this regard.

Section 28 of the *Information Technology Act* empowers the following to investigate any contravention of the Act and allied rules and regulations: (1) the Controller (2) any officer authorised by the Controller.

Additionally, section 78 of the *Information Technology Act* empowers a police officer not below the rank of Inspector to investigate offence under the Act. Offences are defined under Chapter XI of the Act.

Additionally, rule 4(i) of the *Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003* authorizes the Adjudicating Officer to get a matter or report investigated from an officer in the Office of Controller or CERT-IND or from the concerned Deputy Superintendent of Police [Inspector], to ascertain more facts and whether prima facie there is a case for adjudicating on the matter or not.

¹⁴¹ The word "Inspector" substituted for the words "Deputy Superintendent of Police by Information Technology (Amendment) Act, 2008.

Additionally, section 80 of the *Information Technology Act* provides a special power to police officers not below the rank of a Inspector of Police and to other Government officers authorised by the Central Government. Such authorised persons can enter and search any public place. Public places include cyber cafes, hotels, shops etc accessible to the public.

Additionally, they can arrest without warrant any person found in such a public place who is reasonably suspected of:

(1) having committed an offence under the Act,

(2) committing an offence under the Act,

(3) being about to commit any offence under the Act.

The steps most commonly followed in the investigation and trial of a criminal case are outlined as under (Note: CrPC stands for *Code of Criminal Procedure, 1973*):

1. The complainant approaches the local police station to file a complaint.

2. The police listen to the facts disclosed by the complainant. If the facts disclose a non-cognizable offence then the police make an entry in a special register for non-cognizable complaints. This register is regularly submitted to the local magistrate. A non-cognizable case is one in which the police cannot arrest a person without a warrant.

3. If the facts disclose a cognizable offence then an FIR (First Information Report) is lodged. The FIR is numbered, dated and a copy is given to the complainant. A copy is also submitted to the local Court. A cognizable case is one in which the police can arrest a person without a warrant e.g. cyber terrorism is punishable with life imprisonment and is a cognizable offence.

4. The police then begin the investigation. They may visit the scene of the crime, question witnesses and suspects etc.

5. A person being questioned by the police is legally bound to give true answers. Exception: A person is not legally bound to answer a question if the answer can incriminate him. This exception is provided by section 161 of CrPC. The right against self incrimination is vested by the Constitution of India.

6. The police can write down the statements made by the witnesses, suspects etc. The person making the statement is not required to sign it. Note: A person can voluntarily make a statement or confession to a Court.

7. The police cannot threaten a person into making any statement.

8. The police can search any house, office etc and seize evidence. They do not need a search warrant for this.

9. If some evidence is to be collected from abroad, the Court can make an order which is then forwarded by the Central Government to the suitable authority in the relevant countries.

10. The police can arrest and confine a suspect. The freedom of an arrested person is restricted by the police. The police are empowered to use force if a person attempts to evade arrest. An arrested person must be informed about the grounds for his arrest.

11. The police can search the arrested person and recover evidence.

12. The arrested person must be produced before a Court within 24 hours of his arrest. The Court can then do one of the following:

(a) release the arrested person on bail,

(b) send the arrested person into the custody of the police so that the police can carry out their investigation (police custody),

(c) send the arrested person to jail (judicial / magisterial custody).

It is a common misconception that Courts are closed on weekends and public holidays and a person will have to wait till a Monday to be produced before a Court. There is always at least one criminal court functioning on every holiday and weekend.

13. After completing the investigation, the police are required to submit their report and relevant documents to the Court.

14. After studying the investigation report, the Court can dismiss the complaint if there are insufficient grounds against the accused persons.

15. If there are sufficient grounds to proceed against the accused, the Court can take cognizance of the case and frame charges against the accused.

16. If the accused person pleads guilty to the charges then the court can convict him under the relevant law and impose sufficient imprisonment term and / or fine.

17. If the accused person does not plead guilty to the charges, the trial takes place. The prosecution and the defence argue the case, examine witnesses and place evidence before the court.

18. If scientific reports are provided as evidence, then the Court can call the scientific expert to Court to examine him e.g. the director, deputy director or assistant director of a Central or State Cyber Forensic Laboratory is usually summoned to court in cases involving cyber crime and digital evidence. 19. After hearing the arguments, the Court gives the judgment. If the accused is found guilty then the court can convict him under the relevant law and impose sufficient imprisonment term and / or fine. The convicted person can appeal to a higher court against this judgment.

20. If the accused is found not guilty, then the court can acquit him. The Court can also order the complainant to pay compensation if the case appears to be frivolous.

21. Once a person has been tried by a Court, he cannot be prosecuted again for the same offence or for another offence based on the same facts. It does not matter whether the person was convicted or acquitted.

Cyber Crime Investigation

Cyber Crime Investigation is the collecting, analyzing and investigation of digital evidence and cyber trails.

This digital evidence and cyber trail may be found in computer hard disks, cell phones, CDs, DVDs, floppies, computer networks, the Internet etc.

Digital evidence and cyber trails can be hidden in pictures (steganography), encrypted files, password protected files, deleted files, formatted hard disks, deleted emails, chat transcripts etc.

Given below are some of the cases that cyber crime investigators are called in to solve. All these cases involve recovery and analysis of digital evidence and cyber trails (1) Divorce cases (2) Murder cases (3) Organized crime, Terrorist operations, Extortion (4) Defamation, Pornography (5) Online banking / share trading / credit card fraud (6) Smuggling, Tax evasion, Money laundering (7) Virus attacks, Cyber sabotage, Source code theft (8) Phishing attacks, Email hijacking, Denial of service (9) Counterfeit currency, stamp papers, postage stamps etc

The actual process of the investigation of any computer related crime begins with an external examination of the premises. Normally, for this part of the investigation, the rules and regulations of investigation and forensics related to traditional crimes also apply to some extent.

This part of the investigation basically assists the computer forensics expert in adjudging the strengths and vulnerabilities of the network. It also helps him in deciding the steps to be taken to investigate the crime and also the peculiarities of the incident.

A cyber crime investigator also has to decide whether it is prudent to confiscate computer resources from the suspect's premises or to complete the investigation at the scene. Confiscating and carrying out the investigation off-site would involve proper packaging and transporting of the computers and accessories, reassembling them at the laboratory and then recreating the network or configuration.

This can be a complex and sensitive issue and hence the cyber crime investigator must decide based on the volume of evidence, technical and infrastructural issues and time available.

Cyber Forensics is a wide term that encompasses computer forensics (gathering evidence from computer media seized at the crime scene) and network forensics (gathering digital evidence that is distributed across networks).

Digital evidence is the foundation of any case involving computers. Searching, examining, collecting, and preserving digital evidence has to be done in such a manner that the court can rely upon the evidence to deliver its judgment. Any errors in gathering, developing, or presenting digital evidence can adversely affect the trial.

As per the definition provided by the Computer Emergency Response Team of the Asian School of Cyber Laws (ASCL-CERT):

Cyber Forensics is the discovery, analysis, and reconstruction of evidence extracted from and / or contained in a computer, computer system, computer network, computer media or computer peripheral.

Discovery implies recovery of something previously unknown or unrecognized. Analysis is the detailed examination of something made in order to understand its nature or determine its essential characteristics. Reconstruct means to construct again, to rebuild, and to form again or anew. Evidence refers to all documents including electronic records produced for the inspection of the Court. Extract means to take out or derive.

Broadly speaking, Cyber Forensics involves: (1) finding and decrypting password protected information, encrypted information and steganography content (2) tracing the source of e-mail (3) tracking software piracy (4) recovering deleted data (5) matching information to computers that created them (6) remotely monitoring computers and (7) preserving digital evidence for presentation in court.

Some of the basic techniques that are used for cyber crime investigation are: (1) whois search (2) IP tracing from ISP (3) analyzing a web server log (4) analyzing email headers (5) tracking an email account (6) recovering deleted evidence (7) cracking passwords (8) handling encrypted information (9) handling steganographic information (10) handling hidden data (11) using keyloggers for investigation.

CHAPTER XII - INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES¹⁴²

79. Exemption from liability of intermediary in certain cases.

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of subsections (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; or

(b) the intermediary does not -

(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.

¹⁴² Substituted by Information Technology (Amendment) Act, 2008 for "NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES - 79. Network service providers not to be liable in certain cases. – For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence for contravention. Explanation.- For the purposes of this section,- (a) "network service provider" means an intermediary; (b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;

(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 purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

COMMENTS:

As per section 2(1)(w) of the Information Technology Act, the term "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.

The term 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.

Intermediaries are not liable for any third party information, data, or communication-link made available or hosted by them. "Third party information" means any information dealt with by an intermediary in his capacity as an intermediary. This exemption is provided to them subject to the condition that:

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

(2) the intermediary does not – initiate the transmission, (ii) select the receiver of the transmission, or select or modify the information contained in the transmission;

(3) the intermediary observes due diligence while discharging his duties under this Act and also observes guidelines prescribed by the Central Government. This exemption is not applicable if:

(1) the intermediary has conspired or abetted or aided or induced in the commission of the unlawful act; or

(2) the intermediary fails to expeditiously remove or disable access to that material (without vitiating the evidence in any manner) upon being informed about the unlawful act.

Illustration: Sameer creates an obscene profile using the free social networking website provided by Google. As long as Google is unaware about this, it is not liable.

If Google is informed about this profile (by a user, the police etc), and it does not remove access to the profile, then it will be liable.

If Google sends out promotional emails that contain obscene matter then it will be liable as that is not third party information

Section 67C of the *Information Technology Act* is also relevant. Under this section, intermediaries are required to: (1) preserve and retain information specified by the Central Government (2) for the time period specified by the Central Government.

Illustration: The Central Government specifies that all search engines must keep a record of the IP addresses of users searching for certain key words e.g. "rdx". The Government also specifies that the date and time of the search by the user must be recorded and stored for 3 years.

Noodle search engine stores only the IP address of the user and not the date and time when the user made the search. The Noodle management would be liable under this section.

Several liabilities have been imposed on intermediaries under the *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.*

Additionally, several liabilities have been imposed on intermediaries under the *Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.*

Additionally, several liabilities have been imposed on intermediaries under the *Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.*

In respect of Internet Service Providers (ISP) in India, their liabilities are also determined by the License for Internet Services based on guidelines dated 24th August, 2007.

According to clause 33 of this license:

(1) ISPs must prevent unlawful content, messages or communications from being carried on their network. This includes objectionable, obscene, unauthorized and other content.

(2) Once specific instances of such content are reported to the ISP by the enforcement agencies, they must immediately prevent the carriage of such material on their network.

(3) ISPs must ensure that content carried by them does not infringe "international and domestic cyber laws".

(4) The use of ISP networks for anti-national activities would be construed as an offence punishable under the Indian Penal Code or other laws.

(5) ISPs are required to comply with the IT Act provisions. They are responsible for any damages arising out of default in this compliance.

(6) ISPs must ensure that their networks cannot be used to endanger or make vulnerable a networked infrastructure.

(7) ISPs must ensure that their services are not used to break-in or attempt to break-in to Indian networks.

(8) ISPs must provide, without any delay, all the tracing facilities to trace nuisance, obnoxious or malicious calls, messages or communications transported through their equipment and network. These tracing facilities are to be provided to authorized officers of Government of India including Police, Customs, Excise, Intelligence Department officers etc.

(9) ISPs must provide necessary facilities to the Government to counteract espionage, subversive acts, sabotage or any other unlawful activity.

According to clause 34 of this license:

(1) Government can monitor telecommunication traffic in the ISP network. The ISP has to pay for the necessary hardware and software for this monitoring.

(2) ISPs must maintain a log of all users connected and the service they are using (mail, telnet, http etc.).

(3) ISPs must also log every outward login or telnet through their computers. These logs, as well as copies of all the packets originating from the Customer Premises Equipment of the ISP, must be available in real time to the Telecom Authority.

Logs are computer based records of activities e.g. a log of a web server may contain details of the users who visited the website, their IP addresses, the Internet browsers used by them etc. Data travels on the Internet in the form of packets. Each packet carries information that will help it get to its destination. This information includes: (a) the sender's IP address, (b) the intended receiver's IP address, (c) how many packets this e-mail message has been broken into (d) identification number of the particular packet.

Customer Premises Equipment (CPE) is the equipment and inside wiring located at a subscriber's premises and connected with the ISPs channels. E.g. Pooja has signed up for Noodle's Internet services. Noodle has placed a telephone, a modem and some wiring at Pooja's house. This equipment is for use with Noodle's services and is CPE.

Real time means instantaneous. In the current context it means that the packets and logs must be made available at the very instant that they are generated or transmitted.

(4) ISPs must ensure privacy of communication on their network.

(5) ISPs must ensure that unauthorized interception of messages does not take place on their networks.

(6) The Government can take over the service, equipment and networks of ISPs in case of emergency, war etc.

(7) The complete and updated list of the ISP's subscribers must be available in a password protected portion of the ISP's website. This is for the use of authorized Intelligence Agencies.

(8) In case of dedicated line customers, the ISP must maintain logs in the following format:

Customer	IP	Bandwidth	Address of	Date of	Contact
name	Address allotted	provided	Installation	Installation / Commissioning	person with Phone / email

(9) The Chief Officer-In-Charge of technical network operations and the Chief Security Officer of the ISP should be a resident Indian citizen.

(10) ISP must ensure that the information transacted by the subscribers is secure and protected.

(11) The ISP officials dealing with the lawful interception of messages must be resident Indian citizens.

(12) The majority Directors on the Board of the ISP must be Indian citizens.

(13) Ministry of Home Affairs will regularly do security vetting in case foreigners are holding the positions of the Chairman, Managing Director, Chief Executive Officer (CEO) and/or Chief Financial Officer (CFO) of the ISP.

(14) ISPs are required to physically monitor, on a monthly basis, those customers who have a high UDP traffic value.

UDP (user datagram protocol) is generally used for transmitting voice, streaming video, IP TV, voice over IP and online games.

CHAPTER XIIA - EXAMINER OF ELECTRONIC EVIDENCE¹⁴³

79A. Central Government to notify Examiner of Electronic Evidence.

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation – For the purposes of this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.

CHAPTER XIII - MISCELLANEOUS

80. Power of police officer and other officers to enter, search, etc.

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 any police officer, not below the

¹⁴³ Inserted by Information Technology (Amendment) Act, 2008.

rank of a Inspector¹⁴⁴, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Explanation.- For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 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.

COMMENTS:

The provisions of Chapter 5 of the *Code of Criminal Procedure* are relevant for arrest of persons. Some of the sections are:

Section 45 - Protection of members of the Armed Forces from arrest

(1) Notwithstanding anything contained in sections 41 to 44 (both inclusive), no member of the Armed Forces of the Union shall be arrested for anything done or purported to be done by him in the discharge of his official duties except after obtaining the consent of the Central Government.

Section 46 - Arrest how made

(1) In making an arrest the police officer or other person making the same shall actually touch or confine the body of the person to

¹⁴⁴ The word "Inspector" substituted for the words "Deputy Superintendent of Police by Information Technology (Amendment) Act, 2008.

be arrested, unless there be a submission to the custody by word or action.

(2) If such person forcibly resists the endeavour to arrest him, or attempts to evade the arrest, such police officer or other person may use all means necessary to effect the arrest.

(3) Nothing in this section gives a right to cause the death of a person who is not accused of an offence punishable with death or with imprisonment for life.

(4) Save in exceptional circumstances, no women shall be arrested after sunset and before sunrise, and where such exceptional circumstances exist, the woman police officer shall, by making a written report, obtain the prior permission of the Judicial Magistrate of the first class within whose local jurisdiction the offence is committed or the arrest is to be made.

Section 47 - Search of place entered by person sought to be arrested

(1) If any person acting under a warrant of arrest, or any police officer having authority to arrest, has reason to believe that the person to be arrested has entered into, or is within, any place, any person residing in, or being in charge of, such place shall, on demand of such person acting as aforesaid or such police officer, allow him such free ingress thereto, and afford all reasonable facilities for a search therein.

(2) If ingress to such place cannot be obtained under sub-section (1), it shall be lawful in any case for a person acting under a warrant and in any case in which a warrant may issue, but cannot be obtained without affording the person to be arrested an opportunity of escape, for a police officer to enter such place and search therein, and in order to effect an entrance into such place, to break open any outer or inner door or window of any house or place, whether that of the person to be arrested or of any other person, if after notification of his authority and purposes, and demand of admittance duly made, he cannot otherwise obtain admittance:

Provided that, if any such place is an apartment in the actual occupancy of a female (not being the person to be arrested) who, according to custom, does not appear in public, such person or police officer shall, before entering such apartment, give notice to such female that she is at liberty to withdraw and shall afford her every reasonable facility for withdrawing, and may then break open the apartment and enter it.

(3) Any police officer or other person authorised to make an arrest may break open any outer or inner door or window of any house or place in order to liberate himself or any other person who, having lawfully entered for the purpose of making an arrest, is detained therein.

Section 49 - No unnecessary restraint

The person arrested shall not be subjected to more restraint than is necessary to prevent his escape.

Section 50 - Person arrested to be informed of grounds of arrest and of right to bail

(1) Every police officer or other person arresting any person without warrant shall forthwith communicate to him full particulars of the offence for which he is arrested or other grounds for such arrest.

(2) Where a police officer arrests without warrant any person other than a person accused of a non-bailable offence, he shall inform the person arrested that he is entitled to be released on bail and that he may arrange for sureties on his behalf.

Section 51 - Search of arrested persons

(1) Whenever a person is arrested by a police officer under a warrant which does not provide for the taking of bail, or under a warrant which provides for the taking of bail but the person arrested cannot furnish bail, and whenever a person is arrested without warrant, or by a private person under a warrant, and cannot legally be admitted to bail, or is unable to furnish bail.

The officer making the arrests or, when the arrest is made by a private person, the police officer to whom he makes over the person arrested, may search such person, and place in safe custody all articles, other than necessary wearing-apparel, found upon him and where any article is seized from the arrested person, a receipt showing the articles taken in possession by the police officer shall be given to such person. (2) Whenever it is necessary to cause a female to be searched, the search shall be made by another female with strict regard to decency.

Section 52 - Power to seize offensive weapons

The officer or other person making any arrest under this Code may taken from the person arrested any offensive weapons which he has about his person, and shall deliver all weapons so taken to the Court or officer before which or whom the officer or person making the arrest is required by this Code to produce the person arrested.

Section 53 - Examination of accused by medical practitioner at the request of police officer

(1) When a person is arrested on a charge of committing an offence of such a nature and alleged to have been committed under such circumstances that there are reasonable grounds for believing that an examination of his person will afford evidence as to the commission of an offence, it shall be lawful for a registered medical practitioner, acting at the request of a police officer not below the rank of sub-inspector, and for any person acting in good faith in his aid and under his direction, to make such an examination of the person arrested as is reasonable necessary in order to ascertain the facts which may afford such evidence, and to use such force as is reasonably necessary for that purpose.

(2) Whenever the person of a female is to be examined under this section, the examination shall be made only by, or under the supervision of, a female registered medical practitioner.

Explanation.-

In this section and in sections 53A and 54,--

(a) "examination" shall include the examination of blood, blood stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples and finger nail clippings by the use of modern and scientific techniques including DNA profiling and such other tests which the registered medical practitioner thinks necessary in a particular case;

(b) "registered medical practitioner" means a medical practitioner who possess any medical qualification as defined in clause (h) of section 2 of the Indian Medical Council Act, 1956(102 of 1956) and whose name has been entered in a State Medical Register.]

Section 54 - Examination of arrested person by medical officer

(1) When a person who is arrested, whether on a charge or otherwise, alleges, at the time when he is produced before a Magistrate or at any time during the period of his detention in custody that the examination of his body will afford evidence which will disprove the commission by him of any offence or which will establish the commission by any other person of any offence against his body, the Magistrate shall, if requested by the arrested person so to do direct the examination of the body of such person by a registered medical practitioner unless the Magistrate considers that the request is made for the purpose of vexation or delay or for defeating the ends of justice.

Where an examination is made under sub-section (1), a copy of the report of such examination shall be furnished by the registered medical practitioner to the arrested person or the person nominated by such arrested person.

(2) The medical officer or a registered medical practitioner so examining the arrested person shall prepare the record of such examination, mentioning therein any injuries or marks of violence upon the person arrested, and the approximate time when such injuries or marks may have been inflicted.

(3) Where an examination is made under sub-section (1), a copy of the report of such examination shall be furnished by the medical officer or registered medical practitioner, as the case may be, to the arrested person or the person nominated by such arrested person.

Section 54A - Identification of person arrested

Where a person is arrested on a charge of committing an offence and his identification by any other person or persons is considered necessary for the purpose of investigation of such offence, the Court, having jurisdiction, may on the request of the officer in charge of a police station, direct the person so arrested to subject himself to identification by any person or persons in such manner as the Court may deem fit.

Section 56 - Person arrested to be taken before Magistrate or officer in charge of police station

A police officer making an arrest without warrant shall, without unnecessary delay and subject to the provisions herein contained as to bail, take or send the person arrested before a Magistrate having jurisdiction in the case, or before the officer in charge of a police station.

Section 57 - Person arrested not to be detained more than twentyfour hours

No police officer shall detain in custody a person arrested without warrant for a longer period than under all the circumstances of the case is reasonable, and such period shall not, in the absence of a special order of a Magistrate under section 167, exceed twentyfour hours exclusive of the time necessary for the journey from the place of arrest to the Magistrate's Court.

Section 58 - Police to report apprehensions

Officers in charge of police stations shall report to the District Magistrate, or, if he so directs, to the Sub-divisional Magistrate, the cases of all persons arrested without warrant, within the limits of their respective stations, whether such persons have been admitted to bail or otherwise.

Section 59 - Discharge of person apprehended

No person who has been arrested by a police officer shall be discharged except on his own bond, or on bail, or under the special order of a Magistrate.

Section 60 - Powers, on escape, to pursue and re-take

(1) If a person in lawful custody escapes or is rescued, the person from whose custody he escaped or was rescued may immediately pursue and arrest him in any place in India.

(2) The provisions of section 47 shall apply to arrests under subsection (1) although the person making any such arrest is not acting under a warrant and is not a police officer having authority to arrest.

Section 94 - Search of place suspected to contain stolen property, forged documents, etc

(1) If a District Magistrate, Sub-divisional Magistrate or Magistrate of the first class, upon information and after such inquiry as he thinks necessary, has reason to believe that any place is used for the deposit or sale of stolen property, or for the deposit, sale or production of any objectionable article to which this section applies, or that any such objectionable article is deposited in any place, he may by warrant authorise any police officer above the rank of a constable--

(a) to enter, with such assistance as may be required, such place,

(b) to search the same in the manner specified in the warrant,

(c) to take possession of any property or article therein found which he reasonably suspects to be stolen property or objectionable article to which this section applies,

(d) to convey such property or article before a Magistrate, or to guard the same on the spot until the offender is taken before a Magistrate, or otherwise to dispose of it in some place of safety,

(e) to take into custody and carry before a Magistrate every person found in such place who appears to have been privy to the deposit, sale or production of any such property or article knowing or having reasonable cause to suspect it to be stolen property or, as the case may be, objectionable article to which this section applies.

(2) The objectionable articles to which this section applies are—

(a) counterfeit coin;

(b) pieces of metal made in contravention of the Metal Tokens Act, 1889 (1 of 1889), or brought into India in contravention of any notification for the time being in force under section 11 of the Customs Act, 1962 (52 of 1962);

(c) counterfeit currency note; counterfeit stamps;

(d) forged documents;

(e) false seals;

(f) obscene objects referred to in section 292 of the Indian Penal Code (45 of 1860);

(g) instruments or materials used for the production of any of the articles mentioned in clauses (a) to (f).

81. Act to have overriding effect

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 or the Patents Act, 1970.¹⁴⁵

82. Chairperson, Members, officers and employees to be public servants

The Chairperson, Members and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code.

COMMENTS:

Section 21 of the Indian Penal Code is titled "Public Servant" and states:

The words "public servant" denote a person falling under any of the descriptions hereinafter following; namely:-

Second.-- Every Commissioned Officer in the Military, Naval or Air Forces of India;

Third.--Every Judge including any person empowered by law to discharge, whether by himself or as a member of any body of persons, any adjudicatory functions;

Fourth.-- Every officer of a Court of Justice (including a liquidator, receiver or commissioner) whose duty it is, as such officer, to investigate or report on any matter of law or fact, or to make, authenticate, or keep any document, or to take charge or dispose of any property, or to execute any judicial process, or to administer any oath, or to interpret, or to preserve order in the Court, and every person specially authorized by a Court of Justice to perform any of such duties;

Fifth.-- Every juryman, assessor, or member of a panchayat assisting a Court of Justice or public servant;

¹⁴⁵ Inserted by Information Technology (Amendment) Act, 2008.

Sixth.-- Every arbitrator or other person to whom any cause or matter has been referred for decision or report by any Court of Justice, or by any other competent public authority;

Seventh.-- Every person who holds any office by virtue of which he is empowered to place or keep any person in confinement;

Eighth.-- Every officer of the Government whose duty it is, as such officer, to prevent offences, to give information of offences, to bring offenders to justice, or to protect the public health, safety or convenience;

Ninth.-- Every officer whose duty it is, as such officer, to take, receive, keep or expend any property on behalf of the Government, or to make any survey, assessment or contract on behalf of the Government, or to execute any revenue process, or to investigate, or to report, on any matter affecting the pecuniary interests of the Government, or to make, authenticate or keep any document relating to the pecuniary interests of the Government, or to prevent the infraction of any law for the protection of the pecuniary interests of the Government;

Tenth.-- Every officer whose duty it is, as such officer, to take, receive, keep or expend any property, to make any survey or assessment or to levy any rate or tax for any secular common purpose of any village, town or district, or to make, authenticate or keep any document for the ascertaining of the rights of the people of any village, town or district;

Eleventh.--Every person who holds any office in virtue of which he is empowered to prepare, publish, maintain or revise an electoral roll or to conduct an election or part of an election;

Twelfth .-- Every person--

(a) in the service or pay of the Government or remunerated by fees or commission for the performance of any public duty by the Government;

(b) in the service or pay of a local authority, a corporation established by or under a Central, Provincial or State Act or a Government company as defined in section 617 of the Companies Act, 1956 (1 of 1956).

Illustration

A Municipal Commissioner is a public servant.

Explanation 1.--Persons falling under any of the above descriptions are public servants, whether appointed by the Government or not.

Explanation 2.--Wherever the words "public servant" occur, they shall be understood of every person who is in actual possession of the situation of a public servant, whatever legal defect there may be in his right to hold that situation.

Explanation 3.--The word "election" denotes an election for the purpose of selecting members of any legislative, municipal or other public authority, of whatever character, the method of selection to which is by, or under, any law prescribed as by election.

83. Power to give directions.

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

84. Protection of action taken in good faith.

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Chairperson, Members, adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.

84A. Modes or methods for encryption.¹⁴⁶

The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.

¹⁴⁶ Inserted by Information Technology (Amendment) Act, 2008.

84B. Punishment for abetment of offences.¹⁴⁷

Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation.- An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

84C. Punishment for attempt to commit offences.¹⁴⁸

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.

85. Offences by companies.

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

¹⁴⁷ Inserted by Information Technology (Amendment) Act, 2008.

¹⁴⁸ Inserted by Information Technology (Amendment) Act, 2008.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.- For the purposes of this section,-

(i) "company" means and body corporate and includes a firm or other association of individuals; and

(ii) "directors", in relation to a firm, means a partner in the firm.

86. Removal of difficulties.

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty;

Provide that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

87. Power of Central Government to make rules.

(1) The Central Government may, by notification in the Official Gazette and in the Electronic Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:-

(a) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (2) of section 3A;¹⁴⁹

(aa) the procedure for ascertaining electronic signature or authentication under sub-section (3) of section 3A; $^{\rm 150}$

(ab) the manner in which any information or matter may be authenticated by means of electronic signature under section 5; ¹⁵¹

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

(c) the manner and format in which electronic records shall be filed, or issued and the method of payment under sub-section (2) of section 6;

(ca) the manner in which the authorised service provider may collect, retain and appropriate service charges under sub-section (2) of section 6A; ¹⁵²

(d) the matters relating to the type of electronic signature 153 , manner and format in which it may be affixed under section 10;

¹⁴⁹ Substituted by Information Technology (Amendment) Act, 2008 for (a) the manner in which any information or matter may be authenticated by means of digital signature under section 5;

¹⁵⁰ Inserted by Information Technology (Amendment) Act, 2008.

¹⁵¹ Inserted by Information Technology (Amendment) Act, 2008.

¹⁵² Inserted by Information Technology (Amendment) Act, 2008.

¹⁵³ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

COMMENTS:

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009.

(e) the manner of storing and affixing electronic signature creation data under section 15;¹⁵⁴

COMMENTS:

Information Technology (Security Procedure) Rules, 2004 contain the relevant provisions.

(ea) the security procedures and practices under section 16; $^{\rm 155}$

(f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers, Assistant Controllers, other officers and employees¹⁵⁶ under section 17;

(g) omitted by Information Technology (Amendment) Act, 2008¹⁵⁷

(h) the requirements which an applicant must fulfill under sub-section (2) of section 21;

¹⁵⁷ (g) other standards to be observed by the Controller under clause (b) of subsection (2) of section 20;

¹⁵⁴ Substituted by Information Technology (Amendment) Act, 2008 for (e) the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16;

¹⁵⁵ Inserted by Information Technology (Amendment) Act, 2008.

¹⁵⁶ The words ", Assistant Controllers, other officers and employees" substituted for "and Assistant Controllers" by Information Technology (Amendment) Act, 2008.

COMMENTS:

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009. Also relevant are the Guidelines for submission of application for license to operate as a Certifying Authority under the Information Technology Act, 2000.

> (i) the period of validity of licence granted under clause (a) of sub-section (3) of section 21;

COMMENTS:

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009.

(j) the form in which an application for licence may be made under sub-section (1) of Section 22;

COMMENTS:

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009.

(k) the amount of fees payable under clause (c) of subsection (2) of section 22;

COMMENTS:

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and

Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009.

(I) such other documents which shall accompany an application for licence under clause (d) of sub-section (2) of section 22;

COMMENTS:

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009.

Also relevant are the *Guidelines for submission of application for license* to operate as a Certifying Authority under the Information Technology Act, 2000.

(m) the form and the fee for renewal of a licence and the fee payable thereof under section 23;

COMMENTS:

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009.

(ma) the form of application and fee for issue of Electronic Signature Certificate under section 35;¹⁵⁸

COMMENTS:

¹⁵⁸ Inserted by Information Technology (Amendment) Act, 2008.

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009.

(n) the form in which application for issue of a Electronic Signature¹⁵⁹ Certificate may be made under sub-section (1) of section35;

COMMENTS:

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009.

(o) the fee to be paid to the Certifying Authority for issue of a Electronic Signature¹⁶⁰ Certificate under sub-section (2) of section 35;

COMMENTS:

The Information Technology (Certifying Authorities) Rules, 2000 contain the relevant provisions. These rules have been amended by Information Technology (Certifying Authorities) (Amendment) Rules, 2003 and Information Technology (Certifying Authorities) (Amendment) Rules, 2005 and Information Technology (Certifying Authorities) (Amendment) Rules, 2009.

(oa) the duties of subscribers under section 40A; ¹⁶¹

¹⁵⁹ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

¹⁶⁰ The words "electronic signature" substituted for "digital signature" by Information Technology (Amendment) Act, 2008.

¹⁶¹ Inserted by Information Technology (Amendment) Act, 2008.

(ob) the reasonable security practices and procedures and sensitive personal data or information under section 43A; $^{\rm 162}$

(p) the manner in which the adjudicating officer shall hold inquiry under sub-section (1) of section 46;

COMMENTS:

Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 contain the relevant provisions.

(q) the qualification and experience which the adjudicating officer shall possess under sub-section (3) of section 46;

COMMENTS:

Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 contain the relevant provisions.

(r) the salary, allowances and the other terms and conditions of service of the Chairperson and Members¹⁶³ under section 52;

COMMENTS:

Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009 contain the relevant provisions. These rules are in suppression of *Cyber*

¹⁶² Inserted by Information Technology (Amendment) Act, 2008.

¹⁶³ The words "Chairperson and Members" substituted for "Presiding Officer" by Information Technology (Amendment) Act, 2008.

Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003.

(s) the procedure for investigation of misbehaviour or incapacity of the Chairperson and Members¹⁶⁴ under sub-section (3) of section 54;

COMMENTS:

Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009 contain the relevant provisions.

(t) the salary and allowances and other conditions of service of other officers and employees under subsection (3) of section 56;

(u) the form in which appeal may be filed and the fee thereof under sub-section (3) of section 57;

COMMENTS:

Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 contain the relevant provisions.

(v) any other power of a civil court required to be prescribed under clause (g) of sub-section (2) of section 58; and

COMMENTS:

Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 contain the relevant provisions.

(w) the powers and functions of the Chairperson of the Cyber Appellate Tribunal under section 52A;¹⁶⁵

¹⁶⁴ The words "Chairperson and Members" substituted for "Presiding Officer" by Information Technology (Amendment) Act, 2008.

¹⁶⁵ Substituted by Information Technology (Amendment) Act, 2008 for "(w) any other matter which is required to be, or may be, prescribed."

COMMENTS:

Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 contain the relevant provisions.

(x) the information, duration, manner and form of such information to be retained and preserved under section 67C; $^{\rm 166}$

(y) the procedures and safeguards for interception, monitoring, or decryption under sub-section (2) of section 69; $^{\rm 167}$

COMMENTS:

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 contain the relevant provisions.

(z) the procedure and safeguard for blocking for access by the public under sub-section (2) of section 69A; $^{\rm 168}$

COMMENTS:

Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 contain the relevant provisions.

(za) the procedure and safeguards for monitoring and collecting traffic data or information under sub-section (3) of section 69B; 169

¹⁶⁶ Inserted by Information Technology (Amendment) Act, 2008.

¹⁶⁷ Inserted by Information Technology (Amendment) Act, 2008.

¹⁶⁸ Inserted by Information Technology (Amendment) Act, 2008.

¹⁶⁹ Inserted by Information Technology (Amendment) Act, 2008.375

COMMENTS:

Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 contain the relevant provisions.

(zb) the information security practices and procedures for protected system under section 70; ¹⁷⁰

(zc) manner of performing functions and duties of the agency under sub-section (3) of section 70A; ¹⁷¹

(zd) the officers and employees under sub-section (2) of section 70B; $^{\rm 172}$

(ze) salaries and allowances and terms and conditions of service of the Director General and other officers and employees under sub-section (3) of section 70B; ¹⁷³

(zf) the manner in which the functions and duties of agency shall be performed under sub-section (5) of section 70B; $^{\rm 174}$

(zg) the guidelines to be observed by the intermediaries under sub-section (2) of section 79; 175

(zh) the modes or methods for encryption under section 84A; $^{\rm 176}$

¹⁷² Inserted by Information Technology (Amendment) Act, 2008.

¹⁷⁰ Inserted by Information Technology (Amendment) Act, 2008.

¹⁷¹ Inserted by Information Technology (Amendment) Act, 2008.

¹⁷³ Inserted by Information Technology (Amendment) Act, 2008.

¹⁷⁴ Inserted by Information Technology (Amendment) Act, 2008.

¹⁷⁵ Inserted by Information Technology (Amendment) Act, 2008. 376

(3) Every notification made by the Central Government under sub-section (1) of section 70A and every rule made by it ¹⁷⁷ shall be laid, as soon as may be after it is made, before each House of Parliament , while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in ¹⁷⁸ the rule or both Houses agree that ¹⁷⁹ the rule should not be made, ¹⁸⁰ the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be, so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

88. Constitution of Advisory Committee.

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and nonofficial members representing the interests principally

¹⁷⁸ The words "the notification or" omitted by Information Technology (Amendment) Act, 2008.

¹⁷⁹ The words "the notification or" omitted by Information Technology (Amendment) Act, 2008.

¹⁸⁰ The words "the notification or" omitted by Information Technology (Amendment) Act, 2008.

¹⁷⁶ Inserted by Information Technology (Amendment) Act, 2008.

¹⁷⁷ The words "Every notification made by the Central Government under subsection (1) of section 70A and every rule made by it" substituted by Information Technology (Amendment) Act, 2008 for "Every notification made by the Central Government under clause (f) of sub-section (4) of section 1 and every rule made by it".

affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise-

(a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the controller in framing the regulation under this Act.

(4) There shall be paid to the non-official members of such Committee such traveling and other allowances as the Central Government may fix.

COMMENTS:

As per the notification of Ministry of Information Technology, Government of India, dated 17 October, 2000, the Chairman of the Cyber Regulations Advisory Committee is the Minister, Information Technology. The Senior Director, Ministry of Information Technology is the Member Secretary. The other members are:

(1) Secretary, Legislative Department

(2) Secretary, Ministry of Information Technology

(3) Secretary, Department of Telecommunications

(4) Finance Secretary

(5) Secretary, Ministry of Defence

(6) Secretary, Ministry of Home Affairs

(7) Secretary, Ministry of Commerce

(8) Deputy Governor, Reserve Bank of India

(9) Shri T K Vishwanathan, [Member Secretary, Law Commission]

(10) President, NASSCOM

(11) President, Internet Service Providers Association

(12) Director, Central Bureau of Investigation

(13) Controller of Certifying Authority

(14) Information Technology Secretary by rotation from the States

(15) Director General of Police by rotation from the States

(16) Director, IIT by rotation from the IITs

(17) Representative of CII

(18) Representative of FICCI

(19) Representative of ASSOCHAM

Pursuant to this section, an important order relating to blocking of websites was passed on 27th February, 2003. Under this, Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website.

89. Power of Controller to make regulations.¹⁸¹

(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:-

(a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (n) of section 18;

(b) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (1) of section 19;

(c) the terms and conditions subject to which a licence may be granted under clause (c) of sub-section (3) of section 21;

COMMENTS:

Information Technology (Certifying Authority) Regulations, 2001 contain the relevant provisions.

(d) other standards to be observed by a Certifying Authority under clause (d) of section 30;

¹⁸¹ Refer "INFORMATION TECHNOLOGY (CERTIFYING AUTHORITY) REGULATIONS, 2001" issued by Controller of Certifying Authorities on 9th July 2001 [G.S.R. 512 (E)]

COMMENTS:

Information Technology (Certifying Authority) Regulations, 2001 contain the relevant provisions.

(e) the manner in which the Certifying shall disclose the matters specified in sub-section (1) of section 34;

COMMENTS:

Information Technology (Certifying Authority) Regulations, 2001 contain the relevant provisions.

(f) the particulars of statement which shall accompany an application under sub-section (3) of section 35;

(g) the manner by which the subscriber shall communicate the compromise of private key to the certifying Authority under sub-section (2) of section 42.

COMMENTS:

Information Technology (Certifying Authority) Regulations, 2001 contain the relevant provisions.

(3) Every regulations made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation. 90. Power of State Government to make rules.

(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:-

(a) the electronic form in which filing, issue, grant, receipt or payment shall be effected under sub-section (1) of section 6;

(b) for matters specified in sub-section (2) of section6;

(c) omitted by Information Technology (Amendment) Act, 2008. ¹⁸²

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

91. omitted by Information Technology (Amendment) Act, 2008.¹⁸³

92. omitted by Information Technology (Amendment) Act, 2008¹⁸⁴

93. omitted by Information Technology (Amendment) Act, 2008¹⁸⁵

¹⁸⁴ Amendment of Act 1 of 1872. – The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

¹⁸⁵ Amendment of Act 18 of 1891.- The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

 $^{^{182}}$ (c) any other matter which is required to be provided by rules by the State Government.

¹⁸³ Amendment of Act 45 of 1860.- The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

94. omitted by Information Technology (Amendment) Act, 2008¹⁸⁶

¹⁸⁶ Amendment of Act 2 of 1934.- The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act. 382

FIRST SCHEDULE¹⁸⁷

[See sub-section (4) of section 1]

DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY

- SL No Description of documents or transactions
- 1. A negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881.
- 2. A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882.
- 3. A trust as defined in section 3 of the Indian Trusts Act, 1882.
- 4. A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925, including any other testamentary disposition by whatever name called.
- 5. Any contract for the sale or conveyance of immovable property or any interest in such property.

¹⁸⁷ Inserted by Information Technology (Amendment) Act, 2008. 383

THE SECOND SCHEDULE¹⁸⁸ [See sub-section (1) of section 3 A]

ELECTRONIC SIGNATURE OR ELECTRONIC AUTHENTIATION TECHNIQUE AND PROCEDURE

SI. No.	Description		Procedure
(1)	(2)	(3)	

¹⁸⁸ Inserted by Information Technology (Amendment) Act, 2008. 384

AMENDMENTS TO THE INDIAN PENAL CODE¹⁸⁹

The *Information Technology Act, 2000* made the following amendments to the Indian Penal Code:

1. After section 29, the following section shall be inserted, namely:—

"29 A. The words "electronic record" shall have the meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000.".

2. In section 167, for the words "such public servant, charged with the preparation or translation of any document, frames or translates that document", the words "such public servant, charged with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record" shall be substituted.

3. In section 172, for the words "produce a document in a Court of Justice", the words "produce a document or an electronic record in a Court of Justice" shall be substituted.

4. In section 173, for the words "to produce a document in a Court of Justice", the words "to produce a document or electronic record in a Court of Justice" shall be substituted.

5. In section 175, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

6. In section 192, for the words "makes any false entry in any book or record, or makes any document containing a false statement", the words "makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement" shall be substituted.

7. In section 204, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

8. In section 463, for the words "Whoever makes any false documents or part of a document with intent to cause damage or injury", the words "Whoever makes any false documents or false electronic record or part of a document

¹⁸⁹ As made by section 91 of the Information Technology Act, 2000.

or electronic record, with intent to cause damage or injury" shall be substituted.

9. In section 464,—

(a) for the portion beginning with the words "A person is said to make a false document" and ending with the words "by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration", the following shall be substituted, namely:—

"A person is said to make a false document or false electronic record—

First—Who dishonestly or fraudulently—

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any digital signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the digital signature with the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly—Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration.";

(b) after Explanation 2, the following Explanation shall be inserted at the end, namely:—

'Explanation 3.—For the purposes of this section, the expression "affixing digital signature" shall have the meaning assigned to it in clause (d) of sub-section (1) of section 2 of the Information Technology Act, 2000.'

10. In section 466,—

(a) for the words "Whoever forges a document", the words "Whoever forges a document or an electronic record" shall be substituted;

(b) the following Explanation shall be inserted at the end, namely:—

'Explanation.—For the purposes of this section, "register" includes any list, data or record of any entries maintained in the electronic form as defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000.'.

11. In section 468, for the words "document forged", the words "document or electronic record forged" shall be substituted.

12. In section 469, for the words "intending that the document forged", the words "intending that the document or electronic record forged" shall be substituted.

13. In section 470, for the word "document" in both the places where it occurs, the words "document or electronic record" shall be substituted.

14. In section 471, for the word "document" wherever it occurs, the words "document or electronic record" shall be substituted.

15. In section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following shall be substituted, namely:—

"Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code.".

16. In section 476, for the words "any document", the words "any document or electronic record" shall be substituted.

17. In section 477A, for the words "book, paper, writing" at both the places where they occur, the words "book, electronic record, paper, writing" shall be substituted.

The *Information Technology (Amendment) Act, 2008* made the following amendments to the Indian Penal Code:

(a) in section 4, -

(i) after clause (2), the following clause be inserted, namely:-

"(3) any person in any place without and beyond India committing offence targeting a computer resource located in India.";

(ii) for the Explanation, the following Explanation shall be substituted, namely:-

'Explanation. - In this section –

(a) the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Code;

(b) the expression "computer resource" shall have the meaning assigned to it in clause
(k) of sub-section (1) of section 2 of the Information Technology Act, 2000.';

(b) in section 40, in clause (2), after the figure "117", the figures and word "118, 119 and 120" shall be inserted;

(c) in section 118, for the words "voluntarily conceals, by any act or illegal omission, the existence of a design", the words "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design" shall be substituted;

(d) in section 119, for the words "voluntarily conceals, by any act or illegal omission, the existence of a design", the words "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design" shall be substituted;

(e) in section 464, for the words "digital signature" wherever they occur, the words "electronic signature" shall be substituted;

AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872¹⁹⁰

The *Information Technology Act, 2000* made the following amendments to the Indian Evidence Act:

1. In section 3,—

(a) in the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the words "all documents including electronic records produced for the inspection of the Court" shall be substituted;

(b) after the definition of "India", the following shall be inserted, namely:—

'the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.'.

2. In section 17, for the words "oral or documentary", the words "oral or documentary or contained in electronic form" shall be substituted.

3. After section 22, the following section shall be inserted, namely:—

"22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.".

4. In section 34, for the words "Entries in the books of account", the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted.

5. In section 35, for the word "record", in both the places where it occurs, the words "record or an electronic record" shall be substituted.

6. For section 39, the following section shall be substituted, namely:—

"39. When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an

¹⁹⁰ As made by section 92 of the Information Technology Act, 2000.

isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.".

7. After section 47, the following section shall be inserted, namely:—

"47A. When the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.".

8. In section 59, for the words "contents of documents" the words "contents of documents or electronic records" shall be substituted.

9. After section 65, the following sections shall be inserted, namely:—

'65A. The contents of electronic records may be proved in accordance with the provisions of section 65B.

65B. (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:—

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers.

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—

(a) identifying the electronic record containing the statement and describing the manner in which it was produced; (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

'Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.'.

10. After section 67, the following section shall be inserted, namely:—

"67A. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.".

11. After section 73, the following section shall be inserted, namely:—

'73A. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

'Explanation.—For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000'.

12. After section 81, the following section shall be inserted, namely:—

"81A. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.".

13. After section 85, the following sections shall be inserted, namely:—

"85A. The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

85B. (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that—

(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;
(b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature. 85C. The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber."

14. After section 88, the following section shall be inserted, namely:—

'88A. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation.—For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000.'.

15. After section 90, the following section shall be inserted, namely:—

"90A. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation.—Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

This Explanation applies also to section 81A.".

16. For section 131, the following section shall be substituted, namely:—

"131. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if

they were in his possession or control, unless such lastmentioned person consents to their production."

The *Information Technology (Amendment) Act, 2008* made the following amendments to the Indian Evidence Act:

(a) in section 3 relating to interpretation clause, in the paragraph appearing at the end, for the words "digital signature" and "Digital Signature Certificate", the words "electronic signature" and "Electronic Signature Certificate" shall respectively be substituted;

(b) after section 45, the following section shall be inserted, namely:-

"45A. When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000, is a relevant fact.

Explanation.- For the purposes of this section, an Examiner of Electronic Evidence shall be an expert.";

(c) in section 47A, -

(i) for the words "digital signature", the words "electronic signature" shall be substituted;

(ii) for the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted;

(d) in section 67A, for the words "digital signature" wherever they occur, the words "electronic signature" shall be substituted;

(e) in section 85A, for the words "digital signature" at both the places where they occur, the words "electronic signature" shall be substituted; (f) in section 85B, for the words "digital signature" wherever they occur, the words "electronic signature" shall be substituted;

(g) in section 85C, for the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted;

(h) in section 90A, for the words "digital signature" at both the places where they occur, the words "electronic signature" shall be substituted;

AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT¹⁹¹

1. In section 2—

(a) for clause (3), the following clause shall be substituted namely:—

'(3) "bankers' books" include ledgers, day-books, cashbooks, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;

(b) for clause (8), the following clause shall be substituted, namely:—

'(8) "certified copy" means when the books of a bank,— (a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title: and

(b) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.'.

2. After section 2, the following section shall be inserted, namely:—

"2A. A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely:—

¹⁹¹ As made by section 93 of the Information Technology Act, 2000.

(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of—

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(B) the safeguards adopted to prevent and detect unauthorised change of data;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;

(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(F) the mode of identification of such data storage devices;

(G) the arrangements for the storage and custody of such storage devices;

(H) the safeguards to prevent and detect any tampering with the system; and

(I) any other factor which will vouch for the integrity and accuracy of the system.

(c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data."

COMMENTS:

The *Bankers' Books Evidence Act* lays down the rules of evidence in relation to bankers' books. Generally, bankers' books would be adduced as evidence where any financial transaction involving the banking system is in question or has to be examined.

The *Information Technology Act* has amended the *Bankers' Books Evidence Act* to confer equal status on electronic records as compared with paper based documents.

If a "certified copy" of printouts of bankers' books has to be given, then such printouts must be accompanied by three certificates.

Let us take a simple illustration to understand the contents of these certificates.

Illustration: Sameer issued a cheque to Pooja for Rs 3 lakh. The cheque was dishonoured by Sameer's bank (Noodle Bank Ltd) as the balance in Sameer's account was only Rs 50,000. Pooja has filed a case against Sameer under section 138 of the Negotiable Instruments Act for the cheque "bouncing".

Pooja has requested Noodle Bank for a certified copy of Sameer's bank account statement (for January 2008) for producing in court as evidence. The printout of the bank statement will be accompanied by the following 3 certificates:

Certificate u/s 2A(a) of the Bankers' Books Evidence Act

I, the undersigned, state to the best of my knowledge and belief that:

(1) Mr. Sameer Sen is holding account no. 12345 with the Pune branch of the Noodle Bank Ltd.

(2) The accompanying bank account statement is a printout of the transactions and balances in the said bank account for the period beginning 1st January 2008 and ending 31st January 2008.

Siddharth Sharma, Manager, Pune branch, Noodle Bank Ltd.

Certificate u/s 2A(b) of the Bankers' Books Evidence Act

I, the undersigned, state to the best of my knowledge and belief that the enclosed "Information Security Policy of Noodle Bank Ltd." contains true and correct information relating to the computer system used to store bank account related information of Noodle Bank customers including the following information: (1) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(2) the safeguards adopted to prevent and detect unauthorised change of data;

(3) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(4) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electromagnetic data storage devices;

(5) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(6) the mode of identification of such data storage devices;

(7) the arrangements for the storage and custody of such storage devices;

(8) the safeguards to prevent and detect any tampering with the system; and

(9) other factors that will vouch for the integrity and accuracy of the system.

Pooja Singh, System Administrator, Pune branch, Noodle Bank Ltd.

Enclosed: Information Security Policy of Noodle Bank Ltd

Certificate u/s 2A(c) of the Bankers' Books Evidence Act

I, the undersigned, state to the best of my knowledge and belief that:

(1) The Noodle computer system described more accurately in the "Information Security Policy of Noodle Bank Ltd" operated properly at the material time when the said system was used to take the printout relating to the transactions and balances in the bank account no. 12345 for the period beginning 1st January 2008 and ending 31st January 2008 was taken.

(2) The printout referred to above is appropriately derived from the relevant data stored in the said system.

Pooja Singh, System Administrator, Pune branch, Noodle Bank Ltd

AMENDMENTS TO THE RESERVE BANK OF INDIA ACT, 1934¹⁹²

In the Reserve Bank of India Act, 1934, in section 58, in subsection (2), after clause (p), the following clause shall be inserted, namely:—

"(pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of section 45-1, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers;".

COMMENTS:

The *Payment and Settlement Systems Act, 2007* contains provisions relating to the regulation and supervision of payment systems in India. This Act also designates the Reserve Bank of India as the authority for that purpose. According to section 2(1)(c) of this Act:

"electronic funds transfer" means any transfer of funds which is initiated by a person by way of instruction, authorisation or order to a bank to debit or credit an account maintained with that bank through electronic means and includes point of sale transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfers initiated by telephone, internet and card payment;

Two regulations have been made under this Act, namely - the Board for Regulation and Supervision of Payment and Settlement Systems Regulation, 2008 and the Payment and Settlement Systems Regulations, 2008. The Act as well as these regulations came into force on 12th August 2008.

Section 26 of this Act provides penalties for several acts as discussed below:

(1) Commencing or operating a payment system except under and in accordance with an authorisation issued by the Reserve Bank is punishable with imprisonment for a term not less than one month but which may extend to 10 years and / or with fine which may extend to Rs.

¹⁹² As made by section 94 of the Information Technology Act, 2000.

1 crore. A further fine upto Rs 1 lakh per day of the contravention may also be levied.

(2) Failure to comply with the terms and conditions subject to which the authorisation has been issued by the Reserve Bank is punishable with imprisonment for a term not less than one month but which may extend to 10 years and / or with fine which may extend to Rs. 1 crore. A further fine upto Rs 1 lakh per day of the contravention may also be levied.

(3) Wilfully making a false statement or omission in any application for authorisation or in any return or document or information required to be furnished is punishable with imprisonment upto 3 years and fine between Rs 10 lakh and Rs 50 lakh.

(3) Failure to produce or furnish any statement, information, returns or other documents is punishable with fine which may extend to Rs 10 lakh in respect of each offence. Additionally a further fine of upto Rs 25,000 for every day for which the offence continues may also be levied.

(4) Disclosure of information that is required to be kept confidential under this Act is punishable with imprisonment upto 6 months and / or fine. This fine may extend to Rs 5 lakh or an amount equal to twice the amount of the damages incurred by the act of such disclosure, whichever is higher.

(5) Failure to comply with a direction issued under this Act or failure to pay a penalty imposed under this Act is punishable with imprisonment between 1 month and 10 years and / or fine upto Rs 1 crore. A further fine upto Rs 1 lakh per day of the contravention may also be levied.

The Reserve Bank of India also regulates:

(1) National Electronic Funds Transfer (NEFT) system which is a nationwide funds transfer system to facilitate transfer of funds from any bank branch to any other bank branch.

(2) Real Time Gross Settlement (RTGS) system which is a funds transfer mechanism where transfer of money takes place from one bank to another on a 'real time' and on 'gross' basis. This is the fastest possible money transfer system through the banking channel.

(3) Electronic Clearing Service (ECS) which is a mode of electronic funds transfer from one bank account to another bank account using the services of a Clearing House.

ANNEXURE 1 – SAMPLE FIRST INFORMATION REPORT (FIR)

(Under Section 154 Cr.P.C.)

1. District: Zimblia P.S.: Green Lawns Year: 2009 FIR No. 1234 Date: 23rd March

- 2. (i) Act Information Technology Act, 2000 Sections <u>66</u>
 - (ii) Act _____ Sections __
 - (iii) Act _____ Sections __
 - (iv) Other Acts & Sections

3. (a) Occurrence of offence:

- Date from 23rd March 2009Date to 23rd March 2009Time from 1045 hrsTime to 1115 hrs
- (b) Information received at P.S.:

Date <u>23rd March 2009</u> Time <u>1245hrs</u>

(c) General Diary Reference:

Entry No. <u>23</u> Time <u>1245 hrs</u>

4. Type of Information: Written / Qral

5. Place of Occurrence:

(a) Direction and distance from P.S _____Beat No. _____

(b) Address <u>36th Floor, Centrino Towers, Main Street, Green Lawns</u> Enclave, Zimblia

(c) In case, outside the limit of this Police Station, then Name of P.S. District

6. Complainant / Informant:

(a) Name Pooja Malhotra

(b) Father's/Husband's Name Sameer Malhotra

(c) Date/Year of Birth 6th November, 1972 (d) Nationality Indian

(e) Passport No. <u>A12345678</u> Date of Issue <u>20th October 2001</u> Place of Issue Zimblia

(f) Occupation Director, Centrino Technologies Ltd

(g) Address <u>36th Floor, Centrino Towers, Main Street, Green Lawns</u> Enclave, Zimblia

7. Details of known/suspected/unknown accused with full particulars:

(Attach separate sheet, if necessary)

- (1)_____(2)_____
- (3)

8. Reasons for delay in reporting by the complainant / informant Not applicable

9. Particulars of properties stolen (Attach separate sheet, if necessary) Not applicable

10. Total value of property stolen Not applicable

11. Inquest Report / U.D. case No., if any

12. First Information contents (Attach separate sheet, if required):

Centrino Technologies Ltd is a company involved in the business of software development, computer training and allied works. The company relies heavily on Internet, computers, computer systems, computer network and electronic information. The company has a dedicated Research & Development facility that develops the source codes and various programmes thereby developing various software. The company is also involved in promoting, trading in and licensing these software.

On 23rd March 2009 at around 1045 hrs the computer network at Centrino crashed and nearly all the information on the computers was effectively destroyed, altered and/or deleted. Due to the disruption so caused, the computers had to be shut down resulting in stoppage of the business of the company. It is suspected that the company's networks have been deliberately attacked by malicious code sent electronically by unidentified persons.

13. Action taken: Since the above information reveals commission of offence(s) u/s as mentioned at Item No. 2. :

(1) Registered the case and took up the investigation or

(2) Directed (Name of I.O.) _____ Rank _____ No. _____ to take up the Investigation or

 (3) Refused investigation due to ______ or

 (4) Transferred to P.S. _____ District _____ on point

of jurisdiction.

F.I.R. read over to the complainant / informant, admitted to be correctly recorded and a copy given to the complainant /informant, free of cost.

R.O.A.C. Police Station Signature of Officer in charge,

Name Karan Saxena

Rank Asst. Commissioner of Police No. 12345

14. Signature / Thumb impression of the complainant / informant.

15. Date and time of despatch to the court 23^{rd} March 2009 at 1530 <u>hrs</u>

Physical features, deformities and other details of the suspect/accused: (If known / seen)

Sl. No.	Sex	Date/Year of Birth	Build	Height (cms.)	Complexion	Identification Mark(s)
1	2	3	4	5	6	7

Deformities/ Peculiarities	Teeth	Hair	Eyes	Habit(s)	Dress Habit(s)
8	9	10	11	12	13

LANGUAGE/	PLACE OF				
DIALECT	Burn	Leucoderma	Mole	Scar	Tattoo
	Mark				
14	15	16	17	18	19

These fields will be entered only if complainant/informant gives any one or more particulars about the suspect/accused.

ANNEXURE 2 – SAMPLE CRIMINAL COMPLAINT

IN THE COURT OF JUDICIAL MAGISTRATE FIRST CLASS (COURT NO. 4) ZIMBLIA, AT ZIMBLIA

Regular Criminal Complaint No. / 2009

Vs.

Amit Singh,S/o Deepak Singh aged about 40 yearsOccupation-businessComplainantResiding at 2, Deccan, Zimblia

- Sameer Sen Chairman and Managing Director, Hi Tech Ltd,
 MG Road, Zimblia
- 2. Hi Tech Ltd, Accused
 A company registered under the a Companies Act, 1956
 and having Regd. Office at, 1, MG Road, Zimblia
 Complaint u/s 67 of the

Information Technology Act, 2000

The complainant above named submits as follows:

- 1. That the complainant is a resident of the above mentioned address.
- 2. That the complainant is a web development consultant and regularly views websites on the Internet for educational and information purposes.
- 3. That accused number 2 owns, runs, and maintains the website http://www.porn.com (details as per annexure I).

- 4. That the accused number 1 is the Chairman and Managing Director of the accused number 2 (details as per annexure II).
- 5. That it came to the notice of the complainant that pornographic and obscene photographs are available on the above mentioned website.
- 6. That on the 27th day of March, 2009, the complainant viewed the above mentioned website, from a computer at his residence, in order to verify whether the above mentioned website disseminates pornographic and obscene materials.
- 7. On investigation, the complainant found that the website contains obscene and pornographic photographs (as per annexure III). The website states that it is "Dedicated to the beautiful girls of Zimblia".
- 8. The actions of the accused number 1 and 2 fall under the scope of section 67 of the Information Technology Act, 2000.
- 9. That the cause of action for this complaint arose on 27th March, 2009 and hence the complaint filed today is well within limitation.
- 10. That the offence has been committed within the local limits of the jurisdiction of this court and hence this Hon'ble Court has jurisdiction to try and decided this complaint.
- 11. That the necessary court fees have been paid herewith.
- 12. That the complainant therefore prays that the accused be charged with and tried for the offences punishable under section 67 of the Information Technology Act, 2000 and punished according to law.

Zimblia

Date: 27th March, 2009

Advocate for the complainant Complainant

VERIFICATION

I, Amit Singh, S/o Deepak Singh aged about 40 years, Occupationbusiness, residing at Deccan, Zimblia, the above named complainant swear on solemn affirmation that the information contained in paragraphs 1 to 12 above is true to the best of my knowledge and belief.

Complainant

ANNEXURE 3 – SAMPLE PROPERTY SEARCH & SEIZURE FORM

(Search/Production/Recovery u/s 51/102/165 Cr.P.C..... etc.)

1. District: Zimblia P.S.: Green Lawns Year: 2009 FIR No. 1234 Date: 23rd March

2. Act & sections Section 66 of the Information Technology Act, 2000

3. Nature of property seized: Stolen / Unclaimed / Unlawful possession (Involved) Intestate.

4. Property seized/ recovered: (a) Date 24^{th} March 2009 (b) Time 1100 hrs

- (c) Place <u>14 Alex Street</u>, Zimblia
- (d) Description of the place <u>Residence of accused no. 1 and 2</u>

5. Person from whom seized /recovered :

Name Siddharth KapoorFather's/Husband's name Prathmesh KapoorSex MaleAge 21 yearsAddress 14 Alex Street, Zimblia

Professional receiver of stolen property. Yes / No)

6. Witnesses:

(i) Name <u>Savita Kulkerni</u> Father's/Husband's name <u>Gokul</u> <u>Kulkerni</u>

Age <u>43 years</u>Occupation IT ProfessionalAddress <u>123</u>, Sim Lim,Zimblia

(ii) Name <u>Abhijeet Narayan</u> Father's/Husband's name <u>Venkat</u> <u>Narayan</u>

Age 29 yearsOccupation IT ProfessionalAddress 411, Sim Lim,Zimblia

7. Action taken/recommended for disposal of perishable property Not applicable **8.** Action taken/recommended for keeping of valuable property Deposited with computer storage room at the Zimblia District Court

9. Identification required. Yes/No

10. Details of properties seized/ **recovered** (Use appropriate prescribed form(s) and attach).

(1) Toshiba ® Laptop Model no - A48756876 having serial number 95535353BF

(2) Toshiba ® Laptop Model no – A48756876 having serial number 95535354BF

(Attach separate sheet, if required)

11. Circumstances/grounds for seizure

The above laptop computers are suspected to have been used to plan and commit offence by the accused in Case no. 1234 registered with the Green Lawns police station.

12. The above mentioned properties were seized in accordance with the provisions of law in the presence of the above said witnesses/* and a copy of the seizure form was given to the person/ the occupant of the place from whom seized.

13. The following properties were packed and/or sealed and the signature of the above said witnesses obtained thereon or on the body of the property.

Sl. No.	Property	Indicate whether
		signature obtained on
		the packet or on the
		body of the property
1	2	3

Signature of the person from whom seized (if present)

Witness-1 Signature Signature of Investigating officer Name <u>Karan Saxena</u> Rank <u>Asst. Comm. of Police</u> No. <u>12345</u> Place Zimblia Date <u>24th March 2009</u>

Witness-2 Signature

* In case the property is seized from such a place that no receipt is required to be given to anybody, this portion of the sentence should be struck off.

ANNEXURE 4 – FINAL FORM / REPORT

FINAL FORM/ REPORT

(Under Section 173 Cr.P.C.) IN THE COURT OF JUDICIAL MAGISTRATE FIRST CLASS, ZIMBLIA AT ZIMBLIA

1. District Zimblia**P.S.** Green LawnsYear 2009**FIR No** 1234**Date** 23rd March 2009

2. Final Report / Charge Sheet No 1234

3. Date <u>23rd April 2009</u>

4. (i) Act Information Technology Act, 2000	Sections <u>66</u>
(ii) Act	Sections
(iii) Act	Sections
(iv) Other Acts & Sections	

5. Type of Final Form/Report Charge Sheed/ Not charge sheeted for want of evidence / FR True, Undetected / FR True, Untraced / FR True, offence abated / FR Unoccurred. (tick applicable portion).

6. If FR Unoccurred: False/Mistake of Fact/Mistake of law/Non cognisable /Civil nature. (tick applicable portion).

7. If Charge sheet: Original / Supplementary. (tick applicable portion).

8. Name of I.O. <u>Karan Saxena</u> No. <u>12345</u> (at the time of charge sheet) Rank <u>Asst. Commissioner of Police</u>

9. (a) Name of complainant / informant Pooja Malhotra

(b) Father's / Husband's name Sameer Malhotra

10. Details of Properties/Articles/Documents recovered/seized during investigation and relied upon (separate list can be attached, if necessary).

S1.	Property	Estimated	P.S.	From whom/	Disposal
No.	description	value	Property	where	
		(Rs.)	Register	recovered or	
			No.	seized	
1	2	3	4	5	6

11. Particulars of accused persons charge-sheeted: (Use separate sheet for each accused)

Sl. No. 1

(i) Name Siddharth Kapoo	T Whether verified					
(ii) Father's/Husband's name Prathmesh Kapoor						
(iii) Date/ Year of birth 10) th Jan 1988					
(iv) Sex <u>Male</u> (*	(v) Sex <u>Male</u> (v) Nationality <u>Indian</u>					
(vi) Passport No. <u>B123456</u> Place of Issue <u>Zimblia</u>	Date of Issue <u>14th February 2007</u>					
(vii) Religion Hindu	(viii) Whether SC/ST/OBC No					
(ix) Occupation <u>Student</u>						
(x) Address <u>14 Alex Street</u>	, Zimblia Whether verified					
(xi) Provisional criminal N	No. <u>4567</u>					
(xii) Regular criminal No. arrest <u>30th March 2009</u>	(if known) (xiii) Date of					
(xiv) Date of release on ba	il <u>4th April 2009</u>					
(xv) Date on which forward	rded to court					
(xvi) Under Acts & Sectio Act, 2000	ns section <u>66 of the Information Technology</u>					
(xvii) Details of bailers / se	ureties:					
Name Prathmesh Kapoor	Father's/Husband's name Sankalp Kapoor					
Occupation Business	Address 14 Alex Street, Zimblia					

(xviii) Previous convictions with case references

(xix) Status of the accused: Forwarded / Bailed by police Bailed by courd/ Judicial custody / Absconding / Proclaimed offender (tick applicable portion). Sl. No. 2 (i) Name Priyanka Kapoor Whether verified (ii) Father's/Husband's name Prathmesh Kapoor (iii) Date/ Year of birth 16th Jan 1987 (iv) Sex Female (v) Nationality Indian Date of Issue 14th February 2007 (vi) Passport No. B12345679 Place of Issue Zimblia (vii) Religion Hindu (viii) Whether SC/ST/OBC No (ix) Occupation Student (x) Address 14 Alex Street, Zimblia Whether verified (xi) Provisional criminal No. 4568 (xii) Regular criminal No. (if known) (xiii) Date of arrest 30th March 2009 (xiv) Date of release on bail 4th April 2009 (xv) Date on which forwarded to court (xvi) Under Acts & Sections section 66 of the Information Technology Act, 2000 (xvii) Details of bailers / sureties: Name Prathmesh Kapoor Father's/Husband's name Sankalp Kapoor **Occupation** Business Address 14 Alex Street, Zimblia

(xviii) Previous convictions with case references

(xix) Status of the accused:

Forwarded / Bailed by police (Bailed by courd) / Judicial custody / Absconding / Proclaimed offender (tick applicable portion).

12. Particulars of accused persons - not charge sheeted (suspect) : (Use separate sheet for each suspect)

Sl. No. ____

(i) Name	Whet	ther verified
(ii) Father's/Husban	d's name	
(iii) Date/ Year of bi	rth	
(iv) Sex	(v) Nationality	
(vi) Passport No	Date of Issue	Place of Issue
(vii) Religion	_ (viii) Whether S	SC/ST/OBC
(ix) Occupation		
(x) Address	Whether	verified
(xi) Provisional crim	ninal No	

(xii) Suspicion approved: Yes/No

(xiii) Status of the accused (suspect):

Bailed by police/Bailed by court/ Judicial custody/Not arrested (tick applicable portion).

(xiv) Under Acts & Sections

(xv) Any special remarks including reasons for not charge sheeting

13. Particulars of witnesses to be examined:

Sl. No.	Name	Father's / Husband's name	Date / Year of birth	Occupation	Address	Type of evidence to be tendered
1	2	3	4	5	6	7
1	Pravin Kale	Sudhir Kale	1971	Manager, Tetra Internet Services Ltd	12, Sun City, Zimblia	Details of IP addresses
2	Sudhir Sen	Shubro Sen	1976	Cyber Crime Investigator	44, Sim Lim, Zimblia	Forensic report of laptop seized from the accused

14. If FR is false, indicate action taken or proposed to be taken u/s 182/211 I.P.C _____

15. Result of Laboratory analysis

16. Brief facts of the case (Add separate sheet, if necessary)

Centrino Technologies Ltd (the complainant) is a company involved in the business of software development, computer training and allied works. The complainant relies heavily on Internet, computers, computer systems, computer network and electronic information. The company has a dedicated Research & Development facility that develops the information source codes and various programmes thereby developing various software. The complainant is also involved in promoting, trading in and licensing these software.

The complainant has invested substantially, both in computer hardware and software to provide standard quality. Furthermore the complainant has to also hire and/or take help of experts for development of various programmes, source codes and software for which the complainant has to bear heavy expenses.

On 23rd March 2009 at around 1045 hrs the computer network at Centrino crashed and nearly all the information on the computers was effectively destroyed, altered and/or deleted. Due to the disruption so

caused, the computers had to be shut down resulting in stoppage of the business of the company.

The Complainant lost nearly all files thereby losing the important information present in 15 of its computers. All these 15 computers had the major information including the source codes and programmes of various software, all of which were damaged and / or destroyed. The Complainant lost large amounts of software apart from incurring problems on day-to-day basis. The loss of software and Intellectual Property included the following code lines:

ABC Project = 81000 lines of code.

DEF Project = 159000 lines of code.

The incident also resulted in delay in development of most of the software on account of information loss. Thus the Complainant suffered heavy damages and losses on account of the loss of information, source codes, programmes, registry, delay in software development and damage to computer/s, computer system and computer network and irreparable damage to the software.

The detailed examination of the entire incident revealed that the incident of loss of information, source codes and programmes, damage to computers, computer system and the computer network occurred on account of a virus being introduced in the computer / computer system /computer network.

The detailed forensic examination of the computer network led to the conclusion that the virus that caused the damage was sent to two of the company's email accounts as under.

Date	Sender	Receiver	Attachment
23 rd	Sameer Sen	a.singh@centrino.com	Imp.doc
March 2009	<s_sen@hitech.com></s_sen@hitech.com>		
23 rd March 2009	Sameer Sen <s_sen@hitech.com></s_sen@hitech.com>	k.varun@ centrino.com	Vimp.doc

The IP address of the computers from which the emails were sent was ascertained by analyzing the headers of the two emails. A whois search revealed that the IP addresses were registered in the name of Tetra Internet Services Ltd.

Tetra Internet Services Ltd disclosed that at the relevant time periods, the said IP addresses had been allotted to its customer Siddharth Kapoor.

When the residence of Siddharth Kapoor was searched, two laptops were recovered. One of these laptops belonged to Siddharth Kapoor and the other belonged to his sister Priyanka Kapoor. A detailed forensic examination of the laptop computers revealed that the said laptops had been used to create the "belinga" virus and subsequently to email the virus to Centrino.

Siddharth Kapoor and Priyanka Kapoor were subsequently arrested and the Hon'ble Court granted six days police custody. During the custody, the accused confessed to having created the "belinga" virus and subsequently emailing it to Centrino. They had done so on account of a professional rivalry that they had with some of the Directors of Centrino.

17. Refer Notice served: Yes(No)

Date

(Acknowledgement to be placed)

18. Despatched on _

19. No. of enclosures

20. List of enclosures: As annexed

- 1. Printouts of the emails (along with detailed headers) which contained the virus as attachments.
- 2. Details of the IP address provided by Pravin Kale Manager, Tetra Internet Services Ltd.
- 3. Forensic report of laptop seized from the accused provided by Sudhir Sen.
- 4. CD containing source code of the virus as recovered from the laptops seized from the accused.

Forwarded by Officer in charge

Signature of Investigating Officer submitting Final report/Charge sheet

Name Pavan Jain Rank: Deputy Comm. of Police No. 12345 Name Karan Saxena Rank: Asst. Comm. of Police No. 12345

ANNEXURE 5 – SAMPLE COMPLAINT TO ADJUDICATING OFFICER

COMPLAINT TO ADJUDICATING OFFICER UNDER INFORMATION TECHNOLOGY ACT - 2000

I

1. Name of the Complainant	Pooja Sharma
2. E-mail address	ps@asianlaws.org
3. Telephone No.	9112345677
4. Address for correspondence	12, Senapati Bapat Road, Pune
5. Digital Signature Certificate, if any	N.A

II

1. Name of the Respondent	Sameer Sen
2. E-mail address	sameer_sen@internomoda.com
3. Telephone No.	917658756
4. Address for correspondence	173/5, Sadashiv Peth, Pune
5. Digital Signature Certificate, if any	N.A

III

Damages claimed:	Rs 500,000
Fee deposited:	Rs 13,000
Demand Draft No.123456 dated Bank, Pune	5 th January 2008 drawn on Noodle

IV

Complaint under	Section 43 of the IT Act
Section/Rule/Direction/Order etc	

V	
Time of Contravention:	5 pm on 1 st January 2008

VI

Place of Contravention:	Pune
-------------------------	------

VII

Cause of action:		respo virus there	complainant ondent has intr es into her by damaged and other impo	oduo co com	ced mp put	computer uter and er source
VIII						
Brief facts of the case:	1.	The	Complainant	is	а	freelance

Brief facts of the case:	1. The Complainant is a freelance software programmer.
	2. The Respondent is also a freelance software programmer.
	3. On 1 st January 2008 at around 5 pm, the complainant received an email from sameer_sen@internomoda.com
	4. In the past the respondent has sent many emails to the complainant from this email address.
	5. The said email contained an attachment purporting to be the outline of a new software program that the respondent wanted the complainant to design.
	6. As soon as the complainant downloaded and executed the attachment, her computer stopped functioning. When she restarted her computer she realized that all data on her computer had been destroyed.
	7. The loss of software and Intellectual Property included the following code lines:

ABC Project = 8100 lines of code.
DEF Project = 1590 lines of code.
8. The Complainant suffered heavy damages and losses on account of the loss of information, source codes, programmes, and damage to computer.
9. A detailed examination of the entire incident revealed that the incident of loss of information, source codes and programmes, damage to computer etc occurred on account of a virus being introduced into the computer.
10. The Complainant reviewed the computer security in the wake of the above incident and further upgraded the virus detection software. The Complainant also took help of experts to detect the original file that was carrying the virus.
11. The Complainant suspected some foul play on the part of the Respondent and wanted to verify and ascertain the same.
12. The upgradation of the virus detection software and the observations of the experts led to the detection of the Respondent as the originator/sender of the virus.
13. The virus that caused the above mentioned damages and wrongful losses to the Complainant, was sent by the Respondent as an email attachment mentioned in para 5.

(Signature of the Complainant)

ANNEXURE 6 – REAL WORLD CASES

1. Social networking sites related cases

Social networking sites like Orkut and Facebook are very popular nowadays. Users of such sites can search for and interact with people who share the same hobbies and interests. The profiles of such users are usually publicly viewable.

Scenario 1:

A fake profile of a woman is created on a social networking site. The profile displays her correct name and contact information (such as address, residential phone number, cell phone number etc). Sometimes it even has her photograph. The problem is that the profile describes her as a prostitute or a woman of "loose character" who wants to have sexual relations with anyone. Other members see this profile and start calling her at all hours of the day asking for sexual favours. This leads to a lot of harassment for the victim and also defames her.

Usual motives: Jealousy or revenge (e.g. the victim may have rejected the advances made by the suspect).

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 67 of the Information	Sections 66A and 67 of the
Technology Act and section 509 of	Information Technology Act and
Indian Penal Code	section 509 of Indian Penal Code

Scenario 2:

An **online hate community** is created. This community displays objectionable information against a particular country, religious or ethnic group or even against national leaders and historical figures.

Usual motives: Desire to cause racial hatred and communal discord and disharmony.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 153A & 153B of Indian	Section 66A of the Information
Penal Code	Technology Act and sections 153A
	& 153B of Indian Penal Code

Scenario 3:

A **fake profile of a man is created** on Orkut. The profile contains defamatory information about the victim (such as his alleged sexual weakness, alleged immoral character etc).

Usual motives: Hatred (e.g. a school student who has failed may victimize his teachers).

Before 27 October, 2009	After 27 October, 2009
Section 500 of Indian Penal Code	Section 66A of the Information
	Technology Act and section 500 of
	Indian Penal Code

2. Email Account Hacking

Emails are increasingly being used for social interaction, business communication and online transactions. Most email account holders do not take basic precautions to protect their email account passwords. Cases of theft of email passwords and subsequent misuse of email accounts are becoming very common.

Scenario 1:

The victim's email account password is stolen and the account is then misused for sending out malicious code (virus, worm, Trojan etc) to people in the victim's address book. The recipients of these viruses believe that the email is coming from a known person and run the attachments. This infects their computers with the malicious code.

Usual motives: Corporate espionage or a perverse pleasure in being able to destroy valuable information belonging to strangers etc.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the	Sections 43, 66, 66A and 66C of
Information Technology Act	the Information Technology Act

Scenario 2:

The victim's email account password is stolen and the hacker tries to extort money from the victim. The victim is threatened that if he does not pay the money, the information contained in the emails will be misused.

Usual motives: Illegal financial gain.

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the	Sections 43, 66, 66A & 66C of the
Information Technology Act	Information Technology Act

Scenario 3:

The victim's email account password is stolen and obscene emails are sent to people in the victim's address book.

Before 27 October, 2009	After 27 October, 2009
Sections 43, 66 and 67 of the	Section 43, 66, 66A and 67 of the
Information Technology Act	Information Technology Act
	Additionally, depending upon the content, sections 66C and 67B of the <i>Information Technology Act</i> may also apply

3. Credit Card Fraud

Credit cards are commonly being used for online booking of airline and railway tickets and for other ecommerce transactions. Although most ecommerce websites have implemented strong security measures (such as SSL, secure web servers etc), instances of credit card frauds are increasing.

In credit card fraud cases, the victim's credit card information is stolen and misused for making online purchases (e.g. airline tickets, software, subscription to pornographic websites etc).

Modus Operandi 1: The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computer of the victim. Unsuspecting victims would use these infected computers to make online transactions. The credit card information of the victim would be emailed to the suspect.

Modus Operandi 2: Petrol pump attendants, workers at retail outlets, hotel waiters etc note down information of the credit cards used for making payment at these establishments. This information is sold to criminal gangs that misuse it for online frauds.

Usual motives: Illegal financial gain

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the	Sections 43, 66, 66C, 66D of the
Information Technology Act and	Information Technology Act and
section 420 of Indian Penal Code	section 420 of Indian Penal Code

4. Online Share Trading Fraud

With the advent of dematerialization of shares in India, it has become mandatory for investors to have demat accounts. In most cases, an online banking account is linked with the share trading account. This has led to a large number of online share trading frauds.

Scenario 1:

The victim's account passwords are stolen and his accounts are misused for making fraudulent bank transfers.

Usual motives: Illegal financial gain

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the	Sections 43, 66, 66C & 66D of the
Information Technology Act and	Information Technology Act and
section 420 of Indian Penal Code	section 420 of Indian Penal Code

Scenario 2:

The victim's account passwords are stolen and his share trading accounts are misused for making unauthorised transactions that result in the victim making losses.

Usual motives: Revenge, jealousy, hatred.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the	Sections 43, 66, 66C & 66D of the
Information Technology Act and	Information Technology Act and
section 426 of Indian Penal Code	section 426 of Indian Penal Code

Modus Operandi:

The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computer of the victim. Unsuspecting victims would use these infected computers to login to their online banking and share trading accounts. The passwords and other information of the victim would be emailed to the suspect.

5. Tax Evasion and Money Laundering

Many unscrupulous businessmen and money launderers (havala operators) are using virtual as well as physical storage media for hiding information and records of their illicit business.

Scenario 1:

The suspect uses physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc. **Usual motives:** Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Information Technology Act	Information Technology Act
usually does not apply. Applicable	usually does not apply. Applicable
laws are usually the Income Tax	laws are usually the Income Tax
Act and the Prevention of Money	Act and the Prevention of Money
Laundering Act.	Laundering Act.

Scenario 2:

The suspect uses virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, Gspace etc.

Before 27 October, 2009	After 27 October, 2009
Information Technology Act	Information Technology Act
usually does not apply. Applicable	usually does not apply. Applicable
laws are usually the Income Tax	laws are usually the Income Tax
Act and the Prevention of Money	Act and the Prevention of Money
Laundering Act.	Laundering Act.

6. Source Code Theft

Computer source code is the most important asset of software companies. Simply put, source code is the programming instructions that are compiled into the executable files that are sold by software development companies.

As is expected, most source code thefts take place in software companies. Some cases are also reported in banks, manufacturing companies and other organizations that get original software developed for their use.

Scenario 1:

The suspect (usually an employee of the victim) steals the source code and sells it to a business rival of the victim.

Modus Operandi: If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device. If the suspect is not an employee of the victim, he would hack into the victim's servers to steal the source code. Or he would use social engineering to get unauthorised access to the code. He would then contact potential buyers to make the sale.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43, 65 & 66 of the	Sections 43, 65, 66 & 66B of the
Information Technology Act and	Information Technology Act and
section 63 of Copyright Act	section 63 of Copyright Act

Scenario 2:

The suspect (usually an employee of the victim) steals the source code and uses it as a base to make and sell his own version of the software.

Modus Operandi: If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage

device. If the suspect is not an employee of the victim, he would hack into the victim's servers to steal the source code. Or he would use social engineering to get unauthorised access to the code.

He would then modify the source code (either himself or in association with other programmers) and launch his own software.

Usual motives: Illegal financial gain.

Before 27 October, 2009	After 27 October, 2009
Sections 43, 65 & 66 of the	Sections 43, 65, 66 & 66B of the
Information Technology Act and	Information Technology Act and
section 63 of Copyright Act	section 63 of Copyright Act

7. Theft of Confidential Information

Most business organizations store their sensitive information in computer systems. This information is targeted by rivals, criminals and sometimes disgruntled employees.

Scenario 1:

A business rival obtains the information (e.g. tender quotations, business plans etc) using hacking or social engineering. He then uses the information for the benefit of his own business (e.g. quoting lower rates for the tender).

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the	Sections 43, 66 & 66B of the
Information Technology Act and	Information Technology Act and
section 426 of Indian Penal Code	section 426 of Indian Penal Code

Scenario 2:

A criminal obtains the information by hacking or social engineering and threatens to make the information public unless the victim pays him some money.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the	Sections 43, 66 & 66B of the
Information Technology Act and	Information Technology Act and
section 384 of Indian Penal Code	section 384 of Indian Penal Code

Scenario 3:

A disgruntled employee steals the information and mass mails it to the victim's rivals and also posts it to numerous websites and newsgroups.

Usual motives: Revenge.

Before 27 October, 2009	After 27 October, 2009
Sections 43 and 66 of the	Sections 43, 66, 66B of the
Information Technology Act and	Information Technology Act and
section 426 of Indian Penal Code	section 426 of Indian Penal Code

8. Software Piracy

Many people do not consider software piracy to be theft. They would never steal a rupee from someone but would not think twice before using pirated software. There is a common perception amongst normal computer users to not consider software as "property". This has led to software piracy becoming a flourishing business.

Scenario 1:

The software pirate sells the pirated software in physical media (usually CD ROMs) through a close network of dealers.

Modus Operandi: The suspect uses high speed CD duplication equipment to create multiple copies of the pirated software. This software is sold through a network of computer hardware and software vendors.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the <i>Information</i>	Section 43 & 66 of the Information
<i>Technology Act</i> and section 63 of	Technology Act and section 63 of
Copyright Act	Copyright Act

Scenario 2:

The software pirate sells the pirated software through electronic downloads through websites, bulletin boards, newsgroups, spam etc.

Modus Operandi: The suspect registers a domain name using a fictitious name and then hosts his website using a service provider that is based in a country that does not have cyber laws. Such service providers do not divulge client information to law enforcement officials of other countries.

Usual motives: Illegal financial gain.

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the <i>Information</i>	Section 43 & 66 of the Information
Technology Act and section 63 of	Technology Act and section 63 of
Copyright Act	Copyright Act

9. Music Piracy

Many people do not consider music piracy to be theft. They would never steal a rupee from someone but would not think twice before buying or using pirated music. There is a common perception amongst people that music is not "property". There is a huge business in music piracy. Thousands of unscrupulous businessmen sell pirated music at throw away prices.

Scenario 1:

The music pirate sells the pirated music in physical media (usually CD ROMs) through a close network of dealers.

Modus Operandi: The suspect uses high speed CD duplication equipment to create multiple copies of the pirated music. This music is sold through a network of dealers.

Usual motives: Illegal financial gain.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the <i>Information</i>	Section 43 & 66 of the Information
Technology Act and section 63 of	Technology Act and section 63 of
Copyright Act	Copyright Act

Scenario 2:

The music pirate sells the pirated music through electronic downloads through websites, bulletin boards, newsgroups, spam emails etc.

Modus Operandi: The suspect registers a domain name using a fictitious name and then hosts his website using a service provider that is based in a country that does not have cyber laws. Such service providers do not divulge client information to law enforcement officials of other countries.

Usual motives: Illegal financial gain.

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the Information	Section 43 & 66 of the Information
<i>Technology Act</i> and section 63 of	Technology Act and section 63 of
Copyright Act	Copyright Act

10. Email Scams

Emails are fast emerging as one of the most common methods of communication in the modern world. As can be expected, criminals are also using emails extensively for their illicit activities.

In the first step, the suspect convinces the victim that the victim is going to get a lot of money (by way of winning a lottery or from a corrupt African bureaucrat who wants to transfer his ill gotten gains out of his home country). In order to convince the victim, the suspect sends emails (some having official looking documents as attachments).

Once the victim believes this story, the suspect asks for a small fee to cover legal expenses or courier charges. If the victim pays up the money, the suspect stops all contact.

Usual motive: Illegal financial gain.

Before 27 October, 2009	After 27 October, 2009
Section 420 of Indian Penal Code	Sections 66A and 66D of the
	Information Technology Act and
	section 420 of Indian Penal Code

11. Phishing

With the tremendous increase in the use of online banking, online share trading and ecommerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial frauds.

Phishing involves fraudulently acquiring sensitive information (e.g. passwords, credit card details etc) by masquerading as a trusted entity.

Scenario:

The victim receives an email that appears to have been sent from his bank. The email urges the victim to click on the link in the email. When the victim does so, he is taken to "a secure page on the bank's website". The victim believes the web page to be authentic and he enters his username, password and other information. In reality, the website is a fake and the victim's information is stolen and misused.

Modus Operandi: The suspect registers a domain name using fictitious details. The domain name is usually such that can be misused for spoofing e.g. Noodle Bank has its website at <u>www.noodle.com</u> The suspect can target Noodle customers using a domain name like <u>www.noodle.bank-customerlogin.com</u>

The suspect then sends spoofed emails to the victims e.g. the emails may appear to come from <u>info@noodle.com</u>

The fake website is designed to look exactly like the original website.

Usual motive: Illegal financial gain.

Before 27 October, 2009	After 27 October, 2009
Section 43 & 66 of the Information	Sections 66, 66A & 66D of the
<i>Technology Act</i> and sections 419,	Information Technology Act and
420 & 468 of Indian Penal Code	sections 419, 420 & 468 of Indian
	Penal Code

12. Cyber Pornography

Cyber pornography is believed to be one of the largest businesses on the Internet today. The millions of pornographic websites that flourish on the Internet are testimony to this. While pornography per se is not illegal in many countries, child pornography is strictly illegal in most nations today.

Cyber pornography includes pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

Scenario:

The suspect accepts online payments and allows paying customers to view / download pornographic pictures, videos etc from his website.

Modus Operandi: The suspect registers a domain name using fictitious details and hosts a website on a server located in a country where cyber pornography is not illegal. The suspect accepts online payments and allows paying customers to view / download pornographic pictures, videos etc from his website.

Usual motive: Illegal financial gain.

Before 27 October, 2009	After 27 October, 2009
Section 67 of the Information	Section 67 of the Information
Technology Act	Technology Act and depending
	upon the content, sections 67A and
	67B may also apply

13. Online Sale of Illegal Articles

It is becoming increasingly common to find cases where sale of narcotic drugs, weapons, wildlife etc. is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc.

Scenario:

The suspect posts information about the illegal sale that he seeks to make. Potential customers can contact the seller using the email IDs provided. If the buyer and seller trust each other after their email and / or telephonic conversation, the actual transaction can be concluded. In most such cases the buyer and seller will meet face to face only at the time of the final transaction.

Illustration: In March 2007, the Pune rural police cracked down on an illegal rave party and arrested hundreds of illegal drug users. The social networking site, Orkut.com, is believed to be one of the modes of communication for gathering people for the illegal "drug" party.

Modus Operandi: The suspect creates an email ID using fictitious details. He then posts messages, about the illegal products, in various chat rooms, bulletin boards, newsgroups etc. Potential customers can contact the seller using the email IDs provided.

Usual motive: Illegal financial gain.

Before 27 October, 2009	After 27 October, 2009
Information Technology Act	Information Technology Act
usually does not apply. Depending	usually does not apply. Depending
upon the illegal items being	upon the illegal items being
transacted in, the following may	transacted in, the following may
apply: Narcotic Drugs and	apply: Narcotic Drugs and
Psychotropic Substances Act, Arms	Psychotropic Substances Act, Arms
Act, Indian Penal Code, Wildlife	Act, Indian Penal Code, Wildlife
related laws etc	related laws etc

14. Use of Internet and Computers by Terrorists

Many terrorists are using virtual as well as physical storage media for hiding information and records of their illicit business. They also use emails and chat rooms to communicate with their counterparts around the globe.

Scenario:

The suspects carry laptops wherein information relating to their activities is stored in encrypted and password protected form. They also create email accounts using fictitious details. In many cases, one email account is shared by many people.

E.g. one terrorist composes an email and saves it in the draft folder. Another terrorist logs into the same account from another city / country and reads the saved email. He then composes his reply and saves it in the draft folder. The emails are not actually sent. This makes email tracking and tracing almost impossible.

Terrorists also use physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc. They also use virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, Gspace etc.

Modus Operandi: The terrorists purchase small storage devices with large data storage capacities. They also purchase and use encryption software. The terrorists may also use free or paid accounts with online storage providers.

Usual motives: Keeping terrorism related information confidential; securing communication amongst terrorist group members.

Before 27 October, 2009	After 27 October, 2009
Apart from conventional terrorism	Apart from conventional terrorism
laws, section 69 of the Information	laws, section 69 of the Information
<i>Technology Act</i> may apply	Technology Act may apply

15. Virus Attacks

Computer viruses are malicious programs that destroy electronic information. As the world is increasingly becoming networked, the threat and damage caused by viruses is growing by leaps and bounds.

Scenario 1:

The virus is a general "in the wild" virus. This means that it is spreading all over the world and is not targeted at any specific organization.

Modus Operandi: A skilled programmer creates a new type or strain of virus and releases it on the Internet so that it can spread all over the world. Being a new virus, it goes undetected by many anti-virus software and hence is able to spread all over the world and cause a lot of damage. Anti-virus companies are usually able to find a solution within 8 to 48 hours.

Usual motives: Thrill and a perverse pleasure in destroying data belonging to strangers.

Applicable law

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the	Sections 43, 66 & 66A of the
Information Technology Act and	Information Technology Act and
section 426 of Indian Penal Code	section 426 of Indian Penal Code

Scenario 2:

The virus targets a particular organization. This type of a virus is not known to anti-virus companies as it is a new virus created specifically to target a particular organization.

Modus Operandi: A skilled programmer creates a new type or strain of virus. He does not release it on the Internet. Instead, he sells it for a huge amount of money. The buyer uses the virus to target his rival company. Being a new virus, it may go undetected by the victim company's anti-virus software and hence would be able to cause a lot of damage. Anti-virus companies may never get to know about the existence of the virus.

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the	Sections 43, 66 & 66A of the
Information Technology Act and	Information Technology Act and
section 426 of Indian Penal Code	section 426 of Indian Penal Code

16. Web Defacement

Website defacement is usually the substitution of the original home page of a website with another page (usually pornographic or defamatory in nature) by a hacker.

Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs. Disturbing images and offensive phrases might be displayed in the process, as well as a signature of sorts, to show who was responsible for the defacement. Websites are not only defaced for political reasons, many defacers do it just for the thrill.

Scenario:

The homepage of a website is replaced with a pornographic or defamatory page. In case of Government websites, this is most commonly done on symbolic days (e.g. the Independence day of the country).

Modus Operandi: The defacer may exploit the vulnerabilities of the operating system or applications used to host the website. This will allow him to hack into the web server and change the home page and other pages.

Alternatively, he may launch a brute force or dictionary attack to obtain the administrator passwords for the website. He can then connect to the web server and change the webpages.

Usual motives: Thrill or a perverse pleasure in inciting communal disharmony.

Before 27 October, 2009	After 27 October, 2009
Sections 43 & 66 of the	Sections 43 & 66 of the
Information Technology Act and in	Information Technology Act and in
some cases sections 67 and 70 may	some cases sections 66F, 67 and 70
also apply	may also apply

ANNEXURE 7 – RELEVANT INDIAN CASES

Diebold Systems Pvt. Ltd vs. Commissioner of Commercial Taxes¹⁹³

1. The appellant is a public limited company engaged in the manufacture and supply of Automated Teller Machines (ATM's for short). In view of the configuration and for the purpose for which is put to use, the appellant company is of the view that the sale of ATM's is eligible to single point levy of tax under Sec 5(3)(a) of the Karnataka Sales Tax Act, 1957 (hereinafter for the sake of brevity referred to as 'Act, 1957'). However, in order to have the views of the department in this regard, in particular, the Advance Ruling Authority constituted by the Commissioner of Commercial Taxes in exercise of his powers under Section 4 of the Act, the appellant company had filed an application before the Advance Ruling Authority in Form 54 as provided under Rule 27-E (1) of the Karnataka Sales Tax Rules, 1957 ('Rules' for short), seeking clarification on the rate of tax applicable under the Act on sale of Automated Teller Machines.

2. In response to the notice of the hearing issued by the Advance Ruling Authority, Sri Mohan Mudkavi, learned Chartered Accountant along with the Vice-President of the Company had appeared before the Authority and represented the facts and also had produced the literature and description of the ATM's. The basic submission that was made was, ATM is a combination of a Computer and it runs on a processor and the purpose for which it is put to use, is to dispense with cash and therefore, had requested the Authority to classify ATM's as goods falling under Entry 20 of Part 'C' of the Second Schedule to the Act and not Electronic goods falling under Entry 4 of Part 'E' of Second Schedule to the Act.

3. The Advance Ruling Authority (Majority View) after referring to the dictionary meaning of the word "Automated Teller Machines" and the product literature produced by the appellant company, by their order No. CLR.CR. 6/2002-03 dated 1.10.2002 have clarified that ATM's can be classified under the caption "computer terminals" and therefore, ATM's would fall under Entry 20 (ii) (b) of Part 'C' of Second Schedule to the Act and the basic tax applicable is four percent.

¹⁹³ MANU/KA/0155/2005; ILR 2005 KAR 2210; [2006]144 STC 59 (Kar) 445

4. The Chairman of the Advance Ruling Authority has dissented from the majority view and has opined, that the goods in question would fit into the description of electronic goods, parts and accessories thereof and therefore, falls under Entry 4 of Part 'E' of the Second Schedule to the KST Act and the basic rate of tax applicable is 12%.

5. The Commissioner of Commercial Taxes being of the view, that the Authority for clarification and Advance Ruling, has erroneously classified ATM's as "computer terminals" and the basic rate of tax is at 4%, instead of classifying the product as electronic goods falling under Entry 4 of Part 'E' of the Second Schedule to the Act and liable to tax at 12% and thereby has caused prejudice to the interest of the revenue, had initiated suomotu revisional proceedings under Section 22-A(1) of the Act by issuing a show cause notice dated 2.9.2003, interalia directing the appellant company to show cause, why the order passed by the Authority for clarification and Advance Ruling vide order No. CLR.CR. 6/2002-03 dated 1.10.2002 should not be set aside and the 'goods' in question should not be treated as "electronic goods" falling under Entry 4 Part 'E' of Second Schedule to the Act liable to tax at 12%. After receipt of the show cause notice, the appellant company has filed its reply dated 16.9.2003, interalia requesting the Commissioner of Commercial Taxes to accept the order passed by the Advance Ruling Authority dated 1.10.2002 and to drop the proposal made in show cause notice dated 2.9.2003.

6. The Commissioner of Commercial Taxes, after considering the reply filed by the appellant company, has confirmed the proposal made by him in the show cause notice dated 2.9.2003, by his order dated 29.11.2003. The findings and the conclusions reached by the Commissioner of Commercial Taxes is as under:

"As stated by the dealer himself, ATM consists of apart from the other things, computer (i.e., mother board with processor), computer peripherals such as RAM, drives, Key board, monitor, mouse, etc., and also software. In common parlance or popular sense, ATM is a Teller Machine (that is, which disburses cash issues statement of account etc.,) which is automated with the aid of computer, computer peripherals, software and other devices. Technically as contended by the dealer it can be held to be a computer terminal. However, going by the principles of common parlance as applicable to interpretation of entries under the KST Act, it cannot be classified as computer terminal for the purpose of the KST Act when it is not specifically included in the entry relating to computer terminals. The Hon'ble Supreme Court in the case of Deputy Commissioner of Sales Taxes (Law), Board of Revenue (Taxes), Ernakulam v. GS. Pai and Company (reported in 45 STC 58) has held that 'while interpreting entries in the sales tax legislation, the words used in the entry must be construed not in any technical sense from the scientific point of view but as understood in common parlance'. Similar view has been taken by the Hon'ble Supreme Court and High Courts in may other cases."

7. Aggrieved by the aforesaid order passed by the Commissioner of Commercial Taxes in SMR CR No. 04/2003-04 dated 29.11.1993, the appellant company is before this Court in this appeal filed under Section 24(1) of the KST Act.

8. The question of law raised for our consideration and decision are as under.

"I. Whether the Commissioner of Commercial Taxes has power and authority under Section 22-A(2) of the Act, to revise an order of the Advance Ruling Authority passed under Section 4 of the Act?

II. Is ATM a computer and whether it would fall under Entry 20(i) of Part 'C of Second Schedule to the Act?"

9. At the time of hearing of the appeal, the learned Senior Counsel Sri K.P. Kumar, would submit that in view of the amendment made to the provisions of Section 4 of the Act and the corresponding amendment of the Rules, he would not press for an answer on the first question of law raised in the memorandum of appeal. In view of the submission made by the learned Senior Counsel, we need not consider and answer the first legal issue raised by the appellant company in the appeal for our consideration and decision.

10. To answer the second question of law raised, the entries which the authorities have considered to give their ruling requires to be noticed and therefore, they are extracted:

Entry 20 of Part 'C of the Second Schedule has amended by Karnataka Act No. 3/1998, which is given effect from 1.4.1998, is as under:

"20. (i) Computer of all	1.4.98 to 31.12.99	Four percent
kinds namely,-	1.1.2000 to 31.3.2001	Eight percent
main frame, mini,	1.4.01 to 31.5.03	Four percent
personal, micro	From 1.6.2003	Five percent

computers and the like and their parts		
(ii) Peripherals, that is to say		
 (a) All kinds of printers and their parts, namely,- Dot matrix, ink jet, laser, Line, line matrix and the Like 	1.4.98 to 31.12.99 1.1.00 to 31.3.02 1.4.02 to 31.5.03 From 1.6.2003	Four percent Eight percent Four percent Five percent
(b) Terminals, scanners, multi media kits, plotters, modem and their parts	1.4.98 to 31.12.99 1.1.00 to 31.3.02 1.4.02 to 31.5.03 From 1.6.2003	Four percent Eight parent Four percent Five percent
(iii) Computer consumables namely stationery, floppy disks, CD ROMs, DAT tapes, Printer ribbons, printer Cartridges and cartridge Tapes.	1.4.98 to 31.12.99 1.1.00 to 31 3.02 1.4.02 to 31.5.03 From 1.6.2003	Four percent Eight percent Four percent Five percent
(iv) Computer Cleaning Kit	1.4.99 to 31.12.99 1.100 to 31.3.02 1.4.02 to 31.5.03 From 1.6.2003	Four percent Eight percent Four percent Five percent
(v) Computer Software	1.4.01 to 31.5.03 From 1.6.2003	Four percent Five percent

11. Entry 4 of Part 'E' of the Second Schedule to the Act as amended by Karnataka Act 5/1996 with effect from 1.4.1996 reads as under:

"Entry 4: Electronic Goods and parts and accessories thereof other than those falling under any other entry of this Schedule.

(The basic rate of lax for the relevant assessment year was 32 percent)."

12. The primary question that requires to be considered and decided in this appeal is the rate of tax applicable on the sale of 'Automated Teller Machines under KST Act, 1957? Alternatively, whether the revising authority was justified in clarifying that ATM's would fall under Entry 4 of Part 'E' of Second Schedule to the Act and the basic rate of tax on the sale of ATM's is at 12%?

13. ATM's are not included under Entry 20 Part 'C of the Second Schedule to the Act. However, the appellant company is of the view that ATM is a combination of a computer and it runs on a processor and therefore, the 'goods' in question would fall under Entry 20(i) of Part 'C' of the Second Schedule to the Act, and not under Entry of Part 'E' of Second Schedule to the Act.

14. In order to resolve the controversy between the parties to the lis, we need to know what is ATM and how it works?

ATM is the acronym for Automated Teller Machine. This Machine has a data terminal with two input and four output devices. The ATM connects to and communicates with a host processor that is analogous to an Internet Service provider. Then as a way of supporting the Machine to the host processor, dial up or leased lines are used. With the dial up, the Machine would dial into the host processor, using a standard telephone line and modem. With the leased line, the Machine is connected through the host processor through what is called a four-wire, point to point, dedicated telephone line. The ATM docs not have many parts, There is a card reader, which is what captures a person's account information that is stored on the magnetic strip located on the back of the ATM/debit card. This information is actually used by the host processor in routing the transaction to the appropriate bank. Then in has a 'Key pad', which is used by the cardholder to tell the machine what type of transaction is needed. It has an 'electric eye' that is used for cash dispensing mechanism. In addition to the eye, the ATM has a 'sensor' that is capable of evaluating the thickness of each of the bills being dispensed.

15. The world's first ATM was installed in Enfield Town in the London Borough Enfield, London, on June 27, 1967 by Barclay's Bank. This instance of the invention is credited to John Shephered-Birron, although George Simjian registered patents in New York, JSA, in the 1930's and Don Wetzel and two other Engineers from Ducted registered a patent on June 4, 1973.

16. ATM's are found at banks, grocery stores, shopping racks, convenience stores and some times on the side of the road. They are used by the bank's customers to make cash withdrawal and check their account balances at any time without the need of human teller. Many ATM's also allow people to deposit cash or cheques, transfer money between their bank or even buy postage stamps. ATM's are known by a wide variety of names. Some of which are more common in certain countries than others. Examples include Automated Teller Machine, Automated Banking Machine, Bank Box, Cash Box, Cash Dispenser, Cash Point, Hole in the Wall, Mac Machine Mini Bank, MAC Machine, Robotic Teller, Tele Banco, Ugly Teller, etc.

17. The book on Computers, concepts and applications for users by Robert C. Nikenson has explained the configuration and its uses in the day-to-day affairs by banks, stores etc. According to the learned Author, an ATM is not a computer by itself. It is connected to a computer that performs the tasks requested by the person using the ATM._ The computer is connected electronically to many ATM's that may be located some distance from the computer.

18. In so far as its use is concerned, the learned Author says that when you use an ATM, you are using a computer. When you insert your card and press keys on the ATM, you are entering input into the computer. The computer process the input to perform the banking transactions you requested and you receive output in the form for a paper summary and cash. The computer is a multiple user computer, because different people use it through many ATM's at one time. When you use an ATM, you are using the computer to keep with your personal banking needs.

19. In modern ATM's customer's authenticate themselves by using a plastic card with a magnetic stripe, which encodes the customer's account number, and by entering a numeric pass-code called a PIN (Personal Identification Number) number, which in some cases, may be changed using a machine. Most ATM's are connected to authorisation of a transaction by the card user or authorising Institution via communications network.

20. Now we need to notice what is a "computer terminal", since the majority view of the Advance Ruling Authority is that ATM is a "computer terminal" and therefore, it would fall under Entry 20 (ii)(b) of Part 'C' of the Second Schedule to the Act.

21. In Columbia Encyclopedia, Sixth Edition, computer terminals are described as under:

A device that enables a computer to receive or deliver data. Computer terminals vary greatly depending on the format of the data they handle. For example, a simply early terminal comprises a typewriter keyboard for input and a typewriter-printing element for alpha-numeric output. A more recent variation includes the key board for input and a television screen to display the output. The screen can be Cathode-ray tube or a gas plasma panel, the later involving an Ionized Gas (sandwiched between glass layers) that glows to form dots which inturn, connect to form lines. Such displays can present a variety of output, ranging from simple alpha numeric to complex graphic images used as design tools by Architects and Engineers. Portable terminals frequently use liquid crystal displays because of their low power requirements. The terminals of pen-based computers use a stylus to input hand writing on the screen. Touch sensitive terminals accept input made by touching a pressure-sensitive panel in front of a menu displayed on the screen. Other familiar types of terminals include store checkout systems that deliver detailed printed receipts and use later scanners to read the bar codes on packages and automatic teller machines in banks.

22. Having noticed what is ATM and its use, and computer terminals, we intend to refer to the observations made by the Apex Court and the manner in which Schedule to the entries under the Statute requires to be interpreted in fiscal laws, since the revising authority has held while accepting that the ATM'S are technically can be held to be a 'computer terminal', however, by common parlance, it cannot be classified as computer terminal for the purpose of the Act. The Supreme Court in the case of TATA CONSULTANCY SERVICES v. STATE OF ANDHRA PRADESH AIR 2004 SCW 6583, has observed.

"61. We, in the case, are not concerned with the technical meaning of computer and computer programme as in a fiscal statute plain meaning rule is applied. (See Partington v. Attorney-General, (1869) LR 4 HL 100,p. 122)

62. In interpreting an expression used in a legal sense, the Courts are required to ascertain the precise connotation, which it possesses in law.

63. It is furthermore trite that a Court should not be overzealous in searching ambiguities or obsequies in words, which are plain. (See Inland Revenue Commissioner v. Rossminster Ltd. (1980) 1 All ER 80, p.90)

64. It is now well settled that when an expression is capable of more than one meaning, the Court would attempt to resolve that ambiguity in a manner consistent with the purpose of the provisions and with regard to the consequences of the alternative constructions. [See Clark & Tokeley Ltd. (t/a Spellbrook) v. Oakes [1998(4) All ER 353].

65. In Inland Revenue Commissioner v. Trustees of Sir John Aird's Settlement [1984] Ch 382, it is stated:

"....... Two methods of statutory interpretation have at times been adopted by the Court, One, sometimes called literalist, is to make a meticulous examination of the precise words used. The other sometimes called purposive, is to consider the object of the relevant provision in the light of the other provisions of the Actthe general intendment of the provisions. They are not mutually exclusive and both have their part to play even in the interpretation of a taxing statute."

23. The learned Senior Counsel Sri K.P. Kumar appearing for the appellant company, relying on the definition of computers' that finds a place in, would firstly contend that ATM's are nothing but computers and therefore, fits into the description of "computers of all kinds" that finds a place under Entry 20 (i) of Part 'C' of Second Schedule to the Act. The learned Senior Counsel did take all the pains to explain the configuration of ATM, and how it works, by referring to the dictionary meaning of the word "computers" and further, to explain the meaning of the words 'namely', 'and the like' and 'their parts', the learned Senior Counsel relies on the observations made by the Supreme Court in the case of INDIAN ALUMINIUM COMPANY LIMITED v. ASSISTANT

COMMISSIONER OF COMMERCIAL TAXES (APPEALS) AND ANR. [2001] 121 STC 510.

24. Nextly, the learned Senior Counsel would contend that the revisional authority can invoke his powers of revisions, only, if the order passed by his subordinate authority is not only erroneous but also prejudicial to the interest of the revenue and if two views are possible, the Commissioner in exercise of his supervisory jurisdiction normally should not interfere with the order passed by his subordinate authorities. In aid of his submissions, the learned Senior Counsel relies on the observations made by Gujarat High Court in the case of COMMISSIONER OF INCOME TAX v. ARVIND **JEWELLERS** MANU/GJ/0318/2002 [2003]259ITR502(Guj) and the observations made by the Punjab & Harvana High Court in the case of COMMISSIONER OF INCOME TAX v. MAX INDIA LTD., MANU/PH/0155/2004.

25. Sri Anand, learned Govt. Advocate would contend that ATM's arc electronic goods, may be operated with the assistance of computer technology in the common parlance theory, they cannot be construed as computers or their terminals. The learned Govt. Advocate has produced before us voluminous literature on computers, only to demonstrate that ATM's by no stretch of imagination could be construed either as computers or as a computer terminals and the Advance Ruling Authority was not justified in answering the clarification sought for by the appellant, that, ATM's are "computer terminals" and they can be fit into one of the sub-entries under Entry 20 Part 'C' of Second Schedule to the Act. In his view, the revisional authority was justified in concluding that ATM's are electronic goods.

26. Now the question that would arise for consideration and decision in this appeal is, is an ATM is a "computer" as contended by learned Senior Counsel or a "computer terminal" as classified by the Advance Ruling Authority (Majority view) in its order dated 1.10.2002? or is it "electronic goods" are classified by the Commissioner of Commercial Taxes in his order dated 29.11.2003, while revising the order passed by the Advance Ruling Authority?

27. The information Technology Act, 2000, is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly

referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government Agencies, etc.

In the dictionary clause of the Act, the meaning of the word "computer" is defined to mean any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network. The "computer network" means the interconnection of one or more computers through the use of satellite, microwave, terrestrial line, or other communication media and terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

28. The purpose and object of Information Technology Act, is to recognise the transactions carried out by means of electronic data interchange and other means of electronic communication. To suit the purpose and object of the Act, the Parliament has defined the expression "computer" by giving a very wide meaning, but at the same time, by using the expression "means" immediately after the words "computers", the Legislature intends to make it clear that the definition is exhaustive and no other meaning can be assigned to the expression than what is included in the definition.

29. The Schedule to an Act is very much part of fiscal enactment. It is enacted by the hand of the Legislature. The Schedule in an Act sets down things and objects and contains their names and descriptions. The expressions in the Schedule have no evocative function. They can neither enlarge nor cut down the meanings or articles or things specifically named in the list. Therefore, the enlarged definition of "computers" in the Information Technology Act cannot be made use of interpreting an Entry under fiscal legislation.

30. Entry 20 of Part 'C' of the Second Schedule to the Act firstly speaks of computers of all kinds namely, main frame, mini personal, micro computers, and the like and their parts. The question of law raised by the appellant before us is whether ATM is a computer and as such squarely falls under Entry 20 (i) Part 'C' of the Second Schedule to the Act,

though the Advance Ruling Authority on the request made by the appellant for clarification has opined, that ATM's are "terminals" and would fall under Entry 20 (ii) (b) of Part 'C' of the Second Schedule to the Act, Sri K.P. Kumar, learned Senior Counsel would submit that ATM's are "computers" in view of the words like "namely" and "and the like" in the Entry immediately after naming the commodity i.e. computer of all kinds. In aid of his submission, the learned Senior Counsel has relied on the observations made by the Supreme Court in the case of COMPANY **INDIA** ALUMINIUM LTD. v. ASSISTANT COMMISSIONER OF COMMERCIAL TAXES (APPEALS) AND ANR. [2001] 121 STC 510. The case was under the provisions of Entry Tax Act. The question before the Court was whether furnace oil is not liable to tax under Entry 11 of the First Schedule to the Karnataka Tax on Entry of Goods Act, 1979. The Entry which came up for consideration was "all petroleum products that is to say petrol, diesel, crude oil, lubricating oil, transformer oil, brake or clutch fluid, bitumen (asphalt) tar and others but excluding LPG, Kerosene and Naphtha for use in the manufacture of fertilizers". The Apex Court while interpreting the use of the words "and others" in the Entry has observed that the use of the words "and others" in the Entry refers to petroleum products other than those which are specifically mentioned therein. To arrive at this conclusion, the Court has noticed that the Legislature has specifically excluded from the Entry aviation fuel, liquid petroleum gas, kerosene and naphtha for use in the manufacture of fertilizers and if not for his exclusion, even those products could have been included in the expression "petroleum products" in view of the language employed in Entry 11 of the Act.

31. The observation made by the Apex Court in the aforesaid decision would not come to the assistance of the learned Senior Counsel for the appellant company in view of the language employed in Entry 20 (i) of Part 'C' of the Second Schedule to the Act. The first limb of the Entry speaks of all kinds of computers and immediately thereafter, the word 'namely' is used. It only indicates what is included in the previous term or alternatively, it can be said the word "namely" imports enumeration of what is comprised in the preceding clause. (See. STATE OF BOMBAY v. BOMBAY EDUCATION SOCIETY: [1955]1SCR568 . Then there is enumeration of the goods such as 'main frame, mini, personal, micro computers and the like'. The use of the word "and the like" is only to include computers, which are akin to, main frame, mini personal, micro computers. To consider whether an item falls within the meaning of an Entry of a Schedule to an Act, it has to be seen whether its qualities

would fall in any one of the entires or in any one of the items included under that Entry. In the present case, since ATM is not a computer by itself, it would not fall under Entry 20 (i) of Part 'C' of Second Schedule to the Act.

32. The Advance Ruling Authority (Majority View) has classified ATM's as 'terminals' falling under Entry 20 (ii) (b) of Part 'C' of the Second Schedule to the Act, since ATM machine is also understood as computer terminal in the commercial world. This view of the Advance Ruling Authority was not strongly supported by learned Senior Counsel, and a passing remark was made, that if it does not fall under Entry 20 (i) of Part 'C' of the Second Schedule to the Act, it can be brought under "terminal" as envisaged under Entry 20 (ii) (b) of Part 'C' of the Second Schedule to the Act.

33. Entry 20 (ii) of Part 'C' of Second Schedule to the Act speaks of "peripherals". The Entry is as under:

(ii) Peripherals that is to say,-

(a) All kinds of printers and their parts namely, dot matrix, ink jet, laser, line matrix and the like

(b) Terminals, scanners, multimedia kits, plotters, modem and their parts.

Immediately after the expression "peripherals", the Legislature has used the expression "that is to say, all kinds of printers and their parts and terminals, scanners, multi-media kits, plotters, modem and their parts".

The expression "that is to say" is the commencement of ancillary clause, which explains the meaning of the principal clause. This expression is explained by the Apex Court in the case of STATE OF TAMILNADU v. PYARELAL MALHOTRA: 1983(13)ELT1582(SC) and in that, the Court has observed that the expression "that is to say" is employed to make clear and fix the meaning of what is to be explained or defined. Such words are not used as a rule, to amplify the meaning while removing a possible doubt for which purpose the word 'includes' is generally employed. In unusual cases, depending upon the context of the words "that is to say", this expression may be followed by illustrative instances. The Supreme Court in the case of SAIT RIKHAJI FURTARNAL v. STATE OF A.P. 1991 Suppl. (I) SCC 2002 has observed that the expression "that is to say" is exhaustive and not illustrative. The meaning of the expression "peripheral equipment" is defined in the Illustrated Computer Dictionary (Donald D. Spencer -Third Edition) to mean input/output units and auxiliary storage units of a

computer system, attached by cables to the Central Processing Unit used to get data in the date out, and to act as a reservoir for large amounts of data that cannot be held in the Central Processing Unit at one time. The word "terminal" means key board/display or key board/printer device used to input programs and data to the computer and to receive the output from the computer.

The Legislature having introduced the phrase "peripherals" under subentry (ii) of Part 'C' of the Second Schedule to the Act, has defined the term by using the expression "that is to say". The definition must determine the application of the phrase. In our view, the context in which the expression "that is to say" is used in exhaustive and not illustrative. Therefore, since ATM's are not included under sub-entry 20 (ii) (b) of the Part 'C' of Second Schedule to the Act, by construction, it cannot be brought under that Entry.

34. Entry 4 of Part 'E' of the Second Schedule to the Act speaks of electronic goods, and its parts and accessories thereof other than those falling under any other Entry of the Second Schedule to the Act.

35. The word "Electronic" has been defined by Megraw-Hill in Dictionary of Scientific and Technical Terms (Second Edition), as pertaining to electron devices or to circuits or systems utilising electron devices, including electron lubes, magnetic amplifiers, transistors and other devices that do the work of electron tubes. The word 'electron' has been defined as a stable elementary particle with an indivisible charge of negative electricity, found in all atoms and acting as a carrier of electricity in solids.

36. With this back ground, let us come back to the findings and the conclusions reached by the regional authority to hold that ATM's cannot be considered as 'computer terminals' but can be considered only as 'electronic goods'. The regional authority had issued a notice dated 2.9.2003 under Section 22-A of the Act, proposing to revise the order passed by the Advance Ruling Authority and further proposing to classify ATM's as electronic goods, and liable to tax at a higher rate, on the ground that the Advance Ruling Authority has erroneously, classified ATM as computer and the same has caused prejudice to the interest of the revenue. A detailed reply had been filed by the appellant company, after receipt of the show cause notice, justifying the findings and the conclusion reached by the Authority for clarifications and Advance Rulings, and nowhere in the reply the appellant company had conceded

that ATM works on the principles of electronics and is commonly understood to be electronic goods. Why we have noticed the aforesaid statement is only because, the revisional authority while concluding and confirming the proposal made by him in the show cause notice, specifically observes this aspect of the matter to conclude his findings, apart from other reasons, that the ATM's are electronic goods. These passing observations made by the regional authority cannot be said that there is total non-application of mind by the authority, while holding that ATM's are electronic goods. Apart from noticing the so called concession made by the appellant/assessee, the revisional authority has assigned other reasons to support his conclusion and therefore, the stray observation made by the revisional authority can be just ignored, while considering the other findings and conclusions reached by the revisional authority.

37. In so far the order passed pursuant to his show cause notice, the regional authority firstly, observes that ATM's are not computers of all kinds, for the reason, that ATM's are not mentioned in any of the subentries of Entry 20 of Part 'C' of Second Schedule to the Act. Secondly, the entries in a Taxing Statutes requires to be construed not in their scientific or technical sense,-but as understood in common parlance or popular sense, Then the revisional authority goes on to observe that ATM consists of apart from other things, computer (i.e. Mother Board with the processor), computer peripherals, such as RAM, Drives, Key Board, Monitor, Mouse etc., and also software. In common parlance or popular sense, ATM is a Teller Machine (that is which disburses cash, issues statement of account, etc.) which is automated with the aid of computer, computer peripherals, software and other devices, and therefore, technically, as contended by the dealer, it can be held to be computer terminal. However, going by principles as applicable to be interpretation of entries under the KST Act, it cannot be classified as computer terminal for the purpose of the Act, when it is not specifically included in the entry relating to computer terminals.

38. The Supreme Court in several of its judgment has laid down the rule of interpretation for articles of daily use and commonly traded items, which are mentioned in the Taxing Statutes. The Rule is that if there is no definition in the Statute, we should follow for tax purposes the definition not of the dictionaries or of technical books but of commercial parlance i.e. the popular meaning. The intention of Legislature is, that in Taxing Statutes, when terms are used of common usage, it is the common man's understanding of the articles which prevails over the technical man's concept. The place of scientific definition based on technical books, technical literature, dictionaries, etc., is relevant. When the goods are technical, there is no market and so, no market parlance. At the same time, if the goods are not technical, the definition in the market parlance would apply. It only means, that if the goods are technical, common parlance or commercial parlance would not apply. Therefore, in our opinion, the revisional authority is firstly justified in observing that though technically goods in question may fall within the meaning of the expression "computer terminals", but in common parlance theory, they are not understood so.

39. An Automatic Teller Machine, in our view, is an electronic device, which allows a bank's customer to make cash withdrawals, and check their account balances at any time without the need of human teller, probably that most widely used means of "electronic funds transfer". From the literature and the books on computers produced before us, we are of the view, that ATM is not a computer by itself and it is connected to a computer that performs the tasks requested by the person using ATM's. The computer is connected electronically to many ATM's that may be located from some distance from the computer. In common parlance, it is understood as electronic device and therefore, the regional authority is justified in holding that ATM's are electronic goods and the levy of tax and the sale of ATM's requires to be made under Entity 4 of Part 'E' of Second Schedule to the Act.

40. The learned Senior Counsel, lastly contended that if two views are possible in understanding the nature of the commodity and the rate of tax applicable on the sale of such commodity, the revisional authority should not exercise his supervisory jurisdiction under Section 22-A of the Act. This is a well settled legal principle and there cannot be any dispute on this proposition of law. But at the same time, it requires to be kept in view that the revising authority is authorised under the Act to revise an order, which is erroneous and prejudicial to the interest of the revenue. What is erroneous and prejudicial to the interest of the revenue is explained by the Apex Court and this Court is several of its decisions. The repetition of this settled principle need not be made for the purpose of deciding this legal issue canvassed by learned Senior Counsel for the appellant company. 41. Section 22-A(2) of the Karnataka Sales Tax Act is amended with effect from 1.4.2002 and the amended provision authorises the Commissioner to invoke his suomotu revisional powers, when there is divergent opinion among the members of the Advance Ruling Authority, and if the majority opinion is erroneous and prejudicial to the interest of the revenue. That is what that has been done by the Commissioner in the present case. Therefore, in our opinion, there is no jurisdictional error committed by the Commissioner of Commercial Taxes invoking his powers under Section 22-A of the Act.

42. In the result, appeal fails and accordingly, it is rejected. In the facts and circumstances of the case, parties are directed to bear their own costs. Ordered accordingly.

P.R. Transport Agency Vs. Union of India¹⁹⁴

1. We have heard Sri Manish Goyal for the petitioner and Sri Madhur Prakash representing respondents No. 2 and 3 at length.

2. During the course of hearing Sri Madhur Prakash raised a preliminary objection regarding want of territorial jurisdiction on part of this Court to entertain and hear this writ petition. The objection of Sri Madhur Prakash can be divided into three parts :-

(1) No part of cause of action has arisen within the territory of U.P.

(2) No facts have been pleaded in the writ petition on the basis of which it can be said that any part of cause of action has arisen within the territory of U.P.

(3) The jurisdiction of this Court under Article 226 of the Constitution of India stands ousted in favour of the Jharkhand High Court under Clause 10.5 of the Tender Agreement, the relevant part of which reads that (any) 'dispute arising out of this scheme shall be subject to the jurisdiction of the Jharkhand High Court'.

3. On this objection, both the sides were granted time to examine the matter. From the petitioner's side, a (second) supplementary affidavit has been filed stating that district Chandauli ('in U.P.) is the principal place of business of the petitioner This averment in para 2 of the second supplementary affidavit of Rakesh Kumar Srivastava is sought to be corroborated by the copy of the registered partnership deed of the petitioner which has been enclosed as 1st Annexure to that affidavit. The said deed is dated 7.7.2000, and in it the principal place of business is at Chandauli and the only other place where the petitioner carries on business is Varanasi, which is also in the State of U.P.

4. Sri Madhur Prakash raised an objection that this second supplementary affidavit, from the side of the petitioner, should not be entertained or accepted by this Court because all the facts mentioned in this affidavit were within the knowledge of the petitioner at the time

¹⁹⁴ P.R. Transport Agency through its partner Sri Prabhakar Singh Vs. Respondent: Union of India (UOI) through Secretary, Ministry of Coal, Bharat Coking Coal Ltd. through its Chairman, Chief Sales Manager Road Sales, Bharat Coking Coal Ltd. and Metal and Scrap Trading Corporation Ltd. (MSTC Ltd.) through its Chairman cum Managing Director. AIR 2006 All 23; 2006(1) AWC 504; MANU/UP/1086/2005

when the writ petition was filed and there is no explanation from the petitioner's side why these facts were not mentioned in the writ petition as originally filed.

5. Having considered the matter, we are unable to sustain this objection. This kind of objection is available either in cases of review under Order 47 Rule 1 (a) or in cases of additional evidence in appeal under Order 41 Rule 27(1)(aa) of the Code of Civil Procedure or in suits for specific performance of contracts where the pleadings of 'readiness and willingness' required under Section 16(1)(c) of the Specific Relief Act has not been made originally in the plaint and is sought to be added by amendment of the plaint. Apart from the above three cases, we are not aware of any other principle of law which permits exception to be taken to narration of additional facts by way of amendment application or by way of supplementary affidavit in a writ petition

6. The contention of the petitioner with regard to territorial jurisdiction is that because the communication of the acceptance of the tender was received by the petitioner by e-mail at Chandauli (U.P.), therefore, the contract from which this dispute arises was completed at Chandauli and in a case seeking performance of the contract or alleging breach of the contract by the respondents, the completion of the contract is a part of the "cause of action". There the place where the contract was completed by receipt of communication of acceptance is a place where 'part of cause of action' arises.

7. According to Halsbury's laws of England 4th Edition Re-issue Vol. 9(1) Paragraph 683 Page-434, 435 it has been said in reference to contracts made orally as by telephone, or in writing as by telex or fax, that the contract is complete when and where the acceptance is received. However, those principles can apply only where the transmitting terminal and the receiving terminal are at fixed points. In case of e-mail, the data (in this case acceptance) can be transmitted from any where by the e-mail account holder, it goes to the memory of a 'server' which may be located anywhere and can be retrieved by the addressee account holder from anywhere in the world and, therefore, there is no fixed point either of transmission or of receipt.

8. Anticipating the difficulties likely to arise from this, the Information Technology Act, 2000 in Section 13(3) provides as follows :-

"(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business."

9. Thus, the acceptance of the tender, communicated by the respondents to the petitioner by e-mail, will be deemed to be received by the petitioner at Varanasi/Chandauli, which are the only two places where the petitioner has his place of business.

10. In view of the facts mentioned in the supplementary affidavit, read with Information Technology Act, the acceptance having been received by the petitioner at Chandauli/Varanasi, the contract became complete by receipt of such acceptance at Varanasi/Chandauli, both of which places are within the territorial jurisdiction of this Court. Therefore, a part of the cause of action having arisen in U.P., this Court has territorial jurisdiction to entertain the writ petition. However, it has to be examined whether the "ouster' Clause (No. 10.5) of the tender agreement has the effect of excluding the writ jurisdiction of this Court.

11. Jurisdiction of civil courts is created by statute and cannot be created or conferred by the consent of the parties upon a court which has not been granted territorial or pecuniary or other (subject matter related) jurisdiction by statute.

12. Under Section 28 of the Indian Contract Act, 1872, the parties by their agreement are not permitted to totally exclude the jurisdiction of civil courts which has been created by statute However, where several civil courts have territorial jurisdiction in respect of a suit, parties may by agreement confine themselves to any one or more of such civil courts and such an agreement would not be violative of Section 28 of the Contract Act.

13. The above principles apply to civil suits and civil courts.

14. Generally, the courts are reluctant to accept ouster of the jurisdiction of the civil courts and, therefore, ouster clauses in agreement are construed strictly and jurisdiction is field to be excluded only when it is inevitable result of the agreement. In this light the Supreme-Court in the case of A.B.C. Laminart Pvt. Ltd and Anr. v. A.P. Agencies, MANU/SC/0001/1989 : [1989]2SCR1a laid down that either the agreement ousting jurisdiction of some courts and confining the jurisdiction to one or more courts should use the words like 'alone', 'only', 'exclusive' etc. in the ouster clause with regard to the courts to which jurisdiction has been confined; or in the alternative where such isolating words have not been used, the maxim 'expressio unius est exclusio allenus' meaning 'expression of one is the exclusion of another' may be applied in appropriate cases where the facts so demand.

15. After considering the facts of the said case as well as the alleged ouster clause which said "any dispute arising out of this sale-shall be subject to Kaira jurisdiction", the Supreme Court held that it would not oust the jurisdiction of other courts which had territorial jurisdiction under Section 20(c) of the Code of Civil Procedure.

16. But, more fundamental question needs to be examined, viz. whether the ouster clauses can exclude the jurisdiction of civil courts only or whether such clause can exclude the jurisdiction under Article 226 of the Constitution of India also-

17. Section 20 C.P.C. for the civil court and Article 226 of the Constitution of India for the High Courts permit the exercise of territorial jurisdiction where the cause of action wholly or in part arises within their territories. To that extent, the words used in the two provisions are similar.

18. But, there is one vital difference, namely, that while the jurisdiction to pass a decree accrues to the civil court only upon institution of suit by filing of a plaint and the civil court cannot act suo moto, but under Article 226 of the Constitution of India the power to issue writs, orders or directions is not necessarily dependant upon filing of a writ petition. The High Court has the power to act suo moto if an appropriate matter comes to its knowledge calling for intervention by it. Such knowledge may be received by the High Court by means of a writ petition or otherwise.

19. When the parties enter into an agreement confining themselves to the jurisdiction of one of the several civil courts having territorial

jurisdiction in respect of a suit, basically the parties are placing a restraint upon themselves from approaching the other civil courts whose jurisdiction has been excluded by the agreement. In this manner the jurisdiction of the other civil courts gets ousted, subject only to one restriction which is provided in Section 28 of the Contract Act, However, the power of judicial review given to the High Courts by Article 226 of the Constitution of India, and being a basic feature of the Constitution, cannot be curtailed even by statute, as held by the Supreme Court in the case of L. Chandra Kumar v. Union of India and Ors.: [1997]228ITR725(SC) . Therefore, it is not possible, to accept the contention that the said constitutional power of the High Court to issue a writ suo moto can be curtailed by an agreement between litigants,

20. We, therefore, hold that the ouster clauses can oust a territorial jurisdiction only of civil courts and not of the High Court in respect of however under Article 226 of the Constitution of India, provided such power exists in the High Court on account of part of cause of action having arisen with its territorial jurisdiction.

21. Coming to the merits of the matter, the case of the petitioner is that respondents no 2 and 3 held an e auction for certain coal in different lots. The petitioner submitted its tender or bid in the said auction and the petitioner's bid was accepted for 4000 metric tons of coal from Dobari Colliery at the price of Rs. 1,625/- per metric tons. The acceptance letter was issued on 19.7.2005 by e-mail at the petitioner's e-mail address. Acting upon the said acceptance, the petitioner deposited the full amount of Rs. 81,12,000/- through cheque in favour of respondent No. 3 on 28.7.2005. The cheque was accepted and encashed by respondent No. 3.

22. Subsequently, instead of delivering the coal to the petitioner, respondent No. 4 sent an e-mail dated 10.8.2005 to the petitioner saying that the sale as well as the e auction in favour of the petitioner stands cancelled "due to some technical and unavoidable reasons". This communication has been challenged in this writ petition and a copy of the same has been enclosed as Annexure 'I' to this writ petition.

23. On 13.9.2005, the following interim order was passed in this case :

"In the meantime, if 4000 metric ton of coal, for which the petitioner had submitted his bid at the e auction, has not been given to any body else, it

will not he transferred to any other person so that if the writ petition succeeds that coal may be directed to be delivered to the petitioner."

24. Sri Madhur Prakash, who had received copy of this writ petition on 29.8.2005 (i.e. almost a month ago) on behalf of respondents No. 2 and 3, has stated on instructions, that the only reason for this cancellation is that there was some other person whose bid for the same coal was slightly higher than the petitioner, but due to some flaw in the computer or its programme or feeding of data the said bid could not be considered.

25. We have considered this defence. The third party is not before us and there is no averment from the side of the petitioner or the respondents that the said third party has so far challenged the acceptance of the bid of the petitioner. In absence of such challenge, respondents No. 2, 3 and 4 are firstly bound by their concluded contract and thereafter they are further bound by the principle of promissory estoppel, in as much as the petitioner has altered its legal position to its disadvantage, acting upon the communication of acceptance sent to it by these respondents, by depositing large amount of money, viz. Rs. 81,12,000/- by cheque which has also been encashed by the respondents.

26. There can be no doubt that the respondents are 'State' within the meaning of Article 12 of the Constitution of India and the cancellation of the auction and the contract of sale in favour of the petitioner at such a highly belated stage, without giving any opportunity of hearing to the petitioner, is violative of the principles of natural justice and on that ground also it cannot be sustained.

27. In view of what has been stated above, we allow the writ petition; set aside the communication dated 10.8.2005 (Annexure 'I' to the writ petition) as well as the decision contained in that communication, and direct respondents No. 2 and 3 to handover the coal, covered by the petitioner's accepted bid, to the petitioner without further delay.

28. As requested, certified copies of this order may be issued to, the parties, on payment of requisite charges, within a week.

Firos Vs. State of Kerala¹⁹⁵

1. Appellant/petitioner approached this Court for declaring that Section 70 of the Information Technology Act, 2000 (hereinafter referred to as 'the Act') is unconstitutional and unenforceable and also for issuance of a writ of certiorari to quash Ext.P10 notification issued by the Government of Kerala under Sub-section (1) of Section 70 of the Act (Central Act No. 21 of 2000). According to the appellant, while disposing of the Writ Petition, the learned single Judge did not enter into any finding regarding the constitutional validity of Section 70 of the Act though it upheld ExtP10 notification issued by the State Government. The learned single Judge also directed to withdraw the suit for declaration of copyright and for injunction filed against the petitioner though the learned single Judge held that the suit is maintainable. The court also directed respondents 1 to 4 to withdraw the criminal complaint filed against the petitioner if the petitioner accepts the judgment and informs the same to the second respondent in writing within a period of one year from the date of judgment. The petitioner did not accept the judgment, but, challenged the same before this Court.

2. The facts of this case are as follows: Government of Kerala, as part of IT implementation in Government departments, conceived a project idea of "FRIENDS" (Fast, Reliable, Instant, Efficient Network for Disbursement of Services). The project envisaged is development of a software for single window collection of bills payable to Government, local authorities, various statutory agencies, Government Corporations etc. towards tax, fees, charges for electricity, water, etc. A person by making a consolidated payment in a computer counter served through "FRIENDS" system can discharge all his liabilities due to the Government, local authorities and various agencies. The first respondent Kerala State Government entrusted the work of developing the "FRIENDS" software with the fourth respondent. Fourth respondent is a registered society under the control of Government as the Total Solution Provider (TSP). The fourth respondent, in turn, entrusted the work of development of pilot project to be set up at Thiruvananthapuram to the petitioner. The application-software "FRIENDS" was first established at Thiruvananthapuram, free of cost, and since the project was successful, Government decided to set up the same in all other 13 district centres. By Ext.P6, fourth respondent entered contract with the petitioner for setting

¹⁹⁵ AIR 2006 Ker 279; 2006(3) KLT 210; 2007(34) PTC 98(Ker); MANU / KE / 0181 / 2006

up and commissioning "FRIENDS" software system in 13 centres all over Kerala for providing integrated services to the customers through a single window for a total consideration of Rs. 13 lakhs. Pursuant to Ext.P6 agreement, petitioner set up FRIENDS service centres in all the 13 centres and they were paid the agreed remuneration. After successful completion of the project, there was a subsequent agreement between the fourth respondent and the petitioner (Ext.P9 for continued technical support and for maintenance of system) : Extended period was over. Disputes arose between the petitioner and Government with regard to Intellectual Property Right (IPR) in the software developed, namely, FRIENDS. There is no dispute that IPR software is recognised in law that copyright can be claimed for IPR in the software in view of the amendment in the Copyright Act, 1957 in 1994. When respondents 1 to 4 arranged to modify the software "FRIENDS" to suit its further requirements through another agency, petitioner alleged violation of copyright and petitioner filed criminal complaint against respondents 1 to 4 which was later referred. A counter case was filed by the State and fourth respondent against the petitioner and charge sheet was issued and a crime was registered as Crime No. 119 of 2003 and is pending before the Additional Chief Judicial Magistrate's Court, Thiruvananthapuram. Petitioner filed an application for copyright before the Registrar of Copyright and the first respondent filed a suit before the District Court, Thiruvananthapuram under Sections 60 and 61 of the Copyright Act against the petitioner alleging infringement of copyright and for declaration and injunction. Since the suit is pending in the civil court, the Registrar of Copyright left the matter to be decided by the civil court and rejected petitioner's application for registration of copyright in the "FRIENDS" software applied for by him leaving freedom to any party to apply for registration of copyright after the civil court decides the issue. First respondent, State of Kerala, also issued separate notification, Ext.P10, under Section 70 of the Act declaring, among other items, that the "FRIENDS" software installed in the computer system and computer network established in all centres in Kerala as a 'protected system' for the purpose of the said Act. It is true that the criminal case against the petitioner is pending before the Chief Judicial Magistrate's Court, Thiruvananthapuram and suit filed by the first respondent against the petitioner is pending in the District Court, Thiruvananthapuram. This Writ Petition was filed challenging Section 70 of the Act. It is also contended that Ext.P10 circular issued is arbitrary, discriminatory and violative of Article 19(1)(g) of the Constitution of India and against the statutory right conferred under Section 17 of the Copyright Act.

3. Before going into the contentions raised, we may extract Section 70 of the Information Technology Act, 2000 as follows:

70. Protected system:

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

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised 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.

It is the main contention of the petitioner that the computer programme "FRIENDS" is a literary work as defined under Section 2(0) of the Copyright Act and he, being its creator, is the author as defined under Section 2(d)(vi) and, therefore, he is entitled to registration of copyright. According to him, his application for registration is presently rejected on account of the pendency of the suit in the civil court and ultimately he is entitled to registration of copyright under the Act. According to the petitioner, Section 70 of the Act which confers the unfettered powers on the State Government to declare any computer system as a protected system is arbitrary and unconstitutional and inconsistent with Copyright Act and Section 70 of the Act has to be declared as illegal. The alternative contention of the petitioner is that Government should have declared it as a protected system only after obtaining declaratory decree from the civil court. In the writ petition as well as in the writ appeal even though petitioner challenged Section 70 of the Information Technology Act as unconstitutional, serious contention was regarding Ext.P10 and not regarding the validity of Section 70 of the Act. According to the petitioner, there is direct conflict between the provisions of Section 17 of the Copyright Act and Section 70 of the Information Technology Act. When there is conflict between the two Acts, it is well settled law that a harmonious construction has to be adopted. Further, Information Technology Act is a comprehensive legislation with regard to Information Technology Act and its provisions. The provisions of the same will be binding especially considering Section 81 of the Act which provides as follows:

81. Act to have overriding effect. The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

But, as far as the Copyright Act is concerned, it is a comprehensive special Act and it is a comprehensive legislation regarding the law relating to Copyrights in India. Therefore, as far as copyright in respect of information technology is concerned, it has to be considered with reference to the provisions of the Copyright Act and as rightly held by the learned single Judge Section 70 of the Information Technology Act is directly related to Sections 2(k) and 17(d) of the Copyright Act and Government's authority to notify the system as a protected system applies only to such of the system of "Government work". Description of Government work is defined under Section 2(k) of the Copyright Act on which Government is confirmed copyright under Section 17 (d). The learned single Judge held as follows:

... Therefore while the IT Act deals with all matters pertaining to information technology, copyright in respect of information technology has to be considered with reference to the provisions of the Copyright Act and in this regard the contention of the petitioner, in principle has to be upheld. I feel the petitioner's contention is relevant only when Section 70 is taken in insolation, and if the Government proceeds to declare any computer system or network other than "Government work" as protected. I am of the view that Section 70 of the IT Act is directly related to Sections 2(k) and 17(d) of the Copyright Act and Government's authority to notify any system as protected applies only to such of the system which answers the description of "Government work" as defined in Section 2(k) of the Copyright Act, on which Govt. is conferred copyright under Section 17(d). In other words, a notification under Section 70 of the IT Act is a declaration of copyright under Section 17(d) of the Copyright Act which applies only to "Government work" within the meaning of Section 2(k) of the said Act. Since the apparent conflict between the provisions of both the statutes can be resolved by adopting the interpretation that a "Government work" as defined under Section 2(k) of the Copyright Act on which Government has copyright under Section 17(d) of the said Act only can be declared by Government as a "protected system" under Section 70 of the IT Act, the challenge against Section 70 as against the provisions of the Copyright Act does not survive and is only to be rejected. In other words, Section 70 of the IT Act is not against but subject to the provisions of the Copyright Act and Government cannot unilaterally declare any system as "protected" other than "Government work" falling under Section 2(k) of the Copyright Act on which Govt.'s copyright is recognised under Section 17(d) of the said

Act. However, if the Government proceeds to declare any other computer system or network under Section 70 of the IT Act as a protected system, it will be open to the aggrieved party to challenge such action as arbitrary and unauthorised. So long as the authority of the Government under Section 70 of the IT Act is to declare only "Government work" as defined under Section 2(k) of the Copyright Act as "protected system" the challenge against the validity of the section will not stand and the mere possibility of the Government exceeding it's powers is no ground to declare statutory provision unconstitutional. Hence this contention is rejected.

We agree with the above observations.

4. Section 2(k) of the Copyright Act deals with the Government work as follows:

(k) 'Government work' means a work which is made or published by or under the direction or control of -

(i) the Government or any department of the Government;

(ii) any Legislature in India;

(iii) any Court, Tribunal or other judicial authority in India;

Section 17(d) of the Copyright Act is as follows:

17. First owner of copyright:- Subject to the provisions of this Act, the author of a work shall be the owner of the copyright therein;

XXX XXX XXX

(d) in the case of a Government work, Government shall, in the absence of any agreement to the contrary, be the first owner of the copyright therein;

There is a statutory presumption in favour of every enactment and apart from a vague statement that Section 70 of the Information Technology Act is unconstitutional, petitioner was not able to show it is unconstitutional. Legislative power of Parliament is not questioned by the petitioner in enacting Section 70. When virus of an enactment or section is challenged alleging conflict with the provision in another Act, the conflict should be resolved as far as possible in favour of the legislature putting the most liberal construction and looking at the substance of the legislation by using the principle of harmonious construction. (See: Diamond Sugar Mills v. State of U.P. AIR 1962 SC 652 at 655) and Peerless General Finance and Investment Co. Ltd. and

Anr. v. Reserve Bank of India and Ors.: 1991CriLJ1391). When there is conflict between the provisions of two Acts, court has to construe the provisions in such a way to avoid a 'head on clash' and a harmonious construction should be adopted to resolve the conflict (See: Jogendra Lal Saha v. Stale of Bihar and Ors.: AIR1991SC1148). A harmonious construction of Copyright Act and Information Technology Act is necessary and questions regarding the 'copyrights' for the computer system, electronic devices and other works under the Information Technology Act are covered by the Copyright Act. Copyright (Amendment) Act, 1999 shows that copyrights with regard to the data work, data basis, computer work etc. are specifically covered under the Copyright Act. All matters connected with copyright can be resolved by the provisions in the Copyright Act as it is a special Act for that purpose and matters regarding information technology have to be resolved by applying the provisions of the Information Technology Act as t is a special Act for that purpose. There is no conflict between the provisions of Copyright Act and Section 70 of Information Technology Act. Hence, we are of the opinion that there is no merit in the challenge made in Section 70 of the Information Technology Act.

5. The next question to be considered is whether Ext.P10 notification issued by the Government is liable to be set aside and can Government declare "FRIENDS" application software as a protected system? To decide that question whether petitioner has got a copyright of "FRIENDS" software or whether it is a Government work within the meaning of Section 2(k) of the Copyright Act, this Court declared to decide the matter on merits in O.P. 33536 of 2002 by the District Court, Thiruvananthapuram. We are of the opinion that Ext.P10 could be issued by the Government without registration of the copyright and even without a declaration of copyright by the civil court under Section 60 of the Copyright Act. If any party claims that he has got a copyright and the Government cannot declare it as a protected system, it is for him to go to the civil court and get an injunction and also get a declaration that he has got a copyright of the property. It is settled position that no registration is required to claim copyright under the Copyright Act and non-registration under the Copyright Act does not bar action for infringement. The learned single Judge rightly held as follows:

...A Division Bench of this Court in Kumari Kanaka v. Sundararajan 1972 KLR 536 held that registration of the work under the Copyright is not compulsory, nor is it a condition precedent for maintaining a suit for damages or for injunction against infringement of copyright. Similar is the view taken by the Madras High Court in Manojah Cine Productions

v. Sundaresan AIR 1976 Mad. 22 and by the Allahabad High Court in Nav Sahitya Prakash v. Anand Kumar MANU/UP/0177/1981 : AIR1981All200 . Therefore, if the "FRIENDS" software is a "Government work" as defined under Section 2(k) of the Copyright Act, then by virtue of Section 17(d) of the said Act, the Government is entitled to notify it under Section 70 of the IT Act as a protected system without any prior registration under the Copyright Act. There is nothing to indicate in Section 70 of the IT Act that the Government. should get any declaratory decree of copyright from District Court under Section 60 of the Copyright Act before issuing notification declaring a computer system as protected. Sections 60 and 61 of the Copyright Act are only remedial measures available to an aggrieved party. While Government is free to issue notification under Section 70 of the IT Act without any registration of copyright or without obtaining any declaratory decree of copyright from District Court under Section 60 of the Act, it was open to the petitioner to challenge Ext.P10 by filing a suit under sections 60 and 61 of the Copyright Act, Though the petitioner is defending the suit, it will not be permissible for the petitioner as defendant to challenge Ext.P10 in the pending suit filed by the State.

Admittedly, petitioner did not file any suit. Petitioner was free to file a suit under Sections 60 and 61 of the Limitation Act wherein he could challenge Ext.P10 notification if it infringes his copyright. Sections 60 and 61 of the Copyright Act read as follows:

60. Remedy in the case of groundless threat of legal proceedings:- Where any person claiming to be the owner of copyright in any work, by circulars, advertisements or otherwise, threatens any other person with any legal proceedings or liability in respect of an alleged infringement of the copyright, any person aggrieved thereby may, notwithstanding anything contained in Section 34 of the Specific Relief Act, 1963 (47 of 1963), institute a declaratory suit that the alleged infringement to which the threats related was not in fact an infringement of any legal rights of the person making such threats and may in any such suit --

(a) obtain an injunction against the continuance of such threats; and

(b) recover such damages, if any as he has sustained by reason of such threats:

Provided that this section does not apply if the person making such threats, with due diligence, commences and prosecutes an action for infringement of the copyright claimed by him.

61. Owners of copyright to be party to the proceeding:

(1) In every Civil Suit or other proceeding regarding infringement of copyright instituted by an exclusive licensee, the owner of the copyright shall, unless the Court otherwise directs, be made a defendant and where such owner is made a defendant, he shall have the right to dispute the claim of the exclusive licensee.

(2) Where any Civil Suit or other proceeding regarding infringement of copyright instituted by an exclusive licensee is successful, no fresh suit or other proceeding in respect of the same cause of action shall lie at the instance of the owner of the copyright.

6. We agree with the learned single Judge that Ext.P10 is not an adjudicatory order under Chapter IX of the Information Technology Act to file an appeal to the Cyber Appellate Tribunal constituted under Chapter X of the Information Technology Act. It is true that under Ext.P6 agreement disputes between the parties could be settled by arbitration by second respondent in terms of clause 7 (2) of the said agreement. Petitioner has not chosen to avail such a remedy. Admittedly, petitioner did not file any suit and did not go for arbitration. The remedy of the petitioner was to file a suit or to refer the matter to arbitration instead of filing a writ petition. That was not done. Counsel for the petitioner insisted that since they have not filed any suit and writ petition was pending from about two years, the question whether "FRIENDS" software developed is a Government work and whether Government can issue Ext.P10 notification under Section 17(d) of the Copyright Act should be decided by this Court. Arguments were advanced by both sides to the point. The learned single Judge went through the contentions in detail and found after examining Exts.P1, 3, 6 and 9 that the software was developed for the Government and for the purpose of rendering services by the Government to the public. Even though Exts.P6 and 9 are executed with fourth respondent and Government is not directly a party, fourth respondent was only a Government agency and Government created the above agency as a total solution provider for developing softwares for the Government. Clause (10) of Ext.R4(b) reads as follows:

10. Departmental Task Force will monitor the actual implementation of the project vis-a-vis the milestones set by the TSP.

Intellectual Property Rights of the system developed by all the TSPs and Departments shall vest in the Government of Kerala. Government of Kerala will be free to deploy the same system or

with modification in any of the Government/Semi-Government/Quasi Government Departments/ Organisation.

Fourth respondent was bound by the above clause. Petitioner who understood technical support by executing agreement with fourth respondent is also bound by the above clause in Ext.R4(b). Government has decided itself to the IPR copyright in respect of "FRIENDS" software and there is no document or clause in the agreement to show that fourth respondent has assigned IPR right to the petitioner. The agreement was valid for a definite period and the petitioner was bound to give technical support during the currency of agreement. The software developed is for the sole purpose of collection of tax and amount payable to the various Government agencies through a single window. The learned single Judge held that it answers the definition of 'Government work' under Section 2(k). We agree with the learned single Judge.

7. It is contended by the learned Government Pleader that findings 7 and 8 were not warranted as when suit is maintainable, the court should not have directed to withdraw the suit, but, the question whether Government is entitled to publish Ext.PIO notification under Section 70 was decided by the learned single Judge himself and, therefore, a declaratory suit was not necessary. The learned single Judge also held that the petitioner is prohibited from claiming any right from "FRIENDS" software in view of Ext.PIO notification. Therefore, a further suit is unnecessary and, in any event, no appeal has been filed by the Government. We agree with the finding of the learned single Judge that Section 70 of the Information Technology Act is not unconstitutional, but, while interpreting Section 70 of the Information Technology Act, a harmonious construction with Copyright Act is needed and copyright of IT Government work is also protected under the Copyright Act and remedy provided under the Copyright Act can be availed by the parties, if their copyright is infringed even in respect of IT work. No grounds are made out by the petitioner to set aside Ext.P10 notification issued under Section 70 of the Information Technology Act in a petition under Article 226 of the Constitution of India. Therefore, the Writ Appeal is dismissed.

Avnish Bajaj Vs. State¹⁹⁶

1.1 Over three and a half years ago, an internet website carried a listing which offered for sale a video clip, shot on a mobile phone, of two children of a school in Delhi indulging in an explicitly sexual act. The petitioner, who was the Managing Director (MD) of the company that owned the website at the relevant point in time, asks this Court to annul his criminal prosecution for the offences of making available for sale and causing to be published an obscene product within the meaning of Section 292 Indian Penal Code (IPC) and Section 67 of the Information Technology Act 2000 (IT Act). This petition under Section 482 of the Code of Criminal Procedure 1973 ('CrPC') also raises questions concerning the criminal liability of directors for the offences attributable to a company, both under the IPC as well as the IT Act, particularly when such company is not arraigned as an accused.

1.2 Before discussing the background and the sequence of events leading to the filing of this petition, it is necessary to understand the context in which the issues arise for determination. The regulation of pornography on the internet has posed a serious challenge to governments and legislatures primarily on account of the nature of the medium. The easy availability, even to children, of pornographic material in digital form including video clips, its rapid transmission across the world wide web, and the absence of effective filters to screen out objectionable material from being accessed are factors that compound the challenge. It is said that "controlling pornography on the internet is problematic because we may not know from whom or from where the material originates, how many people are receiving the information, or if the material is crossing international boundaries." [See Robyn Forman Pollack, "Creating the Standards of a Global Community: Regulating Pornography on the Internet- an International Concern" 10 Temple International and Comparative Law Journal, (Fall, 1996) 467].

1.3 It is acknowledged that "the main concern of the legislators and parents in relation to the internet is child pornography, rather than other forms of sexually explicit content. This has been the case ever since paedophiles started to use the internet for circulating pornographic materials related to children." [See Yaman Akdeniz, "Cyber Rights, Protection and Markets: Article Governing Pornography and Child

¹⁹⁶ MANU/DE/0851/2008; 150(2008)DLT769

Pornography on the Internet: The UK Approach" 32 University of West Los Angeles Law Review 247 (2001)] Akdeniz points out that although in some countries there are arguments against proscription of pornography based on freedom of speech concerns, "there is general consensus that the line should be drawn with child pornography." These factors need to be borne in mind while examining the irreversible harm that can be caused by making available on the internet sexually explicit material that answers the description of child pornography.

Background facts

2.1 Baazee.com India Private Limited ('BIPL'), a wholly owned subsidiary of Ebay Inc. USA, and the owner of the website http://www.baazee.com, was during the relevant period in the process of being acquired by and consequently renamed as Ebay India Private Limited (EIPL). BIPL had its main office at Mumbai and another office in Delhi. During November to December 2004 the petitioner Avnish Bajaj was the MD of BIPL (which later was renamed as EIPL).

2.2 The website baazee.com provided an online platform or market where a seller and a buyer could interact. To be either a seller or buyer a person had to first register himself with baazee.com by filling out an online form giving details including the name, email id, date of birth (the age had to be 18 and above). The person registering had to choose an appropriate 'baazee ID' and a password which would be used every time the person logged on to the website baazee.com to transact either as a seller or a buyer. While registering, the applicant had to make a declaration to the following effect:

I have read the User agreement carefully - I am above 18 years of age. I have read and agreed to abide by the baazee.com user agreement...." The next stage in the registering process was reached after the person clicked on "Accept Terms & Submit". Thereafter an email was sent to the person by baazee.com in which a link was provided for activating the account. A person who registered following the above online procedure could either sell or buy products on the electronic market that baazee.com offered by using the baazee.com ID and password.

2.3 To be a seller a two-step process was envisaged. The first step was to get registered following the procedure described hereinbefore. The

second step was to "create a listing." Again several steps were to be followed. First the seller would select a category and sub-category that broadly classified the product proposed to be sold. Then the item details had to be specified. The website advised: "Enter the title that you would like to give your item in the text box provided. Give a title that describes your item best. Try to include specifications such as brand name, model number etc. The idea is to make your title most self explanatory and distinctive. Do not use web language (HTML)." The website also recommended that the seller should "always include an image that depicts your item correctly." The price and payment mode preferences were also to be indicated. Baazee.com also offered a mode of receiving payment under 'paisapay'. The user could also opt for other methods like cheques, demand drafts, cash on delivery etc.

2.4 When a user was listing an item for the first time on the site, a customer support representative had to verify his contact details (address and phone number) by calling up the user on the contact number given in the registration details. For an already registered user who wished to list some other item, there was an automated website filter which checked the item to identify whether it was a prohibited or restricted item. BIPL had a Safety and Trust Division which instituted word and text filters so that objectionable listings could be removed. A Community Watch Programme was also operational. If anyone brought to the notice of BIPL that any objectionable material was being listed, it would trigger a process by which the listing would be deactivated. Once the item was automatically screened by the filter, the listing was placed on the site with a unique computer generated item ID.

2.5 The buying process was fairly straightforward. The registered buyer had to find the item by using the Search box. He then had to browse the categories and sub-categories. After reading the item description, if the person intended to buy, he would click "buy now", select the payment method, specify the delivery details and confirm the order. This resulted in a purchase order being generated. Then came the question of payment through either the credit card or online bank transfer. If the buyer opted for a "paisapay" option and made an online payment, the normal banking payment gateway got attracted. Once the payment gateway confirmed the receipt of the payment then an automated payment confirmation was sent to the buyer. Thereafter the buyer received the item, depending on the product, through email, hand delivery, courier or post.

2.6 When buyers opted for the "paisapay" method, the system would once in a week calculate the amount payable to the listed user and send a file to the HDFC bank to issue a printed demand draft (DD) in the name of bank account number provided by the seller on www. baazee.com. The HDFC Bank would then dispatch the DD to the address provided by the seller. For facilitating this entire transaction BIPL received a commission which was usually a percentage of the selling price of the product.

The sequence of events

3.1 The sequence of events relevant to the present case unfolded thus. Ravi Raj, a fourth year student of the Indian Institute of Technology (IIT) Kharagpur, was registered as a seller with baazee.com since 21st July 2004. He had already been using the site for listing products for sale. His email ID was psell@sify.com.

3.2 In the evening of Saturday 27th November 2004, Ravi Raj placed on the baazee.com website a listing offering an MMS video clip for sale at Rs. 125 per piece. He adopted the seller's name as Alice Electronics and gave his address as 12-A/39, Roshpa Tower, Main Road, Malanche, Kharagpur. In order to avoid detection by the filters installed by baazee.com, Ravi Raj included the clip under the category Books and Magazines and sub-category 'e-books'. Although baazee.com did have a filter for some of the words which appear on the website, the listing nevertheless took place. For instance, the word "sex" at Seriall No. 23 of the list and word "sexual" at Seriall No. 70 of the list were definitely part of the suspected words.

3.3 The electronic website baazee.com when visited had the following item description on its site: "Item 27877408 - DPS Girls having fun!!! full video + Baazee points." The price was Rs. 125. Under the column "seller's details" the name indicated was: "alice elec" and Location: "Kharagpur". The seller was shown as a Member since 21st July 2004. Upon clicking on the item description, the listing read as under:

DPS Girls having fun!!! Do you want to see that video clip which has rocked the whole DELHI and now has become a hot point of discussion in the entire Nation?

YES, Then what are you waiting for!!!!

Just order for this product and it will be delivered to you within few hours.

This video is of a girl of DPS RK PURAM which has been filmed by his boyfriend in very sexual explicit conditions.

Please note: This video clip of around 2:30 Minutes and will be send to you as an email attachment.

3.4 The buyer interested in getting a copy had to click on the 'buy now' option, make a payment through credit card or 'paisa pay' option. The buyer had to pay Rs. 128 per clip which included a commission of Rs.3 that went to BIPL. This was deducted from the amount received from the buyer and the balance of Rs. 125 per clip was remitted to the seller by the HDFC bank. The seller, on receiving confirmation that payment had been made, would send the video clip by an email attachment by a zip file with the description 'dps_rkpuram-sex-scandle.zip'. Between around 8.30 pm in the evening of November 27th 2004 when the listing went on line till around 10 am on 29th November 2004 when the listing was deactivated, eight transactions of sale of the said video clip took place to buyers located in various parts of the country.

3.5 At around 8.20 pm on Saturday 27th November 2004 information was received on email from Amit Vohra using emailed threadsincp@sify.com for Community Watch. The mail titled "fraud report about item ID 27877408" read as under:

User's Message

The username of the party is alice-elec. This person is trying to sell a video which is illegal in India as it was shot on two people who are below the legal age of 18 & pornography is illegal in India. You need to sort this issue & you should even report it to the legal authorities as this can get your site in trouble.

3.6. This email was assigned to Namrata of BIPL at around 8.25pm on 27th November 2004 itself. At around 6:25pm on the next date i.e. 28th November 2004, which happened to be a Sunday, it was assigned to Swapna Sawant of the BIPL and the priority was shifted to the 'high alert' category.

3.7 On 29th November 2004 at 10:10am baazee.com wrote to Alice Electronics that it had noticed "that the listings put up on site by you are either obscene or pornographic in nature" and that the Baazee User Agreement prohibits trade in such items. It accordingly informed the seller "we have closed the item as it is against the User Agreement." Soon thereafter Swapna Sawant of BIPL addressed a letter next morning i.e. on Monday 29th November at 10:38 am to Amit Vohra thanking him for "spotting this and reporting to us at Community Watch that the Item ID: 27877408 is pornographic in nature. We have closed the items and have taken this issue up with the seller." The video clip was removed on 29th November 2004 Monday at around 10:38 am. Meanwhile eight persons with distinct IDs located in different parts of the country including Calcutta, Nellore, Pune, Delhi, Banglore and Chennai had purchased it.

3.8 On 9th December 2004 two events took place. The Crime Branch of Delhi police, on receiving credible information that the said MMS clip was sold for Rs. 125 by a website, registered FIR No. 645 of 2004. On the same day a news item appeared in a Delhi the newspaper "Today" with the headlines "DPS sex video at baazee.com". The news item by Anupam Thapa had the byline "Outrage Exclusive" and stated "online website goes ahead with the sale of the infamous clip". The news item stated: "India's biggest online trading portal baazee.com had listed the said MMS clip under the title 'DPS girls having fun' with the member ID of 27877408. The police upon investigation learnt that one Alice Electronics of Kharagpur West Bengal had since 27th November 2004 sold 8 copies of the said MMS clip."

3.9 The police sent notices under Section 91 CrPC to the petitioner and Sharat Digumarti, the Senior Manager, Trust and Safety, BIPL (who is Accused No. 3) and obtained information on the working of the website. On 10th December 2004 in response to a query addressed to baazee.com, Sharat Digumarti provided "the details of the seller (alice_elec) and the buyers who purchased this item." He stated that they had "already disabled the ability of the seller and the buyers in modifying their contact details and the attached file contains the contact details of these users which was taking from our database (File Name 'DPS Data') and also file (File Name: DPS Listing) which show the item that was listed on the site." 3.10 On 11th December 2004 the police seized the printout of an email containing two pages regarding email ID vishwa777@yahoo.com dated 27th November 2004 with the time as 17:58:26 which was the placement of the order and an email of the same date received at that very address from Ravi Raj the seller at with the time as 20:05:13 with the email attachment dps_rkpuram_sex_scandal.zip which is a zip file sent to the said email ID. The subject of the email was 'DPS Sex Scandal'. The third item seized was an Amkette floppy which had an email from the seller and confirmation email from baazee.com. Details of the email placement of the order and receipt of the product by each of the other buyers was also collected.

3.11 On 12 December 2004 Sharat Digumarti furnished the details of the payments received from the buyers and confirmed that a sum of Rs. 17,787.87 was disbursed to the seller 'alice_elec' through the HDFC Payment Services.

3.12 On 14th December 2004, the petitioner wrote to the police about his role and responsibility. Inter alias he stated that: "I am responsible for the India operations of the Company and my charges, assigns, includes policy decisions, planning, control and overall supervision of day to day functioning of the organization."

3.13 In his letter dated 14th December 2004 Sharat Digumarti explained the registration, buying and selling process and payment process at baazee.com. He enclosed a note on how the "list of the suspected and banned words" worked and the process of detection of leakage. He also gave details of the working of Community Watch. Thereafter a list of 120 words as on 14th December was attached. Although in the said list at Serial No. 106 the word "dps" and at Serial No. 110 the word "RKP" were included, these were admittedly added after the sale of the objectionable video clip came to light. The contents of the clip itself were therefore not under screening in the automated process since the clip itself was not on the baazee.com.

3.14 The Manager, Finance and paisapay of baazee.com wrote a detailed letter to the police giving information on how the said system works and gave a complete list of the transactions involving the video clip. This letter confirmed that Rs. 128 was charged per piece from each of the

buyers. Rs.3 rupees were paisapay charges and Rs. 125 went to the seller.

3.15 On 17th December 2004, Ravi Raj was arrested at Kharagpur and certain recoveries were effected from him including the CPU containing the hard disk of the computer from where the email attachments of the offending video clip were dispatched. The petitioner Avnish Bajaj was arrested in Mumbai on the same day. He was later released on bail by this Court on 21st December 2004. At the conclusion of the investigations, a charge sheet was filed showing Ravi Raj, Avnish Bajaj and Sharat Digumarti as Accused Nos. 1,2 and 3 respectively.

3.16 The learned Metropolitan Magistrate (MM) by an order dated 14th February 2006 took cognizance of the offences under Sections 292 and 294 IPC and Section 67IT Act. The three accused were summoned to face trial. Ravi Raj has since been absconding and his trial has been separated.

3.17 This petition was filed by Avnish Bajaj, the MD of BIPL (EIPL) seeking the quashing of the criminal proceedings on various grounds which will be discussed hereafter. During the pendency of this petition there has been a stay of the proceedings before the trial court.

Submissions of Counsel

4.1 Arguments on behalf of the petitioner were addressed by Mr. Arun Jaitley and Mr. Sidharth Luthra, Senior Advocates.

4.2 According to the petitioner, the case against BIPL is not, and cannot possibly be, in relation to the video clip since the clip itself was not made available on baazee. com. The video clip was transferred directly between the seller and buyer without the intervention of the website. While no submission was made in regard to the video clip being obscene, the submission of the petitioner was that at the highest BIPL was concerned only with the listing placed on the website which by itself was not obscene and did not attract the offence under Section 292/294 IPC or Section 67 IT Act.

4.3 It was then argued that in any event without BIPL (EIPL) being made an accused, no criminal liability attached to the petitioner for an IPC offence only because he happened to be the MD of BIPL (EIPL) at the relevant time. The revenue generated by the website was not profit as contemplated by Section 292 IPC and in any event such income was not generated by the petitioner but by BIPL which is not an accused in the case. Reasonable care was taken by the website to immediately remove the video clip once it was brought to its knowledge that it was objectionable. thereforee the website acted diligently and did not commit any illegality. The charge sheet when read as a whole does not make out even a prima facie case against the petitioner in his individual capacity for the offences under Sections 292/ 294 IPC.

4.4 In relation to Section 67IT Act, it was argued that in the absence of the company BIPL (EIPL) itself being made an accused, no liability could attach to the petitioner with the aid of Section 85IT Act. A reading of the charge sheet as a whole would show that although the petitioner as MD was in overall charge of the policy and planning of the business, he had no direct role in the placing of the listing or its filtering and subsequent removal. This was an automated process and the work of supervising the placing of listings on the website had been delegated to specific individuals like Accused No. 3 Sharat Digumarti. Criminal liability cannot be fastened lightly in the absence of a specific case being made out against the petitioner in his individual capacity, particularly since the company of which he was MD is not arraigned as an accused.

5.1 Appearing for the State, Ms. Mukta Gupta, learned Senior Standing Counsel submitted that the sequence of events, the listing, video clip and the role attributed to the petitioner, fully make out a case against the petitioner for the offences under Section 292 IPC and Section 67IT Act. The offence under Section 292 IPC includes not only overt acts but illegal omissions within the meaning of Sections 32, 35 and 36 IPC. The failure to have adequate filter in a system which is entirely automated, entails serious consequences and a website cannot escape such legal consequences.

5.2 It is further submitted by the learned Counsel for the State that the fact that website earned profits through the sale is evident from the bank statements which show that for each video clip it did earn a commission of Rs.3. The chain of events show that the website had a role to play in several of the stages before the video clip was sent by the seller to the

buyer by an email attachment. The fact that payment was made to the seller even as on 27th December 2004 shows that no attempt was made to prevent or stop the commission of the illegality by the website.

5.3 It was submitted by Ms. Gupta that the petitioner was the person incharge of the affairs of the company that owned the website and was responsible for its policy and planning. There is adequate material set out in the charge sheet which shows that the petitioner had a direct role in the matter. Notwithstanding that the BIPL itself is not arraigned as an accused, the petitioner can nevertheless be proceeded against for the role played by him in the transaction.

5.4 For the offence under Section 67, IT Act, it is not necessary that the company BIPL itself should be an accused. As explained in the judgments of the Supreme Court, what is relevant is whether at the trial a case for convicting the company for the offences had been made out. The present stage was premature to come to a conclusion either way. Even at a subsequent stage in the proceedings, the court can summon the company if sufficient material emerges against it.

5.5 Finally it was submitted that the crime is of an extremely grave nature and cannot go unpunished on technicalities. Even if the charge sheet does not contain specific allegations, the matter can still proceed to the next stages. At this stage the court is only to examine if a prima facie case is made out and on that test no interference is called for.

Are the offences under Sections 292 and 294 IPC and Section 67, IT Act attracted? 6.1 The question that first requires to be addressed is whether in the facts and circumstances of the case, as disclosed in the charge sheet, a prima facie case for offences under Sections 292 and 294 IPC and Section 67IT Act is made out. If the answer to this question is in the affirmative, the further question that arises is whether a prima facie case has been made out against the petitioner for those offences.

6.2 Section 292 IPC concerns the offence of sale of obscene materials and reads thus:

292. Sale, etc., of obscene books, etc.

(1) For the purposes of Sub-section (2), a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other

object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is. if taken as a whole, such as to tend to deprave and corrupt person, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it].

(2) Whoever-

(a) sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or

(b) imports, exports or conveys any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation, or

(c) takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

(d) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or

(e) offers or attempts to do any act which is an offence under this section, shall be punished on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand 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 five thousand rupees.

Exception.- ...

6.3 Section 292 is a deeming provision. If any "book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object" is "lascivious or appeals to the prurient interest" or "if taken as a whole is

such as to tend to deprave or corrupt person, who are likely to read, see or hear the matter contained or embodied in it", then such object "shall be deemed to be obscene." The law in this regard has been explained by the Supreme Court in Ranjit D. Udeshi v. State of Maharashtra: 1965CriLJ8, C.T. Prim v. State: AIR1961Cal177 and Samaresh Bose v. Amal Mitra: 1986CriLJ24.

6.4 In the present case, there are two pieces of material that call for scrutiny. One is the video clip and the other the listing on the website baazee.com. It was not argued by learned Counsel for the petitioner that the video clip in question did not even prima facie attract the definition of an obscene object within the meaning of Section 292(1) IPC. Also, it is a matter of record that a separate case has been instituted before the Juvenile Justice Board against the child involved in the act. As will be noticed hereafter, the listing itself suggested that even according to the seller the clip answered the description of child pornographic material.

6.5 To recall, the petitioner's submission was that BIPL and not the petitioner was, if at all, concerned with the listing on the website which by itself was not obscene. According to the petitioner, the video clip was transferred directly from the seller to the buyer without the intervention of the web site. The question then arises whether the listing even prima facie answers the definition of obscenity attracting Section 292(1) IPC.

6.6 The entire text of the listing has been set out earlier in para 3.3. Prima facie it appears that the listing itself answered the definition of obscenity since it contained words or writing that appealed "to the prurient interest" or if taken as a whole was "such as to tend to deprave or corrupt person, who are likely to read, see or hear the matter contained or embodied in it." The listing contained explicit words that left a person in no doubt that what was sought to be sold was lascivious. The words "This video is of a girl of DPS RK PURAM which has been filmed by his boyfriend in very sexual explicit conditions" are a prominent feature of the listing which invited a potential buyer to purchase the obscene object which was the video clip by projecting it as child pornography since the reference is to school children. Despite the arguments to the contrary of the learned Senior counsel for the petitioner, this Court is not able to agree with their submissions that the listing itself was not even prima facie an obscene material or text.

6.7 It was argued that even then, there was no overt act done by BIPL in relation to the video clip or listing, to even prima facie attract the offence under Section 292(2) IPC. This Court is unable to agree. As far as the listing is concerned, its contents were in the knowledge of BIPL the moment the listing was placed on the website by Ravi Raj. The offence under Section 292(2) (a) IPC gets attracted when the prosecution is able to prove that a person has "publicly exhibited or in any manner put into circulation" or "has in his possession" the obscene object. Even if Ravi Raj, and not BIPL, may have inserted the listing, the website of BIPL certainly "possessed" it. The website was easily accessible on the net and therefore the website also "publicly exhibited" the listing. It cannot be said therefore that in respect of the listing, Section 292(2) (a) IPC is not even prima facie attracted as far as BIPL is concerned.

6.8 In relation to the video clip, the wording of Section 292(2)(d) IPC is wide enough to include an attempt at making known "by any means whatsoever" that "such obscene object can be procured." The placing of an advertisement on the website informing the viewer that an obscene material or object is available for sale, one click away, is enough to attract the offence under Section 292(2)(d). The advertisement might itself have been inserted by the seller but the website facilitated the sale by carrying the listing which informed the potential buyer that such a video clip that is pornographic can be procured for a price. For instance, there could be a notice board in the premises of a club or association, on which is pasted a listing by one of the members offering for sale a pornographic film. It would not be open to the club/association to say that it in providing space on its notice board it is not by itself "making known" that an obscene object "can be procured from or through any person." Section 292(d) would be attracted in such a situation to fasten criminal liability on the club itself. If it is proved that a particular member was aware of the placing of such listing on the notice board such member would also be liable. Baazee.com here was using a public space in the form of a website that could be accessed by any internet user.

6.9 In relation to the essential ingredients of the offence of sale of or offer for sale of obscene products, reference was made to paras 10 and 11 of the judgment in Ranjit D. Udeshi which read thus:

10. Before dealing with that problem we wish to dispose of Mr. Garg's third argument that the prosecution must prove that the person who sells or keeps for sale any obscene object knows that

it is obscene, before he can be adjudged guilty. We do not accept this argument. The first sub-section of Section 292 (unlike some others which open with the words "whoever knowingly or negligently etc.") does not make knowledge of obscenity an ingredient of the offence. The prosecution need not prove something which the law does not burden it with. If knowledge were made a part of the guilty act (acts reus), and the law required the prosecution to prove it, it would place an almost impenetrable defense in the hands of offenders. Something much less than actual knowledge must therefore suffice. It is argued that the number of books these days is so large and their contents so varied that the question whether there is means era or not must be based on definite knowledge of the existence of obscenity. We can only interpret the law as we find it and if any exception is to be made it is for Parliament to enact a law. As we have pointed out, the difficulty of obtaining legal evidence of the offender's knowledge of the obscenity of the book etc., has made the liability strict. Under our law absence of such knowledge, may be taken in mitigation but it does not take the case out of the sub-section.

11. Next to consider is the second part of the guilty act (actus reus), namely, the selling or keeping for sale of an object which is found to be obscene. Here, of course, the ordinary guilty intention (mens rea) will be required before the offence can be said to be complete. The offender must have actually sold or kept for sale, the offending article. The circumstances of the case will then determine the criminal intent and it will be a matter of a proper inference from them. The argument that the prosecution must give positive evidence to establish a guilty intention involves a supposition that means read must always be established by the prosecution through positive evidence. In criminal prosecution means read must necessarily be proved by circumstantial evidence alone unless the accused confesses. The sub-section makes sale and possession for sale one of the elements of the offence. As sale has taken place and the appellant is a book-seller the necessary inference is readily drawn at least in this case. Difficulties may, however, arise in cases close to the border. To escape liability the appellant can prove his lack of knowledge unless the circumstances are such that he must be held guilty for the acts of another. The court will presume that he is guilty if the book is sold on his behalf and is later found to be obscene unless he can establish that the sale was without his knowledge or consent. The law against obscenity has always imposed a strict responsibility.

When Wilkes printed a dozen copies of his Essay on Woman for private circulation, the printer took an extra copy for himself. That copy was purchased from the printer and it brought Wilkes to grief before Lord Mansfield. The gist of the offence was taken to be publication-circulation and Wilkes was presumed to have circulated it. Of course, Wilkes published numerous other obscene and libellous writings in different ways and when Madame Pampadour asked him:

How far does the liberty of the Press extend in England?" he gave the characteristic answer: "I do not know. I am trying to find out !" (See 52 Harv. L. Rev. 40).

6.10 A reading of the above paragraphs shows that there are two elements to be satisfied in order to prove the offence under Section 292 IPC. The first is that the person accused of the offence had the knowledge that what was being offered for sale or exhibited or possessed was obscene. The second is that such person had the intention to commit any of the acts mentioned in Section 292(2) IPC. In Ranjit D. Udeshi it was held that the prosecution did not have to prove that the accused had knowledge that the contents of the books being offered for sale were in fact obscene since the deeming provision in Section 292(1) IPC stood attracted. However the prosecution was required to prove that the accused did intend to sell such obscene object.

6.11 Turning to the case on hand, the listing here was carried by the website baazee.com. The text of the listing leaves no doubt that the object being offered for sale was obscene. By not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was in fact obscene. These are the attendant risks that a website owner attracts when he exploits cyber space for profits. The proliferation of the internet and the possibility of a widespread use through instant transmission of pornographic material, calls for a strict standard having to be insisted upon. Owners or operators of websites that offer space for listings might have to employ content filters if they want to prove that they did not knowingly permit the use of their website for sale of pornographic material. Given the nature of the offence and the 'strict liability' envisaged by Section 292(1) IPC, even if for some reason the filters fail, the presumption that the owner of the website had the knowledge that the product being offered for sale was obscene would get attracted. This of course would be a rebuttable presumption. It would be open to the owner of the website to show that it took reasonable precaution to filter the listing for obscene material, this it was nevertheless placed on the website listed without its knowledge and that it took prompt corrective once it knew that the listing or the product offered for sale was obscene. But that would be a matter for evidence at the trial.

6.12 For the purposes of the present petition it is enough to examine if the offence under Section 292 IPC is prima facie attracted. This Court finds that it does as far as BIPL (EIPL) is concerned. It is therefore not necessary at this stage for this Court to examine if there is a valid defense available to BIPL or, whether, as contended by the prosecution, the offence would get attracted even on account of the illegal omissions of BIPL.

- 7.1 Next, we turn to Section 67 of the IT Act which reads as under:
 - Section 67-Publishing of information which is obscene 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 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.

7.2 The plain words of the above provision unambiguously state that the offence stands attracted when there is publishing, transmitting or where anyone "causes to be published in the electronic form" any material that 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." The remaining portion of the provision borrows the language of Section 292(2)(d) IPC. As far as the present case is concerned it has already been held that what was offered for sale through the listing and the listing itself were prima facie obscene.

7.3 The question for the purposes of Section 67 is whether the website caused the publishing of such obscene material. For this purpose, the chain of transactions is relevant. Once the interested buyer gets on to baazee.com and views the listing, he then opts to buy the said product and then makes payment. Only then the remaining part of the chain is complete and the product, which in this case is the video clip in electronic form, is then transmitted through an email attachment and then can get further transmitted from one person to another. The video clip sent as an email attachment can straightway be downloaded onto to the buyer's hard disc and numerous copies thereof can be made for further transmission. The 'publishing' in this form is thereforee instantaneous and can be repeated manifold. In fact in the present case, the transmission of the clip to eight buyers located in different parts of the country took place in a very short span of time.

7.4 Therefore, it cannot be said that baazee.com in this case did not even prima facie "cause" the publication of the obscene material. The ultimate transmission of the video clip might be through the seller to the buyer but in a fully automated system that limb of the transaction cannot take place unless all the previous steps of registration with the website and making payment take place. It is a continuous chain. When five to six links of the chain are under the direct control of the website and it is only on completion of each step that the final two steps which result in the actual publication of the obscene material ensue, it cannot be said that the website did not even prima facie cause publication of the obscene material.

8.1 As far as the offence under Section 294 is concerned, the learned Counsel for the prosecution did not dispute the contention of the learned Counsel for the petitioner that the said offence was not attracted in the facts of the case. A reference may nevertheless be made to the Section 294 IPC:

294. Obscene acts and songs

Whoever, to the annoyance of others--

(a) does any obscene act in any public place, or

(b) sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both. 8.2 It appears that Section 294 IPC deals only with doing obscene acts and singing or reciting or uttering obscene songs in a public place. It cannot be said that the website itself did an obscene act or performed any obscene song. The offence under Section 294 is not even attracted prima facie in the facts and circumstances of the present case.

9. To summarise this part of the discussion, this Court finds that a prima facie case for the offence under Section 292 IPC and Section 67IT Act is made out as far as the owner of the website baazee.com, i.e. the company BIPL (renamed as EIPL) is concerned. The offence under Section 294 IPC is not even prima facie attracted.

Is a prima facie case made out for the offences under Sections 292 IPC and 67 IT Act against the petitioner?

10. The question that arises next is whether a prima facie case for the offence under Section 292, IPC and Section 67, IT Act is made out against the petitioner. It has been argued by the learned Senior counsel for the petitioner that nowhere in the charge sheet is there any allegation that the petitioner himself facilitated the publishing of the obscene material or is in any way directly involved in the transaction.

11. It has been held that a prima facie case is indeed made out against BIPL. However, for some reason BIPL has not been arraigned as an accused. No satisfactory Explanationn has been offered by the prosecution except suggesting during the course of arguments that the law in regard to corporate criminal liability was not very clear. This is not an acceptable position in view of the clear position in the law as explained by the Supreme Court. The word 'person' is defined under Section 11 IPC to include "any Company or Association or body of persons, whether incorporated or not." therefore for an offence under the IPC there is no immunity granted to a company as such from prosecution. Even if, like in Section 292 IPC, the offence is punishable with imprisonment and fine, a company can still be arraigned and tried as an accused. Section 305 CrPC deals with the procedure that is to be followed when the accused is a company. A person will be nominated by such company to represent it during the trial. It may ultimately be punished only with fine (since most offences are punishable with fine in addition to imprisonment). This position in law has now been settled by the Constitution Bench of five judges of the Supreme Court Standard

Chartered v. Directorate of Enforcement: [2005]275ITR81(SC). Overruling an earlier decision of a three Judge Bench in Assistant Commissioner v. Velliappa Textiles: 2004CriLJ1221, the Constitution Bench by a 3:2 majority held that for an offence under the IPC or any other penal statute where the provision makes the offence punishable with imprisonment fine, a company can nevertheless be prosecuted. It was held (AIR, paras 7 and 8):

7. As in the case of torts, the general rule prevails that the corporation may be criminally liable for the acts of an officer or agent, assumed to be done by him when exercising authorized powers, and without proof that his act was expressly authorized or approved by the corporation. In the statutes defining crimes, the prohibition is frequently directed against any "person" who commits the prohibited act, and in many statutes the term "person" is defined. Even if the person is not specifically defined, it necessarily includes a corporation. It is usually construed to include a corporation so as to bring it within the prohibition of the statute and subject it to punishment. In most of the statutes, the word "person" is defined to include a corporation. In Section 11 of the Indian Penal Code, the "person" is defined thus:

The word "person" includes any Company or Association or body of persons, whether incorporated or not.

8. therefore, as regards corporate criminal liability, there is no doubt that a corporation or company could be prosecuted for any offence punishable under law, whether it is coming under the strict liability or under absolute liability.

12. Therefore, there was no legal bar in arraigning BIPL as an accused in the present case. It was then submitted by the State, on the strength of the decision of the Supreme Court in SWIL Ltd. v. State of Delhi: 2001CriLJ4173, that at a later point in time, even before passing an order on charge, the trial court can summon the company as an accused. Even if this were to happen, that still does not obviate the requirement in law for the prosecution to show that a prima facie case has been made out against the petitioner in his individual capacity for the IPC offence. While, as will be discussed hereafter, the position is different with regard to the offence under Section 67IT Act, as far as the offence under Section 292 IPC is concerned, the law as it presently stands does not envisage an automatic liability attaching to a Director for the offences committed by a company. therefore even if at a subsequent stage of the proceedings BIPL is summoned to face trial for the IPC offence, that

would not, in the absence of a specific case being made out against the petitioner in his individual capacity, result in his being an accused.

13. It requires to be noted that, unlike some other statutes containing penal provisions, the IPC does not incorporate the concept of criminal liability of a Director or an employee where the principal accused is a company. In other words, there is no provision similar to Section 141 of the Negotiable Instruments Act, 1881 ('NI Act') or Section 140 of the Customs Act, 1962 or Section 85 of the IT Act. These are provisions that provide for a deemed criminal liability of a person who, at the time of commission of the offence by the company, was in charge of the affairs of the company or responsible to it for the conduct of its business. The proviso to such provision makes it possible for such person to escape liability by proving at the stage of trial that the offence was committed by the company without his or her knowledge. therefore once the deemed criminal liability gets attracted under the substantive provision, the burden shifts to the accused under the proviso to rebut such presumption. However, there is no such provision in the IPC.

14. In Maksud Saiyed v. State of Gujarat: (2008)5SCC668, the Supreme Court explained that (SCALE p. 323):

13. Indian Penal Code does not contain any provision for attaching vicarious liability on the part of the Managing Director or the Directors of the Company when the accused is the Company. The learned Magistrate failed to pose unto himself the correct question viz. as to whether the complaint petition, even if given face value and taken to be correct in its entirety, would lead to the conclusion that the respondents herein were personally liable for any offence. The Bank is a body corporate. Vicarious liability of the Managing Director and Director would arise provided any provision exists in that behalf in the statute. Statutes indisputably must contain provision fixing such vicarious liabilities. Even for the said purpose, it is obligatory on the part of the complainant to make requisite allegations which would attract the provisions constituting vicarious liability.

15. Recently this position was reiterated in S.K. Alagh v. State of U.P.: 2008CriLJ2256 where the Supreme Court observed (SCALE p. 527):

16. Indian Penal Code, save and except some provisions specifically providing therefore, does not contemplate any vicarious liability on the part of a party who is not charged directly for commission of an offence.

18. As, admittedly, drafts were drawn in the name of the company, even if appellant was its Managing Director, he cannot be said to have committed an offence under Section 406 of the Indian Penal Code. If and when a statute contemplates creation of such a legal fiction, it provides specifically therefore. In absence of any provision laid down under the statute, a Director of a company or an employee cannot be held to be vicariously liable for any offence committed by the company itself. (See Sabitha Ramamurthy and Anr. v. R.B.S. Channabasavaradhya MANU/SC/8486/2006 : 2006CriLJ4602).

15. We may, in this regard, notice that the provisions of the Essential Commodities Act, Negotiable Instruments Act, Employees' Provident Fund (Miscellaneous Provision) Act, 1952 etc. have created such vicarious liability. It is interesting to note that Section 14A of the 1952 Act specifically creates an offence of criminal breach of trust in respect of the amount deducted from the employees by the company. In terms of the Explanations appended to Section 405 of the Indian Penal Code, a legal fiction has been created to the effect that the employer shall be deemed to have committed an offence of criminal breach of trust. Whereas a person in charge of the affairs of the company and in control thereof has been made vicariously liable for the offence committed by the company along with the company but even in a case falling under Section 406 of the Indian Penal Code vicarious liability has been held to be not extendable to the Directors or officers of the company. (See Maksud Saiyed v. State of Gujarat and Ors.).

16.1 Although the Supreme Court has termed the liability of a Director, where the company is the accused, as being 'vicarious', the classical understanding of the concept of vicarious liability is invariably in the context of a "master and servant" relationship. For instance, a company can be made vicariously liable for the criminal acts of its employees or directors. In an article by V.S.Khanna titled "Corporate Liability Standards: When should Corporations be held Criminally Liable" 37 Am. Crim. L. Rev. 1239 (2000) the concept is explained thus:

Corporate liability is a form of vicarious liability wherein the corporation is held liable for the wrongs of its agents. Vicarious liability is imposed on corporations under the doctrine of respondeat superior when an agent (1) commits a crime (2) within the scope of employment (3) with the intent to benefit the corporation.

(See also Thomas J. Bernard, "The Historical Development of Corporate Criminal Liability", 22 Criminology 3 1984)

16.2 Here we have a converse situation where the director is sought to be made liable for the criminal acts of the company. Nevertheless, what the above two decisions of the Supreme Court show is that as far as the IPC is concerned there is no automatic criminal liability of a director where the company is arraigned as an accused.

17. The absence of such a provision in the IPC could be viewed as a lacuna but is not to be lightly presumed as there have been numerous statutes enacted by Parliament thereafter which have incorporated such provisions. For instance, Section 85IT Act is similarly worded as Section 141NI Act and incorporates a deemed criminal liability of the director. The IT Act amends certain provisions of the IPC as well. But Parliament has chosen not to make any amendment to incorporate such a provision in the IPC. The Court has therefore to proceed with the law as it exists, particularly since it is a penal statute which admits of strict construction.

18. Does this mean that a Director or employee of a company can never be made an accused? The answer has to be in the negative. What it means is that if the prosecution seeks to make a Director or an employee of a Company, which is the principal accused, liable for an IPC offence, then it will have to make out a case against such person in his or her individual capacity. The precise role of the person concerned in the actions of the company which led to the offence will have to be proved.

19.1 Turning to the case on hand, it is urged by the prosecution that there are enough averments in the charge sheet to establish a prima facie case against the petitioner even in his individual capacity and not merely in his capacity as MD of BIPL. It is submitted that the charge sheet may not contain the precise words but when read as a whole does bring out the prima facie case against the petitioner not only in his designation a the MD of baazee.com but as an individual as well. In the written

submission filed by the State it is asserted that there are "specific averments explicitly describing the role of the petitioner in commission of the offence under Section 292 & 294 IPC and Section 67IT Act by his acts and illegal omissions...." It is further sought to be argued that the charge sheet cannot be complete or accurate thesis of the prosecution case. Reliance is placed on the decision of the Supreme Court in R.K. Administration Dalmia v Delhi MANU/SC/0110/1962 [1963]1SCR253. It is further submitted that "it is wrong to say that the petitioner was charge sheeted and cognizance was taken simply owing to his designation. The offence by the petitioner have been committed by him individually though acting in his capacity as the Managing Director of the company." Elsewhere in the written submission of the State it is averred as under:

It is wrong to suggest that the company merely facilitated the sale between the parties to the transaction while in fact the company was an indispensable ally for the completion of the transaction as is demonstrable from the flow chart.

19.2 The reference here is to a flow chart that the Court had asked the parties to produce which would show the chain of transactions from the stage of the registration of a seller to the ultimate delivery of the product to the buyer. Reliance has been placed by the prosecution on the judgment in Keshub Mahindra v. State of Madhya Pradesh MANU/SC/1236/1996 : (1996)6SCC129 and Sushil Ansal v. State MANU/DE/1267/2001 : 95(2002)DLT623 to contend that the liability for the IPC offences, where the company is the main accused would also be attached to the directors.

19.3 In order to appreciate these submissions the relevant paragraphs of the charge sheet may be noticed:

The user agreement, downloaded from the site and details seized from, Sharat Digumarti, indicates that arrangements arrived at between buyers and sellers are bipartite agreements with no responsibility of Baazee.com whatsoever. However, in this case Baazee.com acted as an agent of the seller as it had taken a commission on the sale. The clip was priced at Rs 125/- each, but billed at Rs. 128/- each with Rs3/- as commission per sale. This commission was credited to PaisaPay, a division of Baazee.com. The website Baazee.com had installed a program which runs SQL cron jobs or checks the written words place by the sellers against a set of banned and suspect words. The web portal is a public

domain and can be accessed and read by just anyone. The language of the advertisement placed on the website was quite explicit and left nothing for the reader to imagine. The website was committed to block off offending words through appropriate filters, as per Clause 1.12.4 Schedule 'C' Part II: Terms & Conditions of the ISP guidelines, issued by the Government of India, which clearly states therein that "The Licensee shall ensure that objectionable, obscene, unauthorized or any other content, messages or communications infringing copyright, Intellectual Property right and International and domestic Cyber Laws, in any form or inconsistent with the laws of India, are not carried in his network, the ISP should take all necessary measures to prevent it." However, in-spite of the filters having the word 'sexual' in its list, the program of Baazee.com failed to block off the offending advertisement. Further, in-spite of being categorically informed by one of the users' thread sincp@sify.com on 27.11.2004 at 8.20 p.m. the company, Baazee.com a 24 x 7 platform, failed to act to stop the sale, immediately. All through the day on 28.11.2004 the sale was going on unabated and it was finally closed on 29.11.04.

The language of the advertisement written down and represented by accused Ravi Raj, on the website clearly conveyed the meaning that school children were involved in explicit sexual act. Further the portal has charged and received commission on the sale of the offending clip. The portal knew of the illegality of the fact, as the same was blocked on 29.11.04 but still chose to profit form it by appropriating the commission, 15 days later. The investigation proves that Avnish Bajaj as the MD of Baazee.com as well as Sharat Digumarti as Head Fraud and Risk Control, had knowledge of the contravention, through the Community Watch scheme. In spite of being informed, the item was not blocked for 38 hours. 75% of all sales took place after the web portal was informed about it. The filters that were put up by the website were also grossly inadequate. In spite of the word 'sexual' (at Seriall number 70) the word 'dps' (at Seriall number 106) and word 'RKP' (at Seriall number 110) existing in the suspect list, their program was not able to detect and block the advertisement which carried the same word. Likewise words like Avnish Bajaj was the domain administrator and all policy decisions were made through him. In spite of the hue and cry made in the media about the issue, the policy makers for the website did not put the names like DPS, RKPuram on their watch list till after the case was registered.

After having gathered enough evidences to establish that the porn video film was listed for sale, that it was actually purchased by at least 8 buyers, that the clipping was delivered to 8 buyers as email attachment through Baazee.com, that payments were passed on to the accused Ravi Raj col. No. 4., after deducting due commissions, that in spite of being categorically informed by one of the users thread sincp@sify.com on 27.11.04 at 8.20 P.M. Baazee.com failed to act to stop the sale, immediately, but closed it only after 38 hours, accused Avnish Bajaj, CEO of Baazee.com mentioned in Col. No. 4 was arrested on 17.12.04.

Avnish Bajaj at the time, when the said porn clip was sold and brought through Baazee.com. was the Managing Director of the Company, Baazee.com India Ltd. He was in charge for the Indian operations of the Company and was responsible for policy decisions, planning, control and overall supervision of day to day functioning of the organization. The profile on checkdomain.com also listed Avnish Bajaj as the administrative contact of Baazee.com. The issue of sale of pornographic CDs involving of two adolescents was widely in the media in the first week of Nov. 2004. However no operative or policy changes were affected by the Company. Baazee.com to prevent the listing/display/sale of the same on the portal. Although, the accused company claimed that filters existed to block such objectionable materials, investigations revealed that the claims made by the company were a mere eyewash. The filters were found to be rudimentary, grossly inadequate and perfunctory. Various other interactive web portals like jeevansaathi.com, naukri.com etc. adopt various measures like delayed insertion and regular online monitoring. This even the established industry norms, to prevent offensive content from coming up on websites were totally ignored. The accused company was even alerted by a customer on 27.11.04 itself, but the site was de-listed as "closed" only after 38 hours. Even after being closed it remained lodged in the closed item list for the general public to access and see. The payments received were routed through PaisaPay, another division of Baazee.com facilitating online money transfer and a commission of Rs.3/- per sale transaction was charged. Although the site was closed on 29.11.04, payments received from the buyers were not blocked but sent to the seller on 3.12.04. Investigation proves that the MD of Baazee.com, who exercised control over the day to day

functioning of the organization did not exercise due diligence to prevent the listing of the said obscene and lascivious clipping. The investigation reveals that the policies and conduct of Baazee.com its MD was designed to increase sale and maximize profits. Safeguard of prevailing moral values and prurient interests of any person in particular and the society at large was not a pressing agenda. The investigations found that the policy makers of the company were negligent in dealing with the matter and failed to exercise due diligence.

19.4 The other relevant portions in the charge sheet are: "Further, subsequent to the registration and arrest in this case, the domain and the network contact information for the website Baazee.com had been changed from Baazee.com to ebay.com, the principal company, who now own the domain name Baazee.com, primarily to insulate the other Directors of the Company from criminal responsibilities. The domain servers were also relocated by the company to xxx.EBAYDNS.COM, USA.

Sharat Digumarti was the Senior Manager, Trust and Safety who was responsible for maintaining the subject and banned key word list and ensuring that no lascivious item is listed for sale on the website. Sharat Digumarti was responsible for ensuring that no banned and illegal items are traded on the website. However, he did not take appropriate measures to ensure that the list of the banned and suspect words are updated keeping in mind the social and moral norms. Although the website runs a 24 x 7 operations, no person had been deputed by him from his unit to review the listings and to respond to alerts generated by the system. This allowed the item to remain listed for 38 hours after an alert was raised by the accused as a measure to block objectionable materials were found to be grossly inadequate during the investigations. Sharat Digumarti has been charge-sheeted on recognizance without arrest."

The investigation conducted till date have gathered enough evidences against accused persons Avnish Bajaj, Ravi Raj and Sharat Digumarti Col. No. 4. It has been clearly established that all the said three accused persons knowing fully well and having reasons to believe, have sold/transmitted a pornographic/obscene MMS clip causing lascivious impact on citizens by appealing to their prurient interest for their undue pecuniary gains. Hence the present charge sheet has been prepared u/s

292/294 IPC r/w 67 IT Act. It is therefore respectfully prayed that accused Avnish Bajaj and Ravi Raj col. No. 4 on bail and Sharat Digumarti on recognizance, may kindly be called through notices and witness through summons for holding their trial in accordance with law. The list of witnesses, documents and materials exhibits have also been enclosed.

19.5 This Court is unable to agree with the submission of the prosecution that the above contents of the charge sheet make out a prima facie case against the petitioner for the IPC offence both in his capacity as MD of BIPL as well as in his individual capacity. When read as a whole, the charge sheet does not bring out the individual culpability of the petitioner at all. It brings out the culpability of the company and the reference throughout to the petitioner is in his role as the MD of such company. A useful contrast can be made with the averments pertaining to Sharat Digumarti which have been extracted in the earlier paragraph. There the precise role of the person who was Senior Manager, Trust and Safety, BIPL has been described. As regards the petitioner, the averment is that he was in charge of policy and planning and was negligent in not putting in place sufficient filtering mechanisms. In light of the strict liability principle, this by itself cannot satisfy the requirement of there being sufficient material against the petitioner to attract even prima facie the offence against him under Section 292 IPC.

19.6 A director does not automatically become criminally liable for the criminal acts of the company. If one carefully reads the judgment in Keshub Mahindra it would be clear that UCIL, the company was itself an accused. It is in that context that the Supreme Court made observations about the individual liability of the directors. There were specific allegations in the charge sheet that each of the directors was party to the decision taken by the UCIL concerning the safety of the Union Carbide Plant. There are no such averments here as to the precise direct role of the petitioner. Even in the case of Sushil Ansal no such argument appears to have been advanced that in the absence of the company the directors could still be made accused. It is not possible to equate the said two decisions with the case on hand because here the company has not been made an accused at all. In the absence of the company being made an accused and in the absence of specific allegations concerning the MD of the company, it is not possible to accept that the submission that the MD can be proceeded against for the IPC offence.

19.7 It was then sought to be argued that even illegal omissions i.e. the failure to do an act would attract Section 292 IPC. Sections 32 and 35 IPC were referred to for this purpose. The law in India as regards illegal omissions has been explained in Ambika Prasad v. Emperor MANU/UP/0086/1932 : AIR1932All506 and Anna v. State of Hyderabad AIR 1956 Hyd 99. There must be a legal compulsion to do an act and the failure to perform such an act would result in illegal omission. Not any and every omission to perform an act would result in a criminal liability. A reference may be made to the decisions in Queen v. Anthony Udyan (1883) 2nd 6 Mad 280 and Basharat v. Emperor AIR 1934 Lah 813. These provisions will have to be strictly construed. Otherwise each and every omission can attract criminal liability. The charge sheet when read as a whole can at best be said to bring out a prima facie case of omission by BIPL which owned the website and not by the petitioner in his individual capacity.

19.8 The charge sheet discloses that at various stages, in an automated system, roles were assigned to individual employees of BIPL. There was a separate Manager for Trust and Safety. When the Community Watch group alerted the website, the matter was first marked to an employee Namrata then to another employee Swapna Sawant. Even with reference to the flow chart, the prosecution was unable to show at what stages the petitioner as MD was himself directly involved in the screening of the listing or its subsequent removal. In the circumstances, it would be a mere surmise that the petitioner was himself responsible for the offence. There must be a specific allegation in the charge sheet that, despite knowing the failure of the filters, he nevertheless did nothing about it. There is no such averment in the charge sheet. In fact the liability sought to be attached to the petitioner is only in his capacity as MD of the company and not in his individual capacity. thereforee it is not possible to accept the argument of the prosecution that the doctrine of illegal omission results in a criminal liability being attached to the petitioner here.

20.1 Next, we turn to the offence under Section 67 of the IT Act vis-à-vis the petitioner here. For this it is necessary to reproduce Section 85 of the IT Act which reads as under:

Section 85 - Offences by companies

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a company, every person who, at the time the

contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in Sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.-For the purposes of this section,-

(i) "company" means any body corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm.

20.2 There are two parts to Section 85IT Act. The first part says "where a person committing a contravention of any of the provision of this Act or of any rule, direction or order made there under is a company." On a plain reading of the provision, therefore, the company has to necessarily be found to be in contravention of a provision of the IT Act. In such event, the deeming provision in the second part gets attracted. This attaches a deemed criminal liability on a person who, at the time of commission of the offence, was in "charge of, and was responsible to, the company". This deemed liability shifts the burden of proof to the individual who is in charge of the affairs of the company.

20.3 The question whether in the absence of arraigning the company as an accused, such a deemed criminal liability can attach to the directors was first addressed in the judgment of a Bench of the three Judges of Supreme Court in State of Madras v. C.V. Parekh MANU/SC/0195/1970 : 1971CriLJ418 . There the Manager and Managing Director of Microtec Castings (P) Ltd. were made the accused along with two other accused

who were a godown clerk and the representative to another company G.Ranji and Co. The company itself i.e. the Microtec Castings (P) Ltd. was not made an accused. They were charged with having committed a contravention of Clause 5 of the Iron and Steel Control Order, 1956 which is framed under the Essential Commodities Act, 1955. The Supreme Court acquitted the accused and in para 3 of the judgment it was observed as under (SCC, p. 493):

3. Learned Counsel for the appellant, however, sought conviction of the two respondents on the basis of Section 10 of the Essential Commodities Act under which, if the person contravening an order made under Section 3 (which covers an order under the Iron and Steel Control Order, 1956) is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of the business of the Company as well as the company, shall be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly. It was urged that the two respondents were in charge of, and were responsible to, the company for the conduct of the business of the company and, consequently, they must be held responsible for the sale and for thus contravening the provisions of Clause 5 of the Iron and Steel (Control) Order. This argument cannot be accepted, because it ignores the first condition for the applicability of Section 10 to the effect that the person contravening the order must be a company itself. In the present case, there is no finding either by the Magistrate or by the High Court that the sale in contravention of Clause 5 of the Iron & Steel (Control) Order was made by the Company. In fact, the Company was not charged with the offence at all. The liability of the persons in charge of the Company only arises when the contravention is by the Company itself. Since, in this case, there is no evidence and no finding that the Company contravened Clause 5 of the Iron & Steel (Control) Order, the two respondents could not be held responsible. The actual contravention was by Kamdar and Villabhadas Thacker and any contravention by them would not fasten responsibility on the respondents. The acquittal of the respondents is, therefore, fully justified. The appeal fails and is dismissed.

20.4. Later, a two-Judge Bench of the Supreme Court in Sheo Ratan Agarwal v. State of Madhya Pradesh MANU/SC/0112/1984 : [1985]1SCR719 while dealing with the same provision held as under (SCC, p.354):

5. ... The Section appears to our mind to be plain enough. If the contravention of the order made Under Section 3 is by a Company, the persons who may be held guilty and punished are (1) the Company itself (2) every person who, at the time the contravention was committed, was in charge of, and was responsible to, the Company for the conduct of the business of the Company whom for short we shall describe as the person-incharge of the Company, and (3) any director, manager, secretary or other officer of the Company with whose consent or connivance or because of neglect attributable to whom the offence has been committed, whom for short we shall describe as an officer of the Company. Any one or more or all of them may be prosecuted and punished. The Company alone may be prosecuted. The person-in-charge only may be prosecuted. The conniving officer may individually be prosecuted. One, some or all may be prosecuted. There is no statutory compulsion that the person-incharge or an officer of the Company may not be prosecuted unless he be ranged alongside the Company itself. Section 10 indicates the persons who may be prosecuted where the contravention is made by the Company. It does not lay down any condition that the person-in-charge or an officer of the Company may not be separately prosecuted if the Company itself is not prosecuted. Each or any of them may be separately prosecuted or along with the Company. Section 10 lists the person who may be held guilty and punished when it is a Company that contravenes an order made Under Section 3 of the Essential Commodities Act. Naturally, before the person-in-charge or an officer of the Company is held guilty in that capacity it must be established that there has been a contravention of the Order by the Company.

20.5 In the same paragraph of Sheo Ratan Agarwal, the above highlighted portions of the judgment in C.V. Parekh were explained thus (SCC, p.355):

That should be axiomatic and that is all that the Court laid down in State of Madras v. C.V. Parekh (supra) as a careful reading of that case will show and not that the person-in-charge or an officer of the Company must be arraigned simultaneously along with the Company if he is to be found guilty and punished. The following observations made by the Court clearly bring out the view of the Court:

It was urged that the two respondents were in charge of, and were responsible to, the company for the conduct of the business of the Company and, consequently, they must be held responsible for the sale and for thus contravening the provisions of Clause 5 of the Iron and Steel (Control) Order. This argument cannot be accepted, because it ignores the first condition for the applicability of Section 10 to the effect that the person contravening the order must be a company itself. In the present case, there is no finding either by the Magistrate Or by the High Court that the sale in convention of Clause 5 of the Iron & Steel (Control) Order was made by the Company. In fact, the Company was not charged with the offence at all. The liability of the persons in charge of the Company only arises when the contravention is by the Company itself. Since, in this case, there is no evidence and no finding that the Company contravened Clause 5 of the Iron & Steel (Control), Order the two respondents could not be held responsible. The actual contravention was by Kamdar and Villabhadas Thacker and any contravention by them would not fasten responsibility on the respondents.

The sentences underscored by us clearly show that what sought to be emphasised was that there should be a finding that the contravention was by the Company before the accused could be convicted and not that the Company itself should have been prosecuted along with the accused. We are therefore clearly of the view that the prosecutions are maintainable and that there is nothing in Section 10 of the Essential Commodities Act which bars such prosecutions.

20.6 Although it was urged by learned Senior Counsel for the petitioner that the above observations of the two-Judge Bench of the Supreme Court are contrary to what was held by the larger bench of three judges in C.V. Parekh, on a careful reflection this Court is of the view that the judgment in Sheo Rattan Agarwal is a possible view to take of what was in fact held by the Supreme Court in C.V. Parekh.

20.7 The next important decision in this regard is U.P. Pollution Control Board v. Messers Modi Distillery and Ors. . There the question that arose was whether without making the company an accused in a case involving

the offences under Sections 47 of the Water (Prevention and Control of Pollution) Act 1974, the directors of that company could be made liable. The said provision was one that provided for a deemed criminal liability of the director. The Single Judge of the Allahabad High Court had discharged the directors on the ground that the company being an accused was a pre-requisite to proceeding against the directors. Reversing the decision of the High Court, the Supreme Court held (SCC, p.689-690)

6. The learned Single Judge has focussed his attention only on the technical flaw in the complaint and has failed to comprehend that the flaw had occurred due to the recalcitrant attitude of Modi Distillery and furthermore the infirmity is one which could be easily removed by having the matter remitted to the Chief Judicial Magistrate with a direction to call upon the appellant to make the formal amendments to the averments contained in para 2 of the complaint so as to make the controlling company of the industrial unit figure as the concerned accused in the complaint. All that has to be done is the making of a formal application for amendment by the appellant for leave to amend by substituting the name of Modi Industries Limited, the company owning the industrial unit, in place of Modi Distillery. Although as a pure proposition of law in the abstract the learned Single Judge's view that there can be no vicarious liability of the Chairman, Vice-Chairman, Managing Director and members of the Board of Directors under Sub-section (1) or (2) of Section 47 of the Act unless there was a prosecution against Modi Industries Limited, the company owning the industrial unit, can be termed as correct, the objection raised by the petitioners before the High Court ought to have been viewed not in isolation but in the conspectus of facts and events and not in vacuum. We have already pointed out that the technical flaw in the complaint is attributable to the failure of the industrial unit to furnish the requisite information called for by the Board. Furthermore, the legal infirmity is of such a nature which could be easily cured. Another circumstance which brings out the narrow perspective of the learned Single Judge is his failure to appreciate the fact that the averment in para 2 has to be construed in the light of the averments contained in paras 17, 18 and 19 which are to the effect that the Chairman, Vice-Chairman, Managing Director and members of the Board of Directors were also liable for the alleged offence committed by the Company.

20.8 The decision in Sheo Ratan Agarwal was reiterated in Anil Hada v. Indian Acrylic Ltd. MANU/SC/0736/1999 : 2000CriLJ373 where the Supreme Court was interpreting Sections 138 and 141 of the NI Act. That was a case where the company itself had not been made an accused but its directors were sought to be made as an accused. The Court noticed C.V. Parekh (but mistakenly to referred to it as a decision of a two Judge Bench) and proceeded to hold: "But if a company is not proceeded due to any illegal snag or otherwise, the other prosecuted persons cannot, on that score alone, escape from the penal liability through the legal fiction envisaged in Section 141 of the Act." The Court in Anil Hada also took note of the observations in Modi Distillery and explained that they "were obiter. That apart, the law on the point was specifically discussed and dealt with in Sheoratan Aggarwal with which we are in respectful agreement."

20.9 Therefore, in light of the law explained in the decisions of the Supreme Court after C.V. Parekh, it appears that without the company being made an accused, its directors can be proceeded against under Section 67 read with Section 85 IT Act. There is another factor which weighs with this Court. At the present stage, it is too early to conclude that the company will never be made an accused. It is possible, following the dictum in SWIL that the trial court may at any stage hereafter summon the company to face trial for the offence under Section 67 IT Act. In SWIL the Supreme Court relied on the earlier decision in Raghubans Dubey v. State of Bihar : 1967CriLJ1081 and held (SCC, p. 689):

6...After taking cognizance of the offence, the Magistrate under Section 204 CrPC is empowered to issue process to the accused. At the stage of issuing process, it is for the Magistrate to decide whether process should be issued against particular person/persons named in the charge-sheet and also not named therein. For that purpose, he is required to consider the FIR and the statements recorded by the police officer and other documents tendered along with charge-sheet. Further, upon receipt of police report under Section 173(2) CrPC, the Magistrate is entitled to take cognizance of an offence under Section 190(1)(b) even if the police report is to the effect that no case is made out against the accused by ignoring the conclusion arrived at by the investigating officer and independently applying his mind to the facts emerging from the investigation by taking into account the statement of the witnesses examined by the police. At this stage, there is no question of application of Section 319 CrPC.

20.10 In that event, the difficulty in the petitioner being proceeded against may not arise at all. Prima facie there appears to be sufficient material to summon the company. In fact the Supreme Court in Modi Distillery observed that the trial court could overcome such technical objection by directing the arraigning of the company as an accused as otherwise it would be "a travesty of justice." For the above reasons it is not possible to hold that not even a prima facie is made out against the petitioner for the offence under Section 67 read with Section 85IT Act.

End Note

21. An end note before summarizing the conclusions. As this case reveals, the law in our country is not adequate to meet the challenge of regulating the use of the internet to prevent dissemination of pornographic material. It may be useful to look at the legislative response in other common law jurisdictions. In the United States, there have been three legislations that have dealt with censorship of pornographic material on the internet: the Communications Decency Act (CDA), which was enacted as a part of the Telecommunications Act of 1996, the Child Online Protection Act 1998 (COPA) and the Children Internet Protection Act 2003 (CIPA). The CDA sought to prohibit the use of an interactive computer service to send or display in any manner to those under the age of 18, any communication that depicts or displays sexual or excretory activities in a manner that is patently offensive. This was which was however struck down as unconstitutional by the U.S. Supreme Court in Reno v. ACLU (1997) 521 U.S. 844. The COPA narrowed the range of the material prohibited but was also held to be unconstitutional. The CIPA, which casts a duty on public libraries and schools to install software to block obscene or pornographic images, was upheld as constitutionally valid by the U.S. Supreme Court in United States v. American Library Association (2003) 194 U.S. 539. There are nevertheless serious concerns expressed about the effectiveness of such laws and the challenges that exist in enforcing prohibition of child pornography on the internet. [For instance, see Heidi Wachs, "Permissive Pornography: the Selective Censorship of the Internet under CIPA", 11 Cardozo Women's L.J. 441] In the United Kingdom, the Obscene Publications Act, 1959 was amended by the Criminal Justice and Public Order Act of 1994 (CJPOA) to deal with the specific problem

of internet pornography by extending the Act to cover the transmission of electronically stored data. It makes service providers liable for material placed on the internet by a third party thus requiring them to monitor material for obscene matter. Further the Protection of Children Act, 1978 was amended by CJPOA, 1994 to include photographs in electronic data format. India may want to develop a different legislative model to regulate the use of the internet with a view to prohibiting its use for disseminating child pornographic materials. Nevertheless, the task deserves the utmost priority.

Summary of conclusions

22. This Court accordingly holds as follows:

(a) The charge sheet when read as a whole brings out a prima facie case attracting the offences under Section 292(1)(a) and 292(2)(d) IPC and Section 67, IT Act. However, not even a prima facie case for the offence under Section 294 IPC is made out.

(b) A prima facie case for the offence under Section 292(2)(a) and 292(2)(d) IPC is made out against BIPL now named as EIPL both in respect of the listing and the video clip respectively.

(c) However, as far as the petitioner Avnish Bajaj is concerned, since the IPC does not recognise the concept of an automatic criminal liability attaching to the director where the company is an accused, not even a prima facie case for the offence under Section 292 IPC is made out even when the charge sheet is read as a whole; it only seeks to implicate him in his designation as MD of BIPL and not in his individual capacity.

(d) therefore, the petitioner will stand discharged as far as the offences under Sections 292 and 294 IPC are concerned. This will however not affect the case against the other accused.

(e) A prima facie case for the offence under Section 67 read with Section 85IT Act is made out against the petitioner since the law as explained by the decisions of the Supreme Court recognises the deemed criminal liability of the directors even where the company is not arraigned as an

accused and particularly since it is possible that BIPL (EIPL) may be hereafter summoned to face trial.

(f) Consequently, while the case against the petitioner of the offences under Sections 292 and 294 IPC is quashed, the prosecution of the petitioner for the offence under Section 67 read with Section 85, IT Act will continue.

23. It is clarified that the learned trial court will proceed to the next stage of passing an order on charge uninfluenced by the observations in regard to the offences in respect of which it has been held by this Court that a prima facie case has been made out against the petitioner. The petition and the application are accordingly disposed of. The interim stay is vacated.

Syed Asifuddin Vs. State of Andhra Pradesh¹⁹⁷

1. These two petitions are filed by different persons under Section 482 of Code of Criminal Procedure, 1973 (Cr. P. C.) seeking similar relief. Both the matters were admitted on the same day and since then both the matters are being listed together for being disposed of as such, this common order covers both the matters. The petitioners in both the matters seek the relief of quashing F. I. R. No. 20 of 2003 of Criminal Investigation Department (C. I. D.) Police, Hyderabad, registered under Sections 409, 420 and 120B of Indian Penal Code, 1860 (for short, IPC), Section 65 of the Information Technology Act, 2000 (for short, IT Act) and Section 63 of the Copyright Act, 1957 (for short, Copyright Act).

2. The crime was registered against the petitioners on a written complaint given by the Head of Sales and Marketing Wing of M/s. Reliance Infocomm Ltd., Hyderabad, the second respondent herein. In the complaint, it is alleged that certain vested elements of the trade of mobile telephone services began to woo the subscribers of Reliance India Mobile (RIM) into various other schemes promoted by other similar service providers, which would have the impact on the image as well as the revenues of the second respondent. Reliance Infocomm under Dhirubhai Ambani Pioneer Offer launched telephone services named as 'Reliance India Mobile' with a view to make communication affordable to the masses. The same was later modified and the scheme titled 'POBF, which is the most affordable in the market today. Under the said scheme, the subscriber gets a digital handset worth Rs. 10.500/- as well as service bundle for three years with an initial payment of Rs. 3.350/-and monthly outflow of meager Rs. 600/-. The subscriber also gets one year warranty and insurance for three years. The handset given to the subscriber is third generation digital handset with a host of features which are of first of its kind coupled with attractive tariff options. In view of this, the market response in twin cities has been phenomenal. This has an impact on the business of other service providers for the reason that those service providers attempted unethical and illegal practices for weaning away the subscribers of the second respondent.

3. In the complaint, the modus operandi adopted by other mobile service providers is described as follows : The subscribers of the second respondent are attracted by making phone calls impressing upon them

¹⁹⁷ MANU/AP/0660/2005; 2006(1)ALD(Cri)96; 2005CriLJ4314

that the tariff plans and services provided by others are better than the services of Reliance Infocomm and also advise them that they have an option to shift the service provider by paying an amount of Rs. $3,000/\sim$ towards plan charges and deposits if desired are only Rs. 540/- towards activation fee. Certain unknown persons in Abids, Begumpet, Koti, Himayatnagar and Malak-pet are making the calls to the subscribers of second respondent. Once the subscriber agrees that he can keep a world class handset which is proprietary to Reliance and also enjoy the best tariff plan of the competitor, he is asked to meet any of the business associates of rival service providers. At the rendezvous, the customer is asked to wait for an hour and an usher carries the handset to an undisclosed location in Secunderabad for conversion process, which takes about 45 minutes to an hour and half. During this time, ESN number of Reliance instrument is hacked by reprogramming and the subscriber is given the handset and instructed to switch off and switch on the handset later in the day and start enjoying the new services.

4. After receiving above written complaint lodged by the second respondent through its Head of Sales and Marketing Wing, the senior executive officer of Criminal Investigation Department, on instructions of the Additional Director General of Police, CID, registered crime No. 20 of 2003 under various provisions of IPC, IT Act and Copyright Act as mentioned hereinabove and took up investigation. The crime was registered on 31-5-2003. Investigation revealed that all the handsets of Reliance India Mobile are being migrated to TATA Indicom network at the behest of TATA Indicome staff members and that same is illegal as there is an agreement between the manufacturers of the Reliance handsets and Reliance India Mobile Limited. In view of the statements given by the witnesses, the investigating officer came to a conclusion that prima facie case is made out against the staff members of TATA Indicom and directed two inspectors to conduct raids at the Head Office of TATA Indicom situated in Khan Lathif Khan Estate, Hyderabad. This was ordered in view of specific information received about tampering of Reliance handsets by the staff members of TATA Indicom. Further on specific information about similar such practices going on at TATA Indicom centre opposite to Harihara Kala Bhavan, Secunderabad, the investigating officer along with two other inspectors and panch witnesses proceeded to LM counter at the above place when one Raj Naren, Officer of TATA Indicom revealed that the General Manager (Marketing), Madhavan and Anil Ambati, Manager (Marketing) of TATA Indicom are accepting the handsets belonging to Reliance Infocomm Limited and re-programming with their network with

different tariff packages. At the time of conducting raid in Secunderabad Office of TATA Indicom, the investigating officer also came across one Shaik Mustaffa who stated that he purchased handset from Reliance Infocomm network. Therefore, the investigating officer arrested Raj Naren and Shaik Mustaffa, and seized two mobile telephone handsets, one each from the possession of the two arrested persons. On examination, it was found that the handset recovered from Raj Naren is Samsung N191 co-branded with Reliance with ESN No. 3F7AB 832. The said set was migrated to TATA Indicom with No. 56376361 allotted by TATA Indicom. Its original Reliance India Mobile number was 31086523. The two accused along with mobile sets were brought to the office of C. I. D., and kept under surveillance of C. I. D., staff. The team of inspectors sent to the Office of TATA Indicom at Khan Lathif Khan Estate also arrested Syed Asifuddin, Patlay Navin Kumar and Khaja/Gareed Nawaj (petitioners in Criminal Petition No. 2601 of 2003) and Manoj (petitioner No. 2 in Criminal Petition No. 2602 of 2003). Two Samsung N191 co-branded with Reliance re-programmed handsets with distinct ESN and serial numbers were also seized along with 63 application forms of persons who migrated from Reliance India Limited to TATA Indicom along with the affidavits. After getting the details of the search team, the investigating officer filed remand report before the Court of IX Metropolitan Magistrate, Hyderabad on 3-6-2003. In the remand report, it is further stated as under:

The investigation made so far revealed that the Reliance Infocomm is offering under Dhirubhai Ambani Pioneer Scheme a third generation digital handset costing about Rs. 10.500/- for a mere payment of Rs. 3.350/- with a condition to sail with their network for a period of 3 years with option to exit either by surrendering the handset or paying the cost of the handset to the company. Investigation also reveals that there is an agreement existing between the Samsung manufacturers and LG manufacturers With Reliance Infocomm regarding their exclusive models Samsung N191 and LG-2030. These model handsets are to be exclusively used by Reliance India Mobile Limited only. In contravention to the above contract the TATA Indicom staff members who are figured as an accused are tampering with pre-programmed CDM-A digital, handsets belonging to Reliance Infocomm and activating with their network with all dubious means which is an offence under Section 65, I.T. Act. Secondly, the customer is not barred from exiting from the Reliance network as such and to quit from that network he has to fulfil the obligations laid down in the terms and conditions of the Reliance company. Till the lock in period of 3 years is over, the

handset supplied to the customer by Reliance Infocomm is a joint property of the company and any kind of transaction on the part of the subscriber without fulfilling the obligations laid down in the terms and conditions is clear case of Breach of Trust since the customer has not settled the accounts with the company. Further as the competition between the CDMA service providers blown out of proportions, the TATA Indicom has hatched a conspiracy to hijack the customers of Reliance Infocomm by all fraudulent means and as a part of their Infocomm by all fraudulent means and as a part of their conspiracy trying to woo the customers of Reliance Infocomm with different tariff packages and trying to trap gullible customers and succeeded in their attempt to attract their customers and so far as many as 63 customers belonging to Reliance Infocomm so far migrated to TATA Indicom by illegal means.

5. These two petitions came to be filed on 17-6-2Q03 for quashing crime No. 20 of 2003 by the means of TATA Indicom. While admitting the petitions, this Court passed orders in criminal miscellaneous petition No. 3951 of 2003 staying all further proceedings including investigation of the crime pending disposal of the main petition. The Public Prosecutor filed criminal miscellaneous petition No. 232 of 2005 for vacating the said order. The matters were "finally heard at that stage itself and are being, disposed of finally.

6. The petitioners in both the petitions are employees of Tata Tele Services Limited (TTSL) which provides basic telephone services including Wireless in Local Loop (WLL) services on non-exclusive basis in the service area including State of Andhra Pradesh under the name of Tata Indicom. All of them are alleged to have committed offences punishable under Sections 420, 409 and 120B of IPC, Section 65 of IT Act and Section 63 of Copyright Act. Learned Senior Counsel for the petitioner, Sri C. Padmanabha Reddy, submits that it is always open for the subscriber to change from one service provider to the other service provider and the subscriber who wants to change from Tata Indicom always takes his handset, to BSNL or to Reliance to get service connected and to give up services of TTSL. According to the learned counsel, the CDMA handsets brought to TTSL by subscribers of other service providers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by TTSL in relation to a handset brought to it by the subscriber of other service provider does not

amount to any crime. According to learned counsel, an offence under Section 409 of IPC is not at all made out even by going through the FIR, as well as remand report. In the absence of dishonest appropriation or conversion to their own use, alleged criminal breach of trust by the petitioners does not arise.

7. The learned Senior Counsel also submits that there was no allegation against the petitioners that they deceived the second respondent fraudulently and dishonestly to deliver the property or to retain the property and therefore the offence of cheating under Section 420 of IPC does not arise: As Section 120B of IPC is relatable only to the offences under Sections 490 and 420 of IPC, the charge under Section 120B of IPC is misconceived. Insofar as the offence under Section 65 of IT Act is concerned, the submission of the learned Senior Counsel is as follows : A telephone handset is not a computer nor a computer system containing a computer programme. Alternatively, in the absence of any law which is in force requiring the maintenance of "computer source code", the allegation that the petitioners concealed, destroyed or altered any computer source code, is devoid of any substance and therefore the offence of hacking is absent. In the absence of any allegation by the second respondent that they have a copyright to the source code of the computer programme in the handsets supplied by second respondent, the infringement of copyright does not arise. He lastly submits that the allegation that TTSL has a subscriber base of 100 thousand (one lakh) customers in Andhra Pradesh and therefore there was no necessity for TTSL to woo the customers/subscribers of second respondent.

8. The learned Additional Public Prosecutor, Sri H. Prahlad Reddy and the learned counsel for the second respondent, Sri D. Seshadri Naidu, submit that when a cognizable offence under various provisions of different statutes is registered and investigation is pending, this Court cannot quash the F. I. R., at the stage of investigation. After conducting appropriate preliminary investigation and examining witnesses the police have come to the conclusion that the petitioners have committed offences involving highly technical aspects, and therefore unless and until proper evidence is let in before the criminal Court, on mere assertions of the accused a crime cannot be quashed. They would contend that the cell phone handsets with CDMA technology supplied by the second respondent to its subscribers are dedicated to Reliance Indicomm Limited and by interfering with the computer programme and converting the handsets to be responsive to the technology adopted by TTSL is itself an offence and therefore these petitions are not maintainable.

9. The submission of the learned Senior Counsel that even if the allegations in F. I. R., are taken to be true, an offence under Sections 409, 420 and 120B of IPC, is not made put has force. Admittedly, a subscriber of second respondent is given a mobile phone instrument and connection with an understanding that the subscriber has exclusive right to use the phone. If the accused allegedly induced the subscriber of the second respondent to opt for the services provided by TTSL, an offence under Section 409 of IPC., cannot be said to have made out. Section 405 of IPC, defines 'criminal breach of trust The offence of criminal breach of trust requires entrustment with property and dishonest use or disposal of the property by the person to whom the property is entrusted. Both these things are absent. There is no allegation that the property in respect of which the second respondent has right was entrusted to TTSL or its employees who are the petitioners herein. Similarly, an offence of cheating as defined under Section 415 of IPC., is not at all made out because a subscriber of second respondent was never induced to deliver the property to TTSL nor there was dishonest or fraudulent inducement by the petitioners of the second respondent or its subscribers to deliver the property. Indeed the delivery of the property as such is not present in the case. In so far as offence of Section 120B of IPC, is concerned, the same is made in relation to alleged offence under Sections 409, 420 and 120B of IPC., and therefore the petitioners cannot be prosecuted for offences under Sections 409, 420 and 120B of IPC. Insofar as these alleged offences are concerned, if any criminal trial is conducted, the same Would result in miscarriage of justice for as held by the Supreme Court in State of West Bengal v. Swapan Kumar,: 1982CriLJ819 and State of Haryana v. Bhajan Lal,: 1992CriLJ527, when the F.I.R., does not disclose commission of cognizable offence, the police have no power to investigate such offence. In such a case, this Court would be justified in quashing investigation on the basis of information laid with the police.

10. The petitioners are also alleged to have committed offences under Section 63 of Copyright Act and Section 65 of IT Act. In the considered opinion of this Court, it would be necessary first to deal with the allegations separately and then deal with the case of the prosecution on the basis of prima facie conclusions. Before doing so, it is necessary to briefly mention about computer and computer source code. 11. The I.T. Act defines computer in clause (i) of Section 2(1) of the Act. According to the definition, 'computer' means any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network. 'Computer system' is defined in clause (1) of Section 2(1) of I.T. Act, as to mean a device or collection of devices, including input and Output support devices which are programmable, capable of being used in conjunction with external files which contain computer programmes, electronic instructions, data storage and retrieval and communication control. The I.T. Act also defines 'computer network' in clause (j) of Section 2(1) of the Act, which reads as under :

(j) computer network' means the interconnection of one or more computer through-

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

12. A reading of clauses (i), (j) and (1) of Section 2(1) of the I.T. Act would show that any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

13. A computer has to be appropriately instructed so as to make it work as per its specifications. The instructions issued .to the computer consists of a series of Os and is in different permutations and combinations. This machine language can be in different form in different manner, which is called computer language. The communicator as well as the computer understand "a language" and mutually respond with each other. When specified or particular instructions are given, having regard to the capacity of the computer it performs certain specified functions. The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. Known as source code in computer parlance, the programme written in whatever computer language by the person who assembled the programme are not seen by the users. A source code is thus a programme as written by the programmer. Every computer functions as a separate programme and thus a separate source code.

14. Computer source code or source code, or just source or code may be defined as a series of statements written in some human readable computer programming language constituting several text files but the source code may be printed in a book or recorded on a tape without a file system, and this source code is a piece of computer software. The same is used to produce object code. But a programme to be run by interpreter is not carried out on object code but on source code and then converted again. [Diane Rowland and Elizabeth Macdonald : Information Technology Law; Canandish Publishing Limited; (1997). p. 17] Thus, source code is always closely guarded by the computer companies, which develop different function specific computer programmes capable of handling various types of functions depending on the need. The law as we presently see is developing in the direction of recognizing a copyright in the source code developed by a programmer. If source code is copied, it would certainly violate copyright of developer. With this brief background in relation to computer source code, we may now consider in brief the technological aspects of a cell phone and how it works. This is necessary to understand the controversy involved in this case.

15. Alexander Graham Bell invented telephone in 1876. This enabled two persons at two different destinations to communicate with each other through a network of wires and transmitters. In this, the sound signals are converted into electrical impulses and again re-converted into sound signals after reaching the destination. The radio communication was invented by Nikolai Tesla in 1880, which was formerly presented by Guglielmo Marconi in 1894. A combination of telephone technology and radio technology resulted in radio telephone, which became very popular as technology advanced. Two persons can communicate with each other through radio telephone without there being any intervention of network of wires and other infrastructure. The radio signals travel through atmosphere medium and remain uninterrupted as long as the frequency at which radio signals travel is not disturbed. The science realized that the radio telephone communication required heavy equipment by way of powerful transmitter and that it can facilitate only 25 people to use the system. The problem was solved by communication technology by dividing a large area like a city into small cells and any two persons

connected to a cell system - at a time receive 800 frequencies and crores of people can simultaneously communicate with each other at the same time. That is the reason why the term 'cell mobile phone or cell phone'.

16. In the cell technology, a person using a phone in one cell of the division will be plugged to the central transmitter, which will receive the signals and then divert the signals to the other phone to which the same are intended. When the person moves from one cell to other cell in the same city, the system i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower when the telephone user moves from one division to another. [How Cell Phones Work? See website - http://electronics.howstuffworks.com. Much of the information on technological aspects of Cell Phones is taken from this. cell phone, it looks the database and diverts the call to that cell phone by picking up frequency pair that is used by the receiver cell phone.] Another advantage in a cell phone compared with radio phone is that when the radio phone is used, one person can talk at a time as both the persons can communicate simultaneously and also receive sound signals simultaneously.

17. All cell phone service providers like Tata Indicom and Reliance India Mobile have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider. To understand how the cell phone works, we need to know certain terms in cell phone parlance. System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing. If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range. When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring. When MTSO gets a call intended to one

18. The essential functions in the use of cell phone, which are performed by the MTSO, is the central antenna/central transmitter and other transmitters in other areas well coordinated with the cell phone functions in a fraction of a second. All this is made possible only by a computer, which simultaneously receives, analyses and distributes data by way of sending and receiving radio/electrical signals.

19. So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

[Analog - Anything analogous to something else.

Analog computer - A computing machine so designed and constructed as to provide information in terms of physical quantities analogous to those in which the problems are formulated.

Digital - 1. Of, pertaining to, or like the fingers or digits 2. Digitate. 3. Showing information, such as numerals, by means of electronics : digital watches.

Digital computer - An electronic computing machine which receives problems and processes the answers in numerical form, especially one using the binary system.

(See "The New International Webster's Comprehensive Dictionary of the English Language", Encyclopedic Edition, 2003 edn., pp. 52 and 358).]

This is a micro processor similar to the one generally used in the compact disk of a DeskTop computer. Without the circuit board, cell phone instrument cannot function. Therefore, it is not possible to accept the submission that a cell phone is not a computer. Even by the very definition of the computer and computer network as defined in IT Act, a cell phone is a computer which is programmed to do among others the function of receiving digital audio signals, convert it into analog audio signal and also send analog audio signals in a digital form externally by wireless technology.

20. The main allegation against the petitioners is that the MIN of Reliance phone is irreversibly integrated with ESN and the petitioners hacked ESN so as to wean away RIM customers to TATA Indicom service. The question is whether the manipulation of this electronic 32-

bit number (ESN) programmed into Samsung N191 and LG-2030 cell phone instrument exclusively franchised to second respondent amounts to altering source code used by these computer handsets i.e., cell phone instruments. In the background facts, a question would also arise whether such alteration amounts to hacking with computer system? If the query answered in the affirmative, it is always open to the police to alter the F. I. R., or it is always open to the criminal Court to frame a charge specifically with regard to hacking with computer system, which is an offence under Section 66 of the IT Act. At this stage, we may read Sections 65 and 66 of the IT Act.

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 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, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

66. Hacking with Computer System :- (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage 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 up to three years, or with fine which may extend up to two lakh rupees, or with both.

21. The offence of tampering with computer source documents under Section 65 of the IT Act is made out when a person,

(i) intentionally conceals, destroys or alters a computer source code used for a computer, computer programme, computer system or computer network; (ii) 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; and

(iii) (a) However, the offence is made out only when computer source code is required to be kept or

(b) when computer source code is maintained by law for the time being in force.

22. The punishment prescribed by law for the above offence is imprisonment up to three years or a fine of Rs. 2,00,000/- or both.

23. What is a computer source code is also defined in the Explanation to Section 65 of IT Act, which reads as under :

Explanation : For the purposes of this, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

24. By the very definition of 'computer source code,' a) list of programmes; b) computer commands; (c) design and layout and d) programme analysis of computer resource in any form, is a 'computer source code' for the purpose of Section 65 of I.-T. Act. Going by the definition, ESN of Samsung N191 model cell phone handset or ESN of LG-2030 model cell phone handset exclusively used by the second respondent as well as SID of second respondent come within the definition of computer source code. Every cell phone operator is required to obtain SID from the licensor i.e., Government of India. Further, ESN is a permanent part of the phone whereas MIN and SID are programmed into phone when one purchases a service plan and have the phone activity. When a customer of second respondent opts for its services, the MIN and SID are programmed into the handset. If some one manipulates and alters ESN, as per the case of second respondent, Samsung/LG handsets which are exclusively used by them become usable by other service providers like TATA Indicom. Therefore, prima facie, when the ESN is altered, the offence under Section 65 of I.T. Act is attracted because every service provider like second respondent has to maintain its own SID code and also gives a customer specific number to each instrument used to avail the services provided. The submission that as there is no law which requires a computer source code to be maintained, an offence cannot be made out, is devoid of any merit. The disjunctive

word "or" is used by the Legislature between the phrases "when the computer source code is required to be kept" and the other phrase "maintained by law for the time being in force" and, therefore, both the situations are different. This Court, however, hastens to add that whether a cell phone operator is maintaining computer source code, is a matter of evidence. So far as this question is concerned, going by the allegations in the complaint, it becomes clear that the second respondent is in fact maintaining the computer source code. If there is allegation against any person including the petitioners, certainly an offence under Section 65 of I.-T. Act is made out. Therefore, the crime registered against the petitioners cannot be quashed with regard to Section 65 of the I.-T. Act.

25. That takes me to the allegation that the petitioners violated Section 63 of Copyright Act, 1957. So as to keep pace with the advancement in science and technology especially in the field of communication and data processing, Parliament has amended Copyright Act, 1957 in 1995 bringing within its fold computer programme also as literary work to be protected by Copyright Act.

26. Section 2(ffb), (fie) and 2(o) of Copy-right Act read as under.

2(ffb) "computer" includes any electronic or similar device having information processing capabilities;

2(ffc) "computer programme" means a set of instructions expressed in words, codes, schemes or in any other form, including a machine readable medium, capable of causing a computer to perform a particular task or achieve a particular result;

2(o) "literary work" includes computer programmes, tables and compilations including computer databases;

27. Section 14 defines the copyright as exclusive right subject to provisions of the Copyright Act, to do or authorise the doing of any of the Acts enumerated in respect of the work or substantial part thereof. Section 14(b) of the Copyright Act reads as under :

14. Meaning of copyright.- For the purposes of this Act, "copyright" means the exclusive right subject to the provisions of this Act, to do or authorise the doing of any of the following acts in respect of a work or any substantial part thereof, namely :- (a) omitted.

(b) in the case of a computer programme,-

(i) to do any of the acts specified in Clause (a);

(ii) to sell or give on commercial rental or offer for sale or for commercial rental any copy of the computer programme :

Provided that such commercial rental does not apply in respect of computer programmes where the programme itself is not the essential object of the rental;

(c) and (d) omitted.

28. Therefore, reading Section 2(o), (ffc) and Sections 13 and 14 together, it becomes clear that a computer programme is by very definition original literary work and, therefore, the law protects such copyright. Under Section 63 of the Copyright Act, any infringement of the copyright in a computer programme/source code is punishable. Therefore, prima facie, if a person alters computer programme of another person or another computer company, the same would be infringement of the copyright. Again the entire issue in this regard is subject to the evidence that may be led by the complainant at the time of trial. This Court, however, examined the submission of the learned senior counsel for the petitioners in the background of the provisions of the Copyright Act and observations made herein are not intended to decide the question one way or the other. The trial Court has to deal with these aspects.

29. As noticed hereinabove, unless and until investigation by the Police into a complaint is shown to be illegal or would result in miscarriage of justice, ordinarily the criminal investigation cannot be quashed. This principle is well settled and is not necessary to burden this judgment with the precedents except making a reference to R.P. Kapoor v. State of Punjab,: 1960CriLJ1239 ; State of Haryana v. Bhajan Lal, 1992 Cri LJ 527 (SC) (supra) and State of Tamil Nadu v. Thirukkural Permal,: [1995]1SCR712.

30. In the result, for the above reasons, Crime No. 20 of 2003 insofar as it is under Sections 409, 420 and 120B of Indian Penal Code, 1860 is quashed and insofar as the crimes under Section 65 of the Information Technology Act, 2000 and Section 63 of the Copyright Act, 1957, the criminal petitions are dismissed. The C.I.D. Police, which registered Crime No. 20 of 2003, is directed to complete investigation and file a final report before the Metropolitan Magistrate competent to take

cognizance of the case within a period of three months from the date of receipt of this order.

31. The criminal petitions are accordingly dismissed.

State Bank of India Vs. Rizvi Exports Ltd.¹⁹⁸

1. Original Application No. 6 of 2000 was filed under Section 19 of the Recovery of Debts Due to Banks and Financial Institutions Act, 1993 for recovery of Rs. 1,89,38,751 44 (Rs. one crore eighty-nine lakhs thirtyeight thousand seven hundred fifty-one and paise forty-four) only against the defendant Nos. 1 to 6 who are jointly and severally liable to repay the Bank's dues together with interest thereon @ 16.83% per annum with quarterly rests in respect of debts due in the Cash Credit (Hypothecation) and EPC accounts and @ 20% per annum with quarterly rests in respect of the BPP Account. The applicant-Bank has also claimed the recovery of this amount through the sale of the hypothecated goods and immovable properties equitably mortgaged with the applicant-Bank. A cost of the suit has also been claimed. The said suit has been received on transfer under operation of law in this Tribunal and renumbered the case as T.A. 1593 of 2000.

2. The facts of the case as contained in the application are that the applicant-Bank is a body corporate constituted under the State Bank of India Act, 1955, having its central office at Mumbai and one of its Local Head Offices at Lucknow and inter alia a Branch known as Overseas Branch, Kanpur Nagar. The Assistant General Manager and Principal Officer Mr. G.D.S. Banga of the said branch is duly conversant with the facts of the present case and is duly authorized by a Power of Attorney to verify and sign the plaint on behalf of the plaintiff-Bank.

3. The defendant Nos. 2, 3 and 4 are the promoters and directors of the defendant No. 1 which is a company duly incorporated under the Companies Act, 1956. The defendant No. 1, sought financial assistance from the applicant-Bank and requested the applicant to finance loan for the business purpose of defendant No. 1 i.e., business of finishing of leather and manufacturing of leather goods. The applicant-Bank considered on their request and sanctioned Rs. 150.00 lakhs and non-funded based limit of Rs. 50.00 lakhs.

4. The defendants accepted the terms and conditions contained in the agreement letter dated 31.12.1996 and the Board of Directors of the defendant No. 1 by virtue of resolution passed in a meeting of Board of

¹⁹⁸ DEBT RECOVERY APPELLATE TRIBUNAL, ALLAHABAD T.A. No. 1593 of 2000 Decided On: 01.10.2002MANU/DA/0003/2002; II(2003)BC96

Directors held on 01.01.1997 resolved and gave consent and allowed the defendant No. 1 to borrow from the applicant-Bank various credit facilities to the tune of Rs. 200.00 lakhs secured by hypothecation and pledge of entire goods, movable and other assets, present and future holding documents of title to goods, book debts, outstanding moneys, receivables, by way of first charge and create second charge on the fixed assets of the defendants and personal guarantee of the defendant Nos. 2, 3, 4 and 5 and corporate guarantee of defendant No. 6. The rate of interest was also agreed in between the parties as per the Reserve Bank of India directives from time-to-time.

5. The defendants in order to secure the due repayment of the Banks dues, executed the following security documents in favour of the applicant-Bank on 04.01.1997:

..... Agreement for Loan for Overall limit (Form C-1) (Exhibit A/3);

..... Agreement of hypothecation of goods and assets (Form C-2) (Exhibit A/4);

...... Agreement for Overdraft hypothecation of debts and assets (Form L) (Exhibit A/5);

..... Agreement regarding grant of individual limits within the overall limit (Form C-5) (Exhibit A/6);

..... Letter of hypothecation (Exhibit A/7);

..... General Letter of Hypothecation (Exhibit A/7 A);

..... Shipping Lien (Exhibit A/8);

..... General Letter of Indemnity (Exhibit A/9);

..... Letter of undertaking by defendant No. 1 not to create any further charge over their property and assets including uncalled capital (Exhibit A/10).

Besides it, the defendant Nos. 2, 3, 4, 5, and 6 projected themselves as guarantors and guaranteed in their individual capacity to strengthen the security to liquidate the amount at debit in the accounts under various heads of credit facilities. They also executed Deed of Guarantee for overall limit of Rs. 2,00,00,000.00 on 04.01.1997 guaranteeing due payment by the defendant No. 1.

6. The defendant No. 6 is also a company incorporated under the Companies Act, 1956, guaranteed the repayment of all notices due from the defendant No. 1 to the applicant. The Board of Directors of defendant No. 6 in the meeting held on 12.12.1996 gave sanction and allowed the defendant No. 6 to stand guarantee to cover the credit facilities provided to the defendant No. 1 by the applicant. The defendant No. 6 has also furnished the corporate guarantee in favour of the applicant.

7. Defendant No. 1 is the owner of land measuring 18,733 sq. meters, comprised in Plot Nos. D-1 and D-2 situated at Industrial Area, Unnao Site 1, Tehsil and Distt. Unnao, U.P. The defendant No. 1 created equitable mortgage in favour of defendant No. 7 to secure credit facilities from it. The defendant No. 1 which has first charge on the aforesaid immovable property and the fixed assets and is entitled to lay hands thereon in priority to the applicant for the recovery of its unpaid dues, if any. However, the defendant No. I created second charge on the aforesaid immovable property and the fixed assets in favour of the applicant. The defendant No. 7 also agreed to create second charge thereon as such the applicant is also entitled to recover its dues from the sale proceeds of the immovable property and fixed assets over which it has a second charge, when the dues of defendant No. 7 not satisfied.

8. In the year 1998, there was a change in the allocation of individual limit within the overall limits inasmuch as limit of letter of credit (import/Inland) was reduced to Rs. 15.00 lakhs from Rs. 40.00 lakhs. The applicant-Bank in the ordinary course of business maintained accounts and a book debt facility account in the name of defendant No. 1 opened account in the applicant-Bank by which they availed and enjoyed the loan facility.

9. But later on the account of the defendant No. 1 became irregular and they failed to maintain financial discipline. The cause of action has arisen when financial assistance was availed by the defendant No. 1.

10. The applicant repeatedly requested the defendants and called upon them to regularize their accounts. But accounts of the defendant No. 1 were as usual. The applicant-Bank served a legal notice upon the defendants on 13.2.1999 that was also not responded by the defendants. Therefore, the applicant-Bank was having no other option except to file the instant application against the defendants for recovery of Rs. 1,89,38.751.44 (Rs. one crore eighty-nine lakhs thirty-eight thousand seven hundred fifty-one and paise forty-four) only together with pendente lite and future interest @ 16.83% per annum with quarterly rests in respect of the debts due in the Cash Credit (Hypothecation) and EPC accounts and @ 20% per annum with quarterly rests in respect of the debts due in the FBP account.

11. The Counsel for the applicant-Bank before the Tribunal at Jabalpur stated that he would not file any evidence. On receipt of the application on transfer from Jabalpur, a show-cause notice was issued by the Tribunal. In response to show cause notice only defendant Nos. 1 and 2 appeared. Service upon rests of the defendants was held sufficient by publication. Defendant No. 1 appeared through defendant No. 2 and filed an application for time to file the reply but did not contest the application of the applicant-Bank. The application, therefore, proceeded ex parte against all the defendants.

12. For determination of the fact that the amount due is a debt and lawfully recoverable, or not the applicant-Bank was required to file evidence on 22.01.2002. The Counsel stated that they have filed all documents to be relied upon.

13. The evidence of the applicant-Bank comprises documentary evidence and oral evidence comprises the affidavit of Mr. G.D.S. Banga and Mr. Akash Mittal.

14. The documentary evidence consisted of copy of resolution Exhibit A/2, Agreement for loan Exhibit A/3, Agreement for hypothecation of goods, Exhibit A/4, Agreement for Overdraft hypothecation Exhibit A/5, Agreement regarding grant of individual limits (Exhibit A/6), Letter of hypothecation Exhibit A/7, General letter of hypothecation Exhibit A/17-A, Shipping lien Exhibit A/8, General letter of indemnity Exhibit A/9. Letter of undertaking by defendant No. 1 Exhibit A/10, Deed of Guarantee overall limit of Rs. 2.00 crores Exhibit A/11, Copy of Form No. 23 Exhibit A/12. Copy of resolution passed in the meeting Exhibit A/13, Resolution of Board of Director of defendant No. 6 Exhibit A/14, Copy of Tripartite Agreement Exhibit A/15. Certificate of Form No. 8 Exhibit A/16, Agreement letter Exhibit A/17, Letter regarding the grant of individual limits with overall limits Exhibit A/18. Copy of Form Nos. 8 and 13 Exhibit A/19, Recall Notice Exhibit A/20, Statement of

accounts Exhibit A/21, Statement of accounts in respect of EPC Limit Exhibit A/22 and Statement of accounts in respect of FBP limit Exhibit A/23. By examining these, documentary evidence only one conclusion is drawn that the applicant-Bank sanctioned the limit and obtained security from the defendants for the repayment of facilities granted to them.

15. The oral evidence comprises affidavit of Mr. Banga. Mr. G.D.S. Banga has derived his knowledge from the record. He has no personal knowledge of the fact and advance of loan, utilization of the loan and outstanding dues of the loan. He states that he has gone through the security documents contained in the record of the documents in respect of the defendants. True copy of the documents have been filed along with the application under Section 19 of the Recovery of Debts Due to Banks and Financial Institutions Act, 1993. The original documents bear the signature of the person/persons stated and described in the documents. He has verified the signatures from the specimen signature given by these persons at the time of applying the credit facility. The signature tallied with the specimen signature and he has identified their signatures on the documents. The deponent thereafter states that a total outstanding of Rs. 1,89,38,751.44 is due upon the defendants. The verification clause of this affidavit states that the content of this affidavit contained in para Nos. 1, 2, 3 and 4 are true to his personal knowledge. If we examine the evidence of the witness then it will be seen that affidavit and its contents belie the verification clause and the affidavit is not trustworthy. Rather it is no evidence in the eve of law. The entire affidavit of the deponent shows that he has derived the knowledge on the basis of the record not from the personal knowledge. The affidavit also does not prove any fact. This conclusion is based on the following facts:

"The evidence of this witness in para No. 1 contains the facts on the basis of the record. He has not seen the borrowers who executed the documents, signing the writing. He does not state that those executants signed the documents in his presence. A witness can prove the execution of the documents only in two ways--firstly, document has been signed by the witness in his presence. Secondly, he is acquainted with the writing of that person as he has seen him writing. The witness shows that he has tallied the signatures of the executant's with the specimen. Neither witness has disclosed where the specimen are nor the specimen have been filed along with this application. In fact there are no specimen. There can be specimen only when these defendants have some accounts or the specimen signature have been taken at the time of the signing of the documents. In this case signature are only on the documents and there are no specimen. Besides it, the version of the witness impresses that he is handwriting expert and is recording the truth by the virtue of his expertise evidence. Thus the evidence of this witness is not trustworthy. Regarding the outstanding dues, outstanding will be when the defendant has utilized the facility. This witness of Mr. Akash Mittal has not stated a word about facts stated in the pleadings of the applicant-Bank. These witnesses do not say how much amount was sanctioned, how much amount was utilized by the defendants. Whether he operated the accounts for utilizing the facility sanctioned to him. Merely the grant of the facility and execution of the documents cannot establish the utilization of the facility and the outstanding balances. The oral evidence of both the witnesses is silent on this point. The witnesses have not stated how much amount was utilized and how much is outstanding."

16. The reference at this stage may be had to the statement of accounts filed by the applicant-Bank. Of course this document can fill the gap, which the evidence of the said witnesses have created the statement of accounts can be read in evidence only when it has been filed as per the requirement of law. This documents is not admissible in evidence at all.

17. The reason of its not being admissible in evidence is as below :

The applicant-Bank has filed the statement of accounts by a mechanized computer system. It has been done by some Private Agency Shiv Ganga, Kota. The law requires that if the statement of accounts has been filed by obtaining the printout then a different certificate is required. The Bankers Books of Evidence Act has been amended by Information Technology Act on 07.06.2000. Sub-section (8) of Section 2 defines the certified copy when it is filed by a Bank. Sub-section (8) of Section 2 of Bankers Books of Evidence Act, 1891 is reproduced below :

"(8) Certified copy" means when the books of a Bank--

(a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the Bank and was made in the usual and ordinary course of business and that such book is still in the custody of the Bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the Bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the Bank with his name and official title; and

(b) consist of printouts of data stored in a floppy, disc, tape or any other electromagnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of Section 2A.

2A. Conditions in the printout.--A printout of entry or a copy of printout referred to in Sub-section (8) of Section 2 shall be accompanied by the following namely--

(a) A certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountants or branch manager; and

(b) A certificate by a person incharge of computer system containing a brief description of the computer system and the particulars of:

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons;

(B) the safeguards adopted to prevent and detect unauthorized change of data;

(C) the safeguards available to retrieve data that is lost due to systematic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electromagnetic data storage devices;

(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media.

(F) the mode of identification of such data storage devices;

(G) the arrangements of the storage and custody of such storage devices;

(H) the safeguards to prevent and detect any tampering with the system; and

(I) any other factor which will vouch for the integrity and accuracy of the system.

(c) a further certificate from the person incharge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, be relevant data."

17. The aforesaid provisions as amended contained in Bankers Books of Evidence Act do cast a duty upon the Bankers either to produce the original ledger or to produce the ledger, which is duly certified as per the provisions of Bankers Books of Evidence Act. The statement of accounts Exhibit A/21 shows that it is a computerized statement of accounts but no such certificate as required by law has been appended to it. Mr. G.D.S. Banga has attempted to certify it. But he being a Senior Officer of the Bank must have known where the signature is to be put. This document bears rubber stamp containing certificate, which is not meant for computerized statement of accounts. The signature by Mr. G.D.S. Banga has been made above the certificate not below the certificate. Meaning thereby he has not placed the horse before the cart but has placed cart before the horse. Normally a certificate if signed men it is signed below the certificate and not above the certificate. Thus there is no certificate as required by the law. Even if a defence was taken that the statement certified has been filed that too is not correct because the certificate does not bear the signature of the authority signing it.

18. Accordingly the application establishes only a contract of loan, execution of documents and not anything beyond it. The evidence of the applicant-Bank is, therefore, deficient and application is likely to be dismissed.

ORDER

The application for the issue of the recovery certificate is dismissed with costs.

Extracts from Parliament Attack Case¹⁹⁹

12. On 13.12.2001, an unsuccessful attempt was made to storm and possibly blow-up the building of Parliament House when Parliament was in session. The Vice-President was in the Parliament House and so were many Central Ministers and M.P's. PW-5, PW-21, PW-55, PW-58, PW-69 and PW-74 gave evidence as to what transpired at Parliament House in the forenoon of 13th December, 2001.

49. PW-61, Abdul Haq Bhutt, Dy.S.P., SGPO, M.R. Ganj, Sri Nagar deposed that he had received information in the morning of 15.12.2001 that two persons after committing attack on the Parliament House had started from Delhi to Srinagar and would be around Fruit Mandi, Srinagar, which is in the jurisdiction of P.S. Parampura. He was informed that these persons had left in truck No. HR-38E-6733. He formed two to three teams to locate the truck. At about 8 A.M. he was able to locate the truck in the Fruit Mandi, but as there was a big crowd, they did not disturb the occupants but kept a watch. At about 10 A.M. the truck started from Fruit Mandi and proceeded towards Baramulla where it was stopped near Police Station Parampura. Two occupants, Mohd. Afzal and Shaukat Hussain were taken into police custody. Personal search was carried out and the two were interrogated. They disclosed that they had Rs. 10 lakhs with them, one computer and one mobile phone. These were seized vide seizure memo Ex.PW-61/4. As per the seizure memo, the mobile phone was of NOKIA make bearing IMEI No. 350102209452432. The accused persons made a joint discloser statement being Ex. PW-61/3. The officials of Delhi Police were informed about the arrest. At about 2.15 P.M. officials of Delhi Police reached Srinagar and the accused persons along with the articles recovered and the seizure memo were handed over to Delhi Police vide memo Ex.PW.-61/6. In cross-examination, the witness stated that information was received by his senior officers which was communicated to him around 5.45 A.M. on 15.12.2001. The truck was

¹⁹⁹ MANU/DE/1026/2003; 2003VIIAD(Delhi)1, 107(2003)DLT385; 2003(71) DRJ 178; 2003(3)JCC1669

IN THE HIGH COURT OF DELHI {Murder Reference No. 1/2003 and Crl. A. No. 43/2003 Decided On: 29.10.2003 Appellants: State Vs. Respondent: Mohd. Afzal and Ors. [Along with Crl. A. Nos. 59 and 80/2003] AND Appellants: Mohd. Afzal Vs. Respondent: State [Along with Crl. A. Nos. 12, 19 and 36/2003]}

being driven by the accused Shaukat. No entry in daily diary of the police was made when he left the police station but volunteered to state that entry was made in the daily diary after completing the operation. The truck was stopped and examined at around 10.30 A.M. He did not paste any slip on the briefcase or on the computer or on the mobile phone. A suggestion was put to the witness that Shaukat and Afzan were apprehended by him from different places and the story of recovery was false, which he denied.

50. PW-62 H.C. Mohd. Akbar deposed that he was present with PW-61 when accused Mohd. Afzan and Shaukat were arrested. He deposed in line with the deposition of PW-61. In cross-examination the suggestion to this witness was that the accused Shaukat and Mohd. Afzal were brought first to the Police Station and the truck came later, which was denied by him.

101. PW-72, Shri Vimal Kant, an employee of Orion Convergence Ltd., a computer expert, deposed that he was called to the Special Cell on 17.12.2001 where he met Inspector Mohan Chand Sharma. He was asked to retrieve the information stored in the laptop. He worked on the laptop to retrieve the information from 17.12.2001 to 29.12.2001 and would report whatever progress he was making to Inspector Mohan Chand Sharma as also ACP Rajbir Singh. He gave his report Ex.PW-72/1. Documents, which were found stored in the laptop and prints out of which were taken out by him and submitted Along with the report were Ex.PW-59/1 to 7, PW-72/2 and PW-72/13. In the cross-examination by accused Afzan Guru and Shaukat, witness stated that his reports contained the sum total of all his observations. He admitted that hard disc is a replaceable component and could be formatted. He admitted that if a hard disc was replaced, it would not contain the data which was stores earlier unless it is re-fed. He stated that the laptop which he examined was already having a hard disc. He stated that hard disc is connected to other organs of the laptop through wires and if the hard disc has to be replaced, the laptop has to be opened and all connections have to be severed. He stated that a layman could not replace the hard disc and that he did not open the laptop to check the date of manufacturing of the hard disc. He stated that operating system, as observed in his report, was installed on 29.7.2000 and, therefore, the manufacturing date had to be prior to this date. He admitted that it was possible to take out the disc from one laptop and put it to another. But if this was done, history stored on the hard disc would reflect a change in the hardware and in the case

of computer handled by him, it was not so reflected. He stated that the history is reflected in REG file which is a internal registering file of the operating system and he did not notice anything of significance in the REG file of the computer. He stated that if internet has been accessed through a computer then actual date would be reflected, additionally, if any change is made to the date setting of the computer, it would be reflected in the history i.e. in the REG file. He denied the suggestion that the date setting is a text editable file but said that a date setting could be edited. He denied the suggestion that a hard disc could be changed without it being reflected in the history maintained in the REG file. He admitted that a REG file could be edited but gualified not fully. In response to the question, "in the absence of verified time setting and reliable information about the hard disc being original, there is no certainty that the material found on a later date, was exactly the material, which may have existed on a previous date?" He replied that the question was vague and in the absence of stipulated time period could not be answered. The laptop always remained in possession of Inspector Mohan Chand Sharma when he was not working on it and after finishing his work, he left the same with Inspector Mohan Chand Sharma. He stated that he had no information about the laptop being referred to Microsoft for information. On further cross-examination by the remaining accused, he admitted that back up of complete hard disc was not taken by him. He stated that certain files were backed up/which fact was not mentioned in his report. He said that the report contained his observations and was not a report of processes which were employed.

102. PW-73, Krishan Shastri, Assistant Government Examiner of Questioned Documents, Hyderabad, deposed that letter dated 19.2.2002 from the DCP was received by him for examining the storage media of the laptop and 210 smart media storage. He deposed that EX.P-83 was the laptop sent to him and EX-73/1 and 73/2 and 3 were smart media storage devise sent to him. After examining he gave his report Ex.PW-73/1. He qualified that he gave opinion dated 31.5.2002 with supplementary opinion dated 25.7.2002. Both constituted the report Ex.PW-73/1. In the cross-examination by accused Afzan Guru and Shaukat, witness deposed that ACGS was a software to view the images and browse them. He had mentioned in the report the various software's installed in the storage media of the laptop. He stated that hard disc could be replaced in a laptop by highly skilled person and many systems crashed because of incompatibility of the replaced hard disc. According to his observation, DAT was last accessed on 21.1.2002 and it was created on 27.9.2001. The win. 386 swp was last accessed on 22.12.2001

and was last written on 22.1.2002. He stated that a file could not be written without being accessed by copying it on each storage media. He admitted that the date setting on the file is related to the date setting on the computer and it is possible to modify the date as date setting was a modifiable act. He said that window ME is a operating system. He stated that internet protocol addresses was found from the file system DAT, which was created on 27.9.2001 and he had mentioned this in his report. The dates of in between access and in between modification do not appear in his report. The operating system MS Windows ME was installed on 29.7.2000. Regarding the files written in 1999 found in the hard disc, he stated that they must have been written by the previous operating system on the laptop and taken from another computer and stored in this computer.

103. PW-79, M. Krishna, Government Examiner of Questioned Documents, Hyderabad, deposed that he had examined the laptop along with PW-73. Report Ex.PW-73/1 also was signed by him. Annexures Q to S were part of the report being Ex.PW-73/3 and 73/7. The laptop was last accessed on 21.1.2002 and the particular file was last created on 27.9.2001 and last accessed on 21.1.2002. (To a Court question whether he could tell if any addition or alteration were made in the file when it was accessed on 21.1.2002, he stated that he had not seen any.) It was a system dat file where details are available. In cross-examination by accused Shaukat and Afzan, witness stated that in computer forensic, one should never work on the original system. The system should be connected with another storage media for analysis. He admitted that CMOS chip reflect the date setting and that date setting could be compared with the current time setting but qualified that this was subjected to date setting not being altered. He stated that if date setting was altered, it would remain the same in the system for the earlier files and the change would be reflected in the file created after the change in the systems date. He said that dates of a particular file could not be flushed unless CMOS setting of the date and time were changed. He stated that noting of CMOS setting is essential to verify the date setting of file. He stated that all that he was required to opine upon was the date of creation of a file and of date of last access. He said that it was not possible to alter the date of any particular file unless the system date had been altered.

118. DW-8, Dr. Arun Mehta, Computer Engineer, deposed that he had a master's degree in Computer Science and was engaged in software

teaching, writing and consultancy. He deposed that information stored in a computer is on a Magnetic medium, for instance a hard disc. Magnetic may be easily polarized one way or the other. Therefore, any data in a computer can be changed by a knowledgeable person. While seizing electronic evidence one should always take a back up and keep it sealed because it is unlike a photograph of a crime scene. Date and time shown in the computer must be recorded because if there is any inaccuracy, it will be reflected. Version of the software installed should be recorded and the software used to examine the computer should also be noted. He deposed that it is easy to introduce a fresh file in a computer. There are utilities available in the internet which may change the date and time. Marks 'A' to 'G' were proof taken out by him through internet informing about the utilities. Time and date settings are easily modified. Knowledgeable person can make the modifications. In some laptops, hard" disc could be removed very easily and in some it may be difficult, but for professionals this was a routine activity. The date of last access is treated differently by different software's and the time of last access was meaningless in the absence of knowledge as to what software is used to process the file. To court questions, witness admitted that when a file is accessed in a computer, the computer records in the history, as to when the file was accessed. He, however, clarified by saying that using special software packages, its history can be edited and the kind of special packages were in documents mark 'A' to 'G'. He deposed that software which was installed in a computer could be modified and un-installed without leaving any trace. Whenever a fresh file was introduced in a computer, computer gives the date but this could be changed. If a hard disc was replaced in a computer, the entire data would vanish. In crossexamination, witness deposed that he had never taken back-up of any computer for a criminal case and had not written any book for use of electronic evidence. Volunteered that he had written some articles concerning Tehlaka.com for submission to Vekataswamy Commission pertaining to use of electronic evidence.

267. Reply of the prosecution was that as per Sub-section (1) of Section 65B computer generated print outs were admissible in evidence provided they satisfied the conditions mentioned in Sub-section (2) and Sub-section (4) merely provided on alternative mode of proof by way of certification.

268. Section 3 of the Evidence Act, 1872 defines evidence as under:

"Evidence" - Evidence means and includes:-

1)-----

2) all documents including electronic records produced for the inspection of the court;

269. By way of amendment to the Evidence Act, 1872, incorporated by Act. No. 21 of 2000 following was inserted:

"The expression "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic records", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000."

270. Section 2(c) of the Information Technology Act, 2000 reads:

"electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro record."

271. Section 65A and 65B of the Evidence Act, 1872, inserted by Act No. 21 of 2000 read as under:-

65A. Special provisions as to evidence relating to electronic record.

The contents of electronic records may be proved in accordance with the provisions of Section 65B.

65B. Admissibility of electronic records.

(1) notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible. (2) the conditions referred to in Sub-section (1) in respect of a computer output shall be following, namely :-

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of said activities;

[c] throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regular carried out on over that period as mentioned in Clause (a) of Sub-section (2) was regularly performed by computers, whether -

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, or one or more computers and one or more combinations of computers,

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly. (4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, -

(a) identifying the electronic record containing the statement and describing the manner which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in Sub-section (2) relate,

and purporting to be signed by a person occupying a reasonable official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section, -

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form or whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer shall be taken to be supplied to it in the course of those activities;

(c) to a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

272. Thus, computer generated electronic records is evidence, admissible at a trial if proved in the manner specified by Section 65B of the Evidence Act.

273. Sub-section (1) of Section 65B makes admissible as a document, paper print out of electronic records stored in optical or magnetic media produced by a computer, subject to the fulfillment of the conditions specified in Sub-section (2) of Section 65B. Following are the conditions specified by Sub-section (2) :

a) The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by a person having lawful control over the period, and relates to the period over which the computer was regularly used;

b) Information was fed in the computer in the ordinary course of the activities of the person having lawful control over the computer;

c) The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy;

d) Information reproduced is such as is fed into computer in the ordinary course of activity.

274. Under Sub-section (3) of Section 65B, Sub-section (1) and (2) would apply where single or combination of computers, is used for storage or processing in the regular course of activities and the computers used shall be construed as a single computer. Under Sub-section 4 of Section 65B, if evidence is desired to be led under Section 65B, it would be admissible if a certificate is tendered, signed by a person either occupying a responsible official position in relation to the computer or being in the management of the relevant activities; provided the following is certified:

(a) electronic record containing the statement is identified with description of how it was produced;

(b) that electronic record was a computer print out generated by a device particulars whereof are given;

(c) deals with matters to which conditions in Sub-section (2) relate.

275. Under Sub-section (5), information shall be taken to be supplied to a computer by means of an appropriate equipment, in the course of normal activities intending to store or process it in the course of activities and a computer output is produced by it whether directly or by means of appropriate equipment.

276. The normal rule of leading documentary evidence is the production and proof of the original document itself. Secondary evidence of the contents of a document can also be led under Section 65 of the Evidence Act. Under Sub-clause "d" of Section 65, secondary evidence of the contents of a document can be led when the original is of such a nature as not to be easily movable. Computerised operating systems and support systems in industry cannot be moved to the court. The information is stored in these computers on magnetic tapes (hard disc). Electronic record produced there from has to be taken in the form of a print out. Sub-section (1) of Section 65B makes admissible without further proof, in evidence, print out of a electronic record contained on a magnetic media subject to the satisfaction of the conditions mentioned in the section. The conditions are mentioned in Sub-section (2). Thus compliance with Sub-section (1) and (2) of Section 65B is enough to make admissible and prove electronic records. This conclusion flows out, even from the language of Sub-section (4). Sub-section (4) allows the proof of the conditions set out in Sub-section (2) by means of a certificate issued by the person described in Sub-section 4 and certifying contents in the manner set out in the sub-section. The sub-section makes admissible an electronic record when certified that the contents of a computer print out are generated by a computer satisfying the conditions of Sub-section 1, the certificate being signed by the person described therein. Thus, Sub-section (4) provides for an alternative method to prove electronic record and not the only method to prove electronic record.

277. Whether Section 65B casts a positive mandate on the person relying upon electronic record, to adduce affirmative evidence that at all material time the computer was working properly when information was being fed in it, and whether on facts, the computer generated call details have to be ignored due to alleged malfunctioning?

278. The last few years of the 20th Century saw rapid strides in the field of information and technology. The expanding horizon of science and technology threw new challenges for the ones who had to deal with proof of facts in disputes where advanced techniques in technology was used and brought in aid. Storage, processing and transmission of date on magnetic and silicon medium became cost effective and easy to handle. Conventional means of records and data processing became out dated. Law had to respond and gallop with the technical advancement. He who sleeps when the sun rises, misses the beauty of the dawn. Law did not sleep when the dawn of Information and Technology broke on the horizon. World over, statutes were enacted. Rules relating to admissibility of electronic evidence and it's proof were incorporated.

279. Did the law relating to admissibility and proof of electronic record have a positive mandate to be satisfied by the one who relies upon electronic record? The positive mandate being to establish positively that there was no malfunctioning of the equipment processing the operations at the relevant time, to which the record relates.

280. In England this positive mandate was statutorily enacted and the prosecution had to show by positive and affirmative evidence that it was safe to rely upon the document produced by a computer from out of its memory. The Police & Criminal Evidence Act, 1984 was enacted. But, while interpreting Section 69 of the said Act, the courts took a practical approach and gave an interpretation where computer generated record could be proved by a statement, made by an employee unfamiliar with the precise details of the operation of the computer, that the print out was retrieved from the computer memory and the computer was not malfunctioning. Section 69 reads as under:

"(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown -

(a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer.

(b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of it contents; and

[c] that any relevant conditions specified in rules of Court under Sub-section (2) below are satisfied.

(2) Provision may be made by the rules of Court requiring that in any proceedings where it is desired to give a statement in evidence by virtue of this section such information concerning the statement as may be required by the rules shall be provided in such form and at such time as may be so required." 281. In R.V. Shepherd 1993 A.C. 380. Lord Griffiths, dealing with the defense argument held:-

"The principal argument for the defendant starts with the proposition that the store detective was not a person occupying a responsible position in relation to the operation of the computer within the meaning of paragraph 8(d) of Schedule 3 to the Act and, therefore, was not qualified to sign a certificate for the purpose of providing proof of the matters contained in Section 69(a). This I accept. Although the store detective understood the operation of the computer and cold speak of its reliability she had no responsibility for its operation.

I cannot however, accept the next step in the defendant's argument which is that oral evidence is only acceptable if given by a person who is qualified to sign the certificate. The defendant does not go so far as to submit that evidence must be given by a computer expert but insists that it must be someone who has responsibility for the operation of the computer; either the operator or someone with managerial responsibility for the operation of the computer.

Documents produced by computers are an increasingly common feature of all business and more and more people are becoming familiar with their uses and operation. Computers vary immensely in their complexity and in the operations they perform. The nature of the evidence to discharge the burden of showing that there has been no improper use of the computer and that it was operating properly will inevitably vary from case to case. The evidence must be tailored to suit the needs of the case. I suspect that it will very rarely be necessary to call an expert and that in the vast majority of cases it will be possible to discharge the burden by calling a witness who is familiar with the operation of the computer in the sense of knowing what the computer is required to do and who can say that it is doing it properly."

282. Statement by the witness that when the computer was working they had no trouble with operation of central computer was held sufficient in discharge of the affirmative burden.

283. In R v. Ana Marcolino,(CA "Crim.Div"), following the dictum of Lord Griffiths in R.V. Shepherd the evidence of the witness proving electronic record was analysed step wise which analyses is illuminative

as to how the issue was dealt with. Lord Justice Henry posed the question: Does the evidence given by Mr. Slade satisfy the test in Shepherd, 1993 AC 380 ? The answer came as follows:

1). he had been employed by Vodafone for over four years as the risk supervisor and his duties included identifying fraudulently used accounts and liaising with the police. This account had been used fraudulently.

2) He had retrieved from the computer the records relating to this mobile telephone and produced from those records the itemized account for the relevant period. To do so, he had accessed the billing records for that period.

3) he was not familiar with the precise details of the operations of the computer because he had not designed it. However, he had general knowledge of the system. He had no reason to believe that the computer records were inaccurate because of improper use.

4) Vodafone is continuously audited by the DTI. No complaint has been made as to the accuracy of their records. Vodafone has their own quality assurance department which constantly monitored the system.

5) he asserted that the computer was working properly at the relevant time. In support of that assertion he relied upon the following facts :

a) There was no record of any malfunction. Had their been, it would have been drawn to his attention by the billing department. In any event, the computer had ancillary equipment which would have taken over, had there been any failure or malfunction of the primary systems.

b) If there had been any malfunction, the billing records would be classed as 'in suspension'; those records were not.

c) The billing record itself is made without human intervention, although it is triggered by the use of a mobile phone. The system runs a series of internal checks as to accuracy and function before the call is made and the subsequent detail recorded. If there is any malfunction the records are put into suspension. The records of these calls had not been suspended.

d) The records in relation to malfunction were kept by persons who could not reasonably be expected to have any personal recollection of them. These persons had a duty to report any malfunction. None had been reported.

Miss Calder submitted that the evidence of external audit is irrelevant. In our judgment, the jury was entitled to take into account that these records were produced by a large company providing a substantial public service the subject of licensing and external audit by the DTI. Such evidence goes directly as to whether there has been improper use. It is the view of this Court that the totality of the evidence as set out above satisfies the test propounded by Lord Griffiths. Mr. Slade was sufficiently familiar with the workings of the computer. The records are designed to reveal malfunction. None was revealed.

284. The conviction was found to be safe and the appeal was dismissed.

285. In DPP v. Me. Kewon (1997) 1 C A 155, Lord Hoffman, applying Section 69 of the Police and Criminal Evidence Act, 1984 in relation to the inaccuracy in the time display in the computer print out, held:-

"I shall for the moment assume that the inaccuracy in the time display meant that "the computer not operating properly". The question is therefore whether that was "such as to affect the production of the document or the accuracy of its contents". If the words are read literally, it did. The document said that the first test had occurred at 23.00 GMT when it was in fact 00.13 BST. As to one hour, the discrepancy is merely as to the way in which the time was expressed. 23.00 GMT is the same time as 00.00 BST. But the remaining 13 minutes cannot, I think, be dismissed as de minimis. The inaccuracy of the time reading therefore affected the accuracy of a part of the contents of the document.

In my view, however, the paragraph was not intended to be read in such a literal fashion. "The production of the document or the accuracy of its contents" are very wide words. What if there was a software fault which caused the document to be printed in lower case when it was meant to be in upper case? The fault has certainly affected the production of the document. But a rule which excluded an otherwise accurate document on this ground would be quite irrational. To discover the legislative intent, it is necessary to consider the purpose of the rule.

The first thing to notice is that Section 69 is concerned solely with the proper operation and functioning of a computer. A computer is a device for storing, processing and retrieving information. It receives information from, for example, signals down a telephone line, strokes on a keyboard or (in this case) a device for Chemical analysis of gas, and it stores and processes that information. If the information received by the computer was inaccurate (for example, if the operator keyed in the wrong name) then the information retrieved from the computer in the form of a

statement will likewise be inaccurate. Computer experts have colourful phrases in which to express this axiom. But Section 69 is not in the least concerned with the accuracy of the information supplied to the computer. If the gas analyser of the Intoximeter is not functioning properly and gives an inaccurate signal which the computer faithfully reproduces, Section 69 does not affect the admissibility of the statement. The same is true if the operator keys in the wrong name. Neither of these errors is concerned with the proper operation or functioning of the computer.

The purpose of Section 69, therefore, is a relatively modest one. It does not require the prosecution to show that the statement is likely to be true. Whether it is likely to be true or not is a question of weight for the justices or jury. All that Section 69 requires as a condition of the admissibility of a computer-generated statement is positive evidence that the computer has properly processed, stored and reproduced whatever information it received. It is concerned with the way in which the computer has dealt with the information to generate the statement which is being tendered as evidence of a fact which it states.

The language of Section 69(1) recognises that a computer may be malfunctioning in a way which is not relevant to the purpose of the exclusionary rule. It cannot therefore be argued that any malfunction is sufficient to cast doubt upon the capacity of the computer to process information correctly. The legislature clearly refused to accept so extreme a proposition. What, then, was contemplated as the distinction between a relevant and an irrelevant malfunction? It seems to me that there is only one possible answer to that question. A malfunction is relevant if it affects the way in which the computer processes, stores or retrieves the information used to generate the statement tendered in evidence. Other malfunctions do not matter. It follows that the words "not such as to affect the production of the document or the accuracy of its contents" must be read subject to the overall qualification that the paragraph is referring to those aspects of the document or its contents which are material to the accuracy of the statement tendered in evidence."

286. The Law Commission in England reviewed the law relating to computer generated evidence. It summed up the major problem posed for the rules of evidence by computer output in the words of Steyn, J.:-

"Often the only record of the transaction, which nobody can be expected to remember, will be in the memory of a computer. ... if computer output cannot relatively readily be used as evidence in criminal case, much crime (and notably offences involving dishonesty) would in practice be immune from prosecution. On the other hand, computers are not infallible. They do occasionally malfunction. Software systems often have "bugs". --- Realistically, therefore, computers must be regarded as imperfect devices."

287. It noted that given the extensive use of computers, computer evidence could not be unnecessarily imp leaded, while giving due weight to the fallibility of computers. The Law Commission noted that Section 69 had enacted a law which was unsatisfactory for 5 reasons:-

"First, Section 69 fails to address the major causes of inaccuracy in computer evidence. As Professor Taper has pointed out, "most computer error is either immediately detectable or results from error in the data entered into the machine".

Secondly, advances in computer technology make it increasingly difficult to comply with Section 69: it is becoming "increasingly impractical to examine (and therefore certify) all the intricacies of computer operation". These problems existed even before networking became common.

A third problem lies in the difficulties confronting the recipient of a computer-produced document who wishes to tender it in evidence: the recipient may be in no position to satisfy the court about the operation of the computer. It may well be that the recipient's opponent is better placed to do this.

Fourthly, it is illogical that Section 69 applies where the document is tendered in evidence, but not where it is used by an expert in arriving at his or her conclusions, nor where a witness uses it to refresh his or her memory. If it is safe to admit evidence which relies on and incorporates the output from the computer, it is hard to see why that output should not itself be admissible; and conversely, if it is not safe to admit the output, it can hardly be safe for a witness to rely on it."

288. The Commission recommended deletion of Section 69, the opinion was:

"Where a party sought to rely on the presumption, it would not need to lead evidence that the computer was working properly on the occasion in question unless there was evidence that it may not have been - in which case the party would have to prove that it was (beyond reasonable doubt in the case of the prosecution, and on the balance of probabilities in the case of the defense), The principal has been applied o such devices as speedometers and traffic lights, and in the consultation paper we saw no reason why it should not apply to computers.

289. We may note that Section 69 of the Police and Criminal Evidence Act, 1984 has since been repealed and the common law presumption :-"in the absence of evidence to the contrary the courts will presume that mechanical instruments were in order at the material time", operates with full force.

290. Experience has shown to us that development in computer networking, access, control, monitoring and systems security are increasingly making it difficult for computer errors to go undetected. Most computer errors are immediately detected or resultant error in the date is immediately recorded. In a court of law it would be impractical to examine the intricacies of computer functioning and operations. To put it in the words of the Law Commission report in England:-

"Determined defense lawyers can and do cross-examine the prosecution's computer expert at great length. The complexity of modern systems makes it relatively easy to establish a reasonable doubt in a juror's mind as to whether the computer was operating properly. Bearing in mind the very technical nature of computers, the chances of this happening with greater frequency in future are fairly high. We are concerned about smoke-screens being raised by cross-examination which focuses in general terms on the fallibility of computers rather than the reliability of the particular evidence. The absence of a presumption that the computer is working means that it is relatively easy to raise a smoke-screen."

291. The law as it stands enacted in India does not have a provision analogous to Section 69 of the Police and Criminal Evidence Act, 1984 in England. The conditions which require to be satisfied are the ones set

out in Sub-section (2) of Section 65B. The conditions, as noted above are:-

a) The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by a person having lawful control over the period, and relates to the period over which the computer was regularly used;

b) Information was fed in the computer in the ordinary course of the activities of the person having lawful control over the computer;

c) The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy;

d) Information reproduced is such as is fed into the computer in the ordinary course of activity."

292. In effect, substantially, Section 65B of the Indian Evidence Act and Section 69 of the Act in England have same effect.

293. Thus, in the context of Section 65B(2)(c) the condition that throughout the material part of the period to which the computer operations related, the computer was operating properly has to be complied with. However, this compliance would be on the principle laid down in Shepherd (supra) and as applied in Ana Marcolino (supra) and Me. Kewon (supra). Thus in our opinion, is the only practical way to deal with computer generated evidence unless the response is by way of a challenge to the accuracy of computer evidence on the ground of misuse of system or operating failure or interpolation. Such challenge has to be established by the challenger. Generic and theoretical doubts by way of smoke screen have to be ignored.

294. The testimony of PW.35 and PW.36 establishes that the call details Ex.PW.35/2 to Ex.PW.35/8 and Ex.PW.36/1 to Ex.PW. 36/5 were computer generated and pertained to the respective periods indicated in the print outs. Testimony establishes that they related to the services provided by the respective companies in respect of the different mobile phone numbers. It is true that neither witness made a positive statement that during the relevant period, the computers worked properly but reading the statement as a whole, the same is implicit. No suggestion was given to the witness that their computers were malfunctioning. We are satisfied that on the evidence on record, the prosecution has duly proved the electronic record Ex.PW.35/2 to Ex.PW.35/8 and Ex.PW.36/1 to 36/5.

295. The technical flaw whereby on four occasions double entries have been recorded are explainable, in that, they are double entries pertaining to the called and caller numbers. Even otherwise as held in Ana Marcolino (Supra) the malfunction is not sufficient to cast a doubt upon the capacity of the computer to process information correctly. It does not establish in any way that the capacity of. the computer to process, store and retrieve information used to generate the statement, tendered in evidence, was effected.

CONCLUSIONS WHICH EMERGED FROM THE MOBILE PHONES, SIM CARDS RECOVERED DURING INVESTIGATION AND THE RECORDS OF THE CALL DETAILS OF THE VARIOUS TELEPHONE NUMBERS.

337. Testimony of PW-25, PW-50, PW-59, PW-72, PW-73 and PW-79 pertained to the information in the laptop recovered from the truck at Srinagar and the information stored in the memory thereof. From the testimony of PW-1 to PW-4, it stands established that seven I-Cards were recovered from the person of the deceased terrorists, one each from the terrorists Raja, Rana, Hamja and Hayder purporting to be issued by a computer centre at Bunglow Road and purporting to be of Xensa Web City., Two similar cards were recovered from accused Mohd, and one more I-Card purportedly issued by Cyber Tech Computer Hardware was recovered from the terrorist Mohd. In all there were these two formats of the identity cards, one of Xensa Web City and other of Cyber Tech Computer Hardware. Testimony of PW-25 and PW-50 establishes that the cards pertaining to Xensa Webcity were fake. Testimony of PW-59, Sh. N.K. Aggarwal, Sr. Scientific Officer, CFSL; PW-72, Sh. Vimal Kant, a computer engineer; PW-73, Sh. Krishan Shastri from bureau of police research at Hyderabad; and PW-79, Sh. M. Krishna, Government examiner of questioned documents establishes that stored in the memory of the laptop was a file which contained the format of the identity card pertaining to Xensa Webcity recovered from the deceased terrorists and that the said identity cards were prepared by taking print outs from the laptop in question. Also stored was a file from which the fake Home Ministry Sticker pasted on the wind screen of the Ambassador car was recovered. The testimony of these witnesses, inter alia, establish the fact that history of the use of a computer is reflected in the "REG" file which is an internally registering file of the operating system. The "DAT" file could be edited and the date and time setting of a computer could be edited, but if that was done, it would be reflected in the history recorded in the "REG" file. Though date setting could be edited, the "DAT" setting is not a text editable file. The computer records the dates when

the files are created and when the computer was last accessed. The date and time setting is reflected in the CMOS Chip. Further, it stands established that if the date setting was altered it would remain the same in the system for the earlier files and the change would be reflected in the files created after the change in the system's date. It was not possible to alter the date of any particular file unless the system's date had been altered. None of these witnesses deposed that they had noted any such alterations being effected. In the cross-examination, apart from asking theoretical questions, nothing material was brought out on record to challenge the veracity of the reports proved by these witnesses, which reports brought out the position afore stated. It is no doubt true, that the evidence of the technical experts was to the effect that where a laptop is being examined, as a rule of precaution a back up should be taken for if any tampering was alleged against the person examining the computer, the purity of the contents of the memory of the computer could be maintained in the back up file.

338. In the context aforesaid, let us analyze what emerges from the evidence on record pertaining to the laptop. PW-61 corroborated by PW-62 deposed about the recovery of the laptop from the truck at Srinagar. It was identified as Ex.P-83 by PW-61. PW-64 and PW-65, SI Hriday Bhushan and SI Sharad Kohli, who had gone from Delhi to Srinagar to bring accused Afzal and Shaukat deposed that on 15th December, 2001 itself, the laptop was handed over to them and on 15th December, 2001 itself by late evening, was handed over to PW-66, Inspector Mohan Chand Sharma, who called PW-72, Vimal Kant to retrieve information from the computer and furnish the same to him. PW-72 worked on the laptop to retrieve information from 17th December, 2001 to 29th December, 2001. No suggestion in cross-examination has been made to PW-66 or PW-72 that they tampered with the laptop when it remained in their custody. The laptop was sealed and deposited in the Malkhana on 16.1.2002 as per the testimony of PW-80 to which there was no challenge. It is no doubt true that in the report of PW-79, it is recorded that the computer was last accessed on 21.1.2002 but that does not mean that there was interpolation made in the computer, much less interpolation pertaining to the file having the format of the identity card and the writing of the fake Home Ministry Sticker recovered from the car used by the deceased terrorists. It is important to note that PW-72 worked on the computer to retrieve information up to 29.12.2001 and had given the computer print out to the police as retrieved from the computer pertaining to the format of the identity card and the fake Home Ministry Sticker. Thus, the file containing these two documents, being

created by way of interpolation on 21.1.2002 is ruled out. Secondly, PW-79 had categorically stated in response to a court question that no alterations had been made as none were recorded in the history of the computer when it was accessed on 21.1.2002. Further, the report Ex.PW-73/1 shows that the WIN386.SWP5 was accessed last on 22.12.2001 and was last written on 21.1.2002. Now, a file cannot be written upon without being accessed is the question which needs to be answered. The answer would be found in the testimony of PW-79 where in response to a court question, the witness deposed that in the system DAT file system accessing details are available and he had not seen any alterations made. This testimony of PW-79 could be dovetailed to the testimony of PW-73 wherein he deposed that the USER.DAT was last accessed on 21.1.2002 but WIN386.SWP was last accessed on 22.12,2001 but was last written on 21.1.2002. It is evident that WIN386.SWP is a self writing file and, thus, the opening of the laptop on 21.1.2002 would have been automatically written on the file. The computer would record the same without any conscious human intervention. This, however, can only take place when a user consciously opens those files and access them. It is, thus, apparent that on 21.1.2002, the laptop was opened but it is equally true that there was no change in any other file, PW-73 has authored a book "Computer Crime and Forensics" which lists WIN386.SWP as a swap file. Our finding, therefore, is that no doubt it stands established that the computer was accessed on 21.1.2002 but the access does not reveal that any of the file was altered or modified. The defense has not brought out anything credible to establish that on 21.1.2002, the computer was tampered with or that any file was created or altered. We, therefore, hold that the I-Cards pertaining to Xansa Webcity, recovered from the deceased terrorists were computer print outs obtained from the laptop in question. We also hold that the fake Home Ministry Sticker recovered from the windscreen of the Ambassador Car used by the terrorists to make an entry into Parliament House was generated from the laptop in question.

ANNEXURE 8 – RELEVANT US CASES

Briggs v State of Maryland²⁰⁰

Terry Dewain Briggs appeals his conviction for the crime of unauthorized access to computers, in violation of Maryland Code (1957, 1996 Repl. Vol., 1997 Supp.) Article 27, § $146(c)^{201}$. The primary issue raised in this case is the meaning of the statutory requirement of access "without authorization" as used in § 146. The question we must answer is whether an employee who is entitled to use an employer's computer system in connection with employment duties, but who exceeds the scope of that authorization, is acting in a manner proscribed by Article 27, §146. Briggs contends that his conduct did not come within the prohibition of the statute. We agree, and accordingly, shall reverse.

I.

In November, 1994, the Scarborough Group, Inc. (Scarborough), a medium sized securities investment company, hired Terry Briggs as a computer programmer and system administrator. Briggs, a twenty-three-year old computer specialist, was hired to program and design software to maintain the company computer system. As part of his job responsibilities, he entered data in the computer system and placed passwords²⁰² on the files to secure the data. The management of the entire computer system was entrusted to Briggs.

Following a dispute on July 24, 1995, about the terms of his employment contract, Briggs resigned as an employee of the company.

Shortly after Briggs left the company, Scarborough realized that some of its computer files were secured with passwords known only to Briggs. Scarborough and Briggs were unable to resolve the situation. Scarborough filed a civil suit against Briggs, and also contacted the Anne Arundel County police.

²⁰⁰ IN THE COURT OF APPEALS OF MARYLAND No. 24 September Term, 1997 TERRY DEWAIN BRIGGS v. STATE OF MARYLAND

Opinion by Raker, J. Filed: January 22, 1998

²⁰¹ Unless otherwise specified, all statutory references herein shall be to Maryland Code (1957, 1996 Repl. Vol., 1997 Supp.) Article 27.

²⁰² A password, the most common form of user authentication, is used to prevent unauthorized access to a computer system. It is a sequence of characters that one must enter prior to gaining access to a computer. See Michael P. Dierks, Symposium: Electronic Communications and Legal Change, Computer Network Abuse, 6 HARV. J. L. & TECH. 307, 311 (1993).

The State charged Briggs in a two count criminal information: count one, theft of computers, in violation of Article 27, § $342(a)(1)^{203}$ and, count two, unauthorized access to computers, in violation of Article 27, § 146(c)(2). At trial, Scarborough contended that Briggs changed the passwords two days before the meeting about Briggs's employment contract, and put them in a subdirectory named "ha-ha he-he," dated July 22, 1995 by the computer. Scarborough maintained that Briggs never had permission to place the company files in a directory and to protect the file with passwords, without anyone else in the company having access to the passwords. Although he denied any knowledge about "ha-ha hehe," Briggs admitted that he placed passwords on company files months earlier as part of his job in securing files, but that he had difficulty remembering the passwords because so much time had passed. Briggs suggested that Scarborough filed criminal charges against him in order to discredit him as a government witness in a Securities and Exchange Commission investigation that Briggs had initiated alleging that certain activities at Scarborough violated federal security regulations. Briggs maintained that the computer date on the password subdirectory had been changed to incriminate him.

The State alleged that Briggs intentionally and willfully and without authorization accessed a computer system to interrupt the operation of the computer system and computer services. In his motion for judgment of acquittal, Briggs argued that he was not guilty as a matter of law (that the statute did not apply to his activities) and as a matter of fact (that he was fulfilling his employment responsibilities). Briggs reasoned that Article 27, § 146 was not intended to apply to authorized computer users who, arguably, used their positions to cause harm to their employers by misusing the computer. The State argued that Briggs was guilty of unauthorized access, because although Briggs was authorized to access the computer system, he was not authorized to access the system in such a way as to interrupt the operation of the computer services of the system. The trial court denied Briggs's motion for judgment of acquittal, and the jury found Briggs guilty of unauthorized access to computers in violation of Article 27, \S 146(c)(2)(i). The court sentenced Briggs to one year incarceration, with all but two days suspended, two years supervised probation, 150 hours of community service, and a fine of \$500. The court also ordered him to cooperate with Scarborough and required him to release any remaining password information and client files. Briggs noted a timely appeal to the Court of Special Appeals. We granted certiorari on our own motion before consideration by that court.

²⁰³ The jury acquitted Briggs of the theft charge.

Appellant argues before this Court that Article 27, § 146 criminalizes the conduct of an individual who intentionally and willfully accesses a computer without authorization and is inapplicable to conduct that can be characterized as only exceeding authorized access. He concludes that the statute is inapplicable on its face because, as part of his employment, he was authorized to access the computer system. The purpose of the statute, Appellant continues, was to deter unauthorized users from breaking into computer systems, i.e., to prevent "hackers"²⁰⁴ from gaining unauthorized access. Briggs distinguishes operating a computer system without authorization from exceeding authorized access by using the computer in an improper manner. He concludes that application of this statute to his conduct is contrary to legislative intent.

The State contends that even though access for other activities may have been authorized, a person, whether he is an employee, "hacker," or otherwise, violates the statute when that person "intentionally, willfully, and without authorization" accesses a computer system or any part of a computer system to cause the malfunction or interrupt the operations of the computer system or any part of that system. The State maintains that there was sufficient evidence to support the verdict because Briggs did not have authority to place passwords on the files without anyone else in the company having those passwords, and that he did so with the intent of interrupting the operation of the computer system.

 $^{^{\}rm 204}$ The term "hacker" has been defined as "a person who views and uses computers as objects for exploration and exploitation." NATIONAL INSTITUTE OF JUSTICE, U.S. DEPT OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL xvi (2d ed. 1989) (hereinafter CRIMINAL JUSTICE RESOURCE MANUAL). A "hacker" commonly refers to a "computer user who intends to gain unauthorized access to a computer system." Dierks, supra, at 310 n.7. The word "hacker" has become synonymous with a computer criminal, and typically refers to a person who breaks into computer networks. Id. Originally, however, the term "hacker" referred to the members of The Tech Model Railroad Club of Massachusetts Institute of Technology (TMRC) and the term "hack" referred to "a project undertaken or a product built not solely to fulfill some constructive goal, but with some wild pleasure, taken in mere involvement." Id. (quoting STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION 23 (1984)). The terms "hack" and "hacker" found their way into the computing world when the members of TMRC began work on the digital computers at Massachusetts Institute of Technology. The TMRC resents the application of the term "hacker" to mean the committing of illegal acts, maintaining that words such as "thieves," "password crackers," or "computer vandals" are better descriptions.

The standard for review of the denial of a motion for judgment of acquittal is "whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." Jackson v. Virginia, 443 U.S. 307, 319, 99 S. Ct. 2781, 2789, 61 L. Ed. 2d 560 (1979); see also State v. Albrecht, 336 Md. 475, 478-79, 649 A.2d 336, 337 (1994).

We do not inquire into the credibility of witnesses, or weigh the evidence to ascertain whether the State has proven their case beyond a reasonable doubt; that is the responsibility given to the trier of fact. Applying the above standard of review, we conclude that the conduct in this case does not constitute the crime of unauthorized access to computers, and the motion for acquittal should have been granted.

Article 27, § 146 provides, in pertinent part:

(c) Illegal access.—(1) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services.

(2) A person may not intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services to:

(i) Cause the malfunction or interrupt the operation of a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services; or

(ii) Alter, damage, or destroy data or a computer program stored, maintained, or produced by a computer, computer network, computer system, computer services, computer database, or any part of these systems or services.

(3) A person may not intentionally, willfully, and without authorization:

(i) Identify or attempt to identify any valid access codes; or

(ii) Distribute or publicize any valid access codes to any unauthorized person.

Access is defined in §146(a) as follows:

(9) "Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including, but not limited to, computers and other data processing equipment or resources connected therewith.

To support a conviction for illegal access to computers under § 146(c)(2)(i), the State must prove: (1) that Briggs intentionally and willfully accessed a computer or computer system; (2) that the access was without authorization; and (3) the access was with the intent to interrupt the operation of the computer services. We need not address Appellant's factual argument that he was authorized to place passwords on Scarborough's computer system, because we find the second element dispositive and hold that Appellant's access to the computer was not "without authorization" within the meaning of the statute.²⁰⁵ When faced with a question of statutory construction, we look first to the plain meaning of the words of the statute, with the goal to ascertain and effectuate legislative intent. Whack v. State, 338 Md. 665, 672, 659 A.2d 1347, 1350 (1995). We give the words of the statute their ordinary and natural meaning. Gargliano v. State, 334 Md. 428, 435, 639 A.2d 675, 678 (1994). If the language of the statute is plain and clear and expresses a meaning consistent with the statute's apparent purpose, no further analysis is ordinarily required. Id. at 435, 639 A.2d at 678. On the other hand, if the language of the statute is ambiguous or unclear, "we must consider 'not only the literal or usual meaning of the words but their meaning and effect in light of the setting, the objectives and purpose of the enactment,' in our attempt to discern the construction that will best

²⁰⁵ We recognize that "[b]usiness, economic, and white-collar crimes have rapidly changed as computers proliferated into the activities and environments in which these crimes occur." CRIMINAL JUSTICE RESOURCE MANUAL, supra, at 1. Scholars have noted that serious economic loss linked to computer abuse is caused by current and former employees rather than by outsiders. "In fact, the available data suggest that serious economic losses linked to computer abuse have been and continue to be attributed to current and former employees of the victimized organization rather than to interloping hackers with modems." Richard C. Hollinger and Lonn Lanza-Kaduce, The Process of Criminalizaton: The Case of Computer Crime Laws, 26 CRIMINOLOGY 101, 116 (1988). For example, use of the employer's computer for one's own purpose may be serious, as where the employee uses the employer's computer to run his or her own business through the employer's facilities, sometimes knows as "time theft." See MARTIN WASIK, CRIME AND THE COMPUTER 55 (1991). See also, CRIMINAL JUSTICE RESOURCE MANUAL, supra, at 38-9. Industrial sabotage may also be inflicted by disgruntled employees. See State v. Corcoran, 522 N.W.2d 226 (Wis. Ct. App. 1994).

further the legislative objectives or goals." Id. at 436, 639 A.2d at 678 (quoting Tucker v. Fireman's Fund Ins. Co., 308 Md. 69, 75, 517 A. 2d 730, 732 (1986)).

The statute is three-pronged. Section 146(c)(1) prohibits unauthorized access or attempted unauthorized access per se to computers. The actor's purpose or motive in accessing the computer—whether there is any intent to alter or damage the computer or the data on it—is irrelevant. Section 146(c)(2) prohibits unauthorized access or attempted access to computers with a further purpose, such as with the intent to cause a malfunction or interrupt the computer operation, or alter, damage, or destroy information. Section 146(c)(3) prohibits willful and intentional identification, publication, or distribution of valid access codes, and has no relevancy to the case before the Court. "Simple" unauthorized access, that is, without intent to damage or alter, is punishable by a maximum prison term of three years, a fine of \$1,000, or both. "Aggravated" unauthorized access is punishable by a maximum prison term of five years, a fine of \$5,000, or both.²⁰⁶

The statute prohibits unauthorized access of a computer, computer network, or computer systems. "Access" is defined in the statute "to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including . . . computers." § 146(a)(9). "Without authorization" modifies the word "access." Therefore, the unlawful act is unauthorized access. "Authorization" is not defined in the statute.²⁰⁷ Turning to dictionary definitions of "authorize," we find that

²⁰⁶ The penalty provision of Article 27, § 146 provides:

⁽d) Penalty. — (1) Any person who violates any provision of subsection (c)(1) of this section is guilty of a misdemeanor and on conviction is subject to a fine not exceeding 1,000 or imprisonment not exceeding 3 years or both.

⁽²⁾ Any person who violates any provision of subsection (c)(2) or (c)(3) of this section is guilty of a misdemeanor and on conviction is subject to a fine not exceeding \$5,000 or imprisonment not exceeding 5 years or both.

²⁰⁷ See CRIMINAL JUSTICE RESOURCE MANUAL, supra, for a discussion of technical definitions in state computer crime law. The author notes that "[t]here are now as many different and conflicting definitions of computer crime as there are states with computer crime statutes. The definitions of those terms, their comprehensibility, rate of obsolescence, and ease of application will play an important role in determining how successfully and effectively these new statutes will be used to deter and prosecute computer crime." Id. at 85.

The federal government, all of our sister states with the exception of Vermont, and most foreign countries, have responded to the problem of computer crimes. The statutes "vary widely in offense named, definitions, and sanctions." Id. at 83; see 18 U.S.C. § 1030 (1994); ALA. CODE §§ 13A-8-103 (1994 & Supp. 1996); ALASKA STAT. § 11.46.740 (1996 & Supp. 1997); ARIZ. REV. STAT.

BLACK'S LAW DICTIONARY 133-34 (6th Ed. 1990) defines "authorize" to mean "[t]o empower; to give a right or authority to act. To endow with authority or effective legal power, warrant, or right. To permit a thing to be done in the future." (Citation omitted). Similarly, WEBSTER'S NEW INTERNATIONAL DICTIONARY, UNABRIDGED 186 (2d ed. 1950) defines "authorize" to mean "to clothe with authority or legal power; to give right to act; to make legal; to legalize; to give authoritative permission to or for; to justify." The testimony at trial that Briggs had authority to enter data in the computer

ANN. § 13-2316 (1989 & Supp. 1997); ARK. CODE ANN. §§ 5-41-101 to 107 (Michie 1997); CAL. PENAL CODE § 502 (West 1988 & Supp. 1997); COLO. REV. STAT. §§ 18-5.5-101 to 102 (1997); CONN. GEN. STAT. ANN. §§ 53a-250 to 261 (West 1994 & Supp. 1997); DEL. CODE. ANN tit. 11, §§ 931 to 939 (1995 & Supp. 1996); FLA. STAT. ANN. §§ 815.01 to .07 (West 1994 & Supp. 1997); GA. CODE ANN. §§ 16-9-91 to 94 (1996 & Supp. 1997); HAW. REV. STAT. §§ 708-890 to 893 (1994 & Supp. 1997); IDAHO CODE §§ 18-2201 to 2202 (1987 & Supp. 1997); ILL. ANN. STAT. ch. 38 para. 16D-1 to 7 (Smith-Hurd 1996); IND. CODE ANN. §§ 35-43-1-4 & 35-43-2-3 (Burns 1994 & Supp. 1997); IOWA CODE ANN. §§ 716A.1 to .16 (West 1993 & Supp. 1997); KAN. STAT. ANN. § 21-3755 (1995); KY. REV. STAT. ANN. §§ 434.840 to .860 (Michie/Bobbs-Merrill 1985 & Supp. 1997); LA. REV. STAT. ANN. §§ 14:73.1 to .5 (West 1997); ME. REV. STAT. ANN. tit. 17-A, § 357 (West Supp. 1997); MD. CODE (1957, 1996 Repl. Vol., 1997 Supp.) Article 27, § 146; MASS. GEN. L. ch. 266, § 30 (1990 & Supp. 1997); MICH. STAT. ANN. § 752.791 to .797 (Callaghan 1991 & Supp. 1997); MINN. STAT. ANN. §§ 609.87 to .891 (West 1987 & Supp. 1997); MISS. CODE ANN. §§ 97-45-1 to 13 (1994 & Supp. 1997); MO. REV. STAT. §§ 537.525, 569.093 to .099 (1988 & Supp. 1997); MONT. CODE ANN. §§ 45-2-101, 45-6-310 to 311 (1997); NEB. REV. STAT. §§ 28.1343 to .1348 (1994 & Supp. 1996); NEV. REV. STAT. ANN. §§ 205.473 to .491 (Michie 1997); N.H. REV. STAT. ANN. §§ 638:16 to :19 (1986 & Supp. 1995); N.J. STAT. ANN. §§ 2C:20-23 to 34 (1995 & Supp. 1997); N.M. STAT. ANN. §§ 30-45-1 to 7 (Michie 1989 & Supp. 1996); N.Y. PENAL LAW §§ 156.00 to .50 (McKinney 1988 & Supp. 1997); N.C. GEN. STAT. §§ 14-453 to 457 (1993 & Supp. 1996); N.D. CENT. CODE ANN. § 12.1- 06.1-08 (1985 & Supp. 1997); OHIO REV. CODE ANN. §§ 2913.01, 2913.81 (Anderson 1996); OKLA. STAT. ANN. tit. 21, §§ 1951 to 1958 (West Supp. 1997); OR. REV. STAT. §§ 164.125, 164.377 (1995); 18 PA. CONS. STAT. ANN. § 3933 (1994 & Supp. 1997); R.I. GEN. LAWS §§ 11-52-1 to 8 (1994 & Supp. 1996); S.C. CODE ANN. §§ 16-16-10 to 30 (Law. Co-op. 1985 & Supp. 1996); S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to 8 (1997); TENN. CODE ANN. §§ 39-14-601 to 603 (1997); TEX. PENAL CODE ANN. §§ 33.01 to .05 (West 1989 & Supp. 1995); UTAH CODE ANN. §§ 76-6-701 to 705 (1995 & Supp. 1996); VA. CODE ANN. §§ 18.2-152.1 to .14 (Michie 1996 & Supp. 1997); WASH. REV. CODE §§ 9A.52.110 to .130 (1988 & Supp. 1996); W.VA. CODE §§ 61-3C-1 to 21 (1993 & Supp. 1997); WIS. STAT. § 943.70 (1996 & Supp. 1997); WYO. STAT. §§ 6-3-501 to 505 (1997).

and to place passwords on the files to secure the data establishes that he was authorized, under the statute, to "instruct, communicate with, store data in, retrieve data from and to make use of computer data equipment and other data processing equipment."

The plain language of the statute suggests that if an employee were initially permitted to "instruct," "communicate with," "store data in," or "retrieve data from" the computer system, then that employee's access would be authorized. The statute makes no reference to authorized users who exceed the scope of their authority. If the Legislature intended the statute to cover employees who exceeded the scope of their authority or who misused their authority, it could have done so explicitly.²⁰⁸

In addition, several states have specific offenses entitled Offenses against computer users, which criminalize the intentional denial to an authorized user of

²⁰⁸ The federal government and several of our sister states have explicitly prohibited computer use beyond the scope of authorization. See 18 U.S.C. § 1030(a)(1), (a)(2), (a)(4) (criminalizing access of a computer without authorization or "exceeding authorized access"). 18 U.S.C. § 1030(e)(6) defines the term "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." See also ARIZ. REV. STAT. ANN. § 13-2316(A) (Supp. 1997) (defining one element of computer fraud as accessing a computer without authorization or exceeding authorization of use); GA. CODE ANN. §§ 16-9-92 (1996 & Supp. 1997) (defining "without authority" to include the use of a computer in a manner that exceeds any permission granted by the owner of the computer); HAW. REV. STAT. §§ 708-890 (1994 & Supp. 1997) (defining "without authorization" to mean without the permission of or in excess of the permission of an owner); KAN. STAT. ANN. § 21-3755(b)(3) (1995) (defining computer crime as "intentionally exceeding the limits of authorization" in conjunction with causing damage); MICH. STAT. ANN. § 752.795 (Callaghan 1991 & Supp. 1997) (prohibiting a person from intentionally accessing a computer "without authorization or by exceeding valid authorization"); N.D. CENT. CODE ANN. § 12.1-06.1-08 (2) (Supp. 1997) (prohibiting access "in excess of authorization given or without authorization"); N.M. STAT. ANN. § 30-45-5 (Michie Supp. 1996) (criminalizing the unauthorized computer use of "any person who knowingly, willfully and without authorization, or having obtained authorization, uses the opportunity such authorization provides for purposes to which the authorization does not extend"); OHIO REV. CODE ANN. § 2913.04(B) (Anderson 1996) (prohibiting access of a computer "without the consent of, or beyond the scope of the express or implied consent of the owner"); OKLA. STAT. ANN. tit. 21, § 1953(3) (West Supp. 1997) (making it unlawful to willfully "exceed the limits of authorization" and damage, modify or alter a computer system); S.C. CODE ANN. § 16-16-20(1) (Law. Co-op. 1985 & Supp. 1996) (prohibiting the willful access to a computer "without authorization or for an unauthorized purpose").

We conclude that the intent of the General Assembly was to criminalize the misuse of computers or computer networks by those whose initial access was unauthorized.

The legislative history supports our reading of the statute. In 1984, in an apparent response to the inadequacies of current criminal law to address disruptive or voyeuristic acts involving computer information systems, House Bill 121, approved by both houses, and enacted as Chapter 588, 1984 Laws of Maryland, criminalized "illegal access to computers."

A representative of the Department of Budget and Fiscal Planning testified in support of the bill:

Generally speaking, th[e] threat [of computer crime] may be viewed as being divided into two reasonably identifiable types: 1) those associated with criminal intent or activity, and 2) those associated with the so called "hacker" type of activity, where just the challenge of penetrating the system, or some sort of "electronic vandalism" or other mischief is the objective. While outright criminal activity involving information systems is covered by current statute, the Department feels this bill provides a needed addition by directly addressing the second type of threat by prohibiting all unauthorized access, for whatever purpose, and by providing penalties for its occurrence.

Testimony Regarding House Bill 121, Department of Budget and Fiscal Planning (available at the Department of Legislative Reference, Bill File for House Bill 121 (1984)) (emphasis added). The legislative history thus suggests that House Bill 121 was drafted in reaction to the concern about the recent "hacker" activity. The Senate Judicial Proceedings Committee Report for House Bill 121, reported favorably by Chairman (now President of the Senate) Thomas V. Mike Miller, underscores our conclusion that the statute should apply to those who break into computers:

BACKGROUND:

Proponents of this bill testified that, under current law, simply breaking into a computer system to vandalize or cause other mischief is not illegal. Thus, the bill was introduced by those who feel unauthorized access alone should be a misdemeanor subject to penalties.

the full and effective use of or access to a computer. See, e.g., FLA. STAT. ANN. § 815.06(1) (West 1994 & Supp. 1997); LA. REV. STAT. ANN. § 73.4(A) (West 1997); MISS. CODE ANN. § 97-45-5(1)(a) (1988 & Supp. 1997); WYO. STAT. § 6-3-504 (1997).

LEGISLATIVE INTENT:

This legislation is intended to make it a misdemeanor for a person intentionally and without authorization to access, attempt to access or cause access to a computer system. *The purpose of the bill is to deter individuals from breaking into computer systems*.

Committee Report System, Summary of Committee Report, House Bill 121 (available at the Department of Legislative Reference, Bill File for House Bill 121 (1984)) (emphasis added).

The 1989 amendment to the statute, House Bill 1065, enacted as Chapter 722, 1989 Laws of Maryland, added subsections (c)(2) and (3) thereby creating two new substantive crimes with more severe penalties. Subsection (c)(2) prohibits a person from intentionally and willfully accessing a computer to cause malfunction or interrupt the operation of a computer, or to alter, damage or destroy data or program stored by a computer, and subsection (c)(3) prohibits a person from intentionally, willfully, and without authorization attempting to identify or distribute computer passwords.²⁰⁹ The Senate Judicial Proceedings Committee Bill Analysis and Floor Report concerning House Bill 1065 states:

BACKGROUND:

This bill upgrades current computer access provisions to address recent well publicized disruptions of public and private computer systems, and invasions of personal privacy by "hackers."

* * * * * *

The first new crime penalizes the damage which hackers may wreak in illegally accessed systems, above and beyond the current penalty for the access itself.

Id. (available at the Department of Legislative Reference, Bill File for House Bill 1065 (1989)). Once again, it appears that the General Assembly sought to address the perceived threat from "hackers," and, in particular, the damages that they may cause beyond mere browsing. See also Testimony Regarding House Bill 1065, Delegate Samuel Rosenberg (stating "much of the current crisis revolves around underground 'hackers'") (available at the Department of Legislative Reference, Bill File for House Bill 1065 (1989)). Contrary to the State's argument, the

 $^{^{209}}$ In addition to creating two new substantive crimes, House Bill 1065 expanded the scope of computer access activities punishable as crimes by changing the definitions such that "computer database" included data produced by a computer or computer system, or a computer network. The bill also extended the definition of "computer network" to include computers intermittently connected. Article 27, § 146(a)(1), (4).

legislative history thus suggests that House Bill 1065 was designed to enlarge the penalties related to mischievous unauthorized access, not to enlarge the definition of access. These comments and reports suggest that the intent of the Legislature was to punish access that was not initially authorized and not to punish conduct that merely exceeded authorized access.

Briggs's access was not unauthorized under Article 27, § 146, the unauthorized access to computers statute. If the law is to be broadened to include Briggs's conduct, it should be modified by the Legislature, not by this Court.

JUD	GME	NT (OF	THE	CIRC	CUIT
COU	JRT	FOR	AN	NE	ARUN	DEL
COU	JNTY	REV	'ERSE	ED.	COSTS	ТО
BE	PAID) BY	AN	INE	ARUN	DEL
COUNTY.						

Pennsylvania v. Michael Murgallis²¹⁰

¶1 This is an appeal from judgment of sentence imposed after a jury convicted appellant of five counts of unlawful use of a computer, 18 Pa.C.S.A. \$3933(a)(1), five counts of theft by deception, 18 Pa.C.S.A. \$3922, and two counts of bad checks, 18 Pa.C.S.A. \$4105(a)(1). Appellant was sentenced to an aggregate term of imprisonment of three to six years and a consecutive term of two years probation.

 $\P 2$ The facts, as gleaned from the record, are that from April through June 1997, appellant used an e-mail account on the Internet to sell and to receive various items of aquarium equipment. Certain items for which he had received payment from the victims were not delivered by appellant to them.

Other items which were provided to appellant by several victims pursuant to e-mail contacts were not paid for because appellant remitted checks drawn on closed accounts. Contact between the victims and appellant was made through e-mail accounts and web pages maintained on the Internet by appellant and others advertising the merchandise.

 \P 3 Appellant presents two issues for review challenging the sufficiency of the evidence and the legality of his sentence. We have reviewed the merits of each and find that no relief on appeal is warranted. Accordingly, we affirm the judgment of sentence.

¶4 The first issue questions the sufficiency of the evidence to support the convictions of unlawful use of a computer. Appellant argues that use of email through the Internet fails to fall within the statutory prohibition of unlawful use of a computer, 18 Pa.C.S.A. $\S3933(a)(1)$, in that the Internet is not a "computer system" and the use of e-mail is not "accessing" a computer system.

¶5 The relevant statutory provisions are as follows:

²¹⁰ 2000 PA Super 167 IN THE SUPERIOR COURT OF PENNSYLVANIA COMMONWEALTH OF PENNSYLVANIA, Appellee v. MICHAEL MURGALLIS, : Appellant : NO. 189 MDA 1999 Appeal from the Judgment of Sentence Entered November 20, 1998 In the Court of Common Pleas of LUZERNE County CRIMINAL NO. 4066 OF 97 BEFORE: CAVANAUGH, MUSMANNO and BROSKY, JJ. OPINION BY CAVANAUGH, J.: Filed: June 2, 2000 Offense defined – A person commits an offense if he:

(1) accesses, alters, damages or destroys any computer, computer system, computer network, computer software, computer program or data base or any part thereof, with the intent to interrupt the normal functioning of an organization or to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises;

Definitions- As used in this section the following words and phrases shall have the meanings given to them in this subsection:

"Access." To intercept, instruct, communicate with store data in, retrieve data from or otherwise make use of any resources of a computer, computer system, computer network or database.

"Computer network." The interconnection of two or more computers through the usage of satellite, microwave, line or other communication medium.

"Computer system." A set of related, connected or unconnected computer equipment, devices and software.

18 Pa.C.S.A. §3933(a), (c).

¶6 Appellant was charged in the information filed against him with five counts of violation of \$3933(a)(1). Each of the five counts alleging violation of the statute quoted the complete definition of the offense as contained in \$3933(a)(1), and added, "...to wit, did access a computer system, the 'internet,' to defraud or deceive or control" specified merchandise or U.S. currency. Therefore, appellant was charged with violation of \$3933(a)(1) through any actions or means specified by the above-quoted statutory language.

¶7 "The Internet is an international network of interconnected computers." Reno v. ACLU, 521 U.S. 844, 117 S.Ct. 2329, 138 L.Ed.2d 874, 884 (1997). "Individuals can obtain access to the Internet from many different sources, generally hosts themselves or entities with a host affiliation." Id. "Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods ...[including] electronic mail ('e-mail')...and the World Wide Web." Id. "E-mail enables an individual to send an electronic message - generally akin to a note or letter - to another individual or to a group of addressees." Id. At 885. "The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in

some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world." Id.

¶8 The record demonstrates that appellant communicated with each of the five victims through e-mail either to sell or to buy merchandise. Although telephone communications were also established, each victim was either the initiator or the recipient of e-mail communication with appellant via the Internet.

¶9 Appellant argues that no expert evidence was offered to prove that the Internet is a "computer system." We find that the apt description of the Internet, as contained in Reno v. ACLU, supra, as "an international network of interconnected computers" has become commonly understood by laypersons and this causes it to fall within the definition of "computer network" contained in §3933(c) without need for expert testimony.

Therefore, sufficient evidence was presented to establish the element of the offense that appellant accessed a computer network.

¶10 As noted above, the information charged appellant with, inter alia, accessing a computer network. The fact that it referred to the Internet as a "computer system" is of no relevance since a variance between the information and the proof at trial is not fatal as long as the defendant had adequate notice of the nature of the crime and it does not cause prejudicial surprise. Com. v. Lohr, 503 Pa. 425, 468 A.2d 1375 (1983); Com. v. Johnson, 719 A.2d 778, 783, n.4 (Pa. Super. 1998).

¶11 Appellant does not maintain that he was surprised or in any manner prejudiced by the, perhaps erroneous, reference in the information to the Internet as a "computer system" rather than a "computer network." We find no prejudice in the inconsequential use of the statutory language.

¶12 The next basis upon which appellant challenges the sufficiency of the evidence is that use of e-mail is not within the statutory definition of "access." We find that the evidence supports the finding that appellant communicated with or otherwise made use of resources of a computer network. The sending of an electronic message over the Internet falls within the statutory definition of access.

 $\P13$ Sufficient evidence is in the record to sustain the convictions of unlawful use of a computer.

¶14 Appellant's second issue is whether the theft by deception convictions merged for sentencing purposes with the convictions of unlawful use of a computer. Where an actor commits a single criminal act, the sentences for multiple convictions based upon that act merge if one offense is a lesser included offense of the other. Com. v. Rippy, 732 A.2d 1216, 1223 (Pa. Super. 1999) (citing Com. v. Anderson, 538 Pa. 574, 650 A.2d 20 (1994)).

A lesser included offense is one whose elements are a necessary subcomponent but not a sufficient component of elements of the other crime. Id. (citing Com. v. Comer, 552 Pa. 527, 716 A.2d 593 (1998)).

 $\P15$ The statutory provisions for the offense of theft by deception are as follows:

Offense defined- A person is guilty of theft if he intentionally obtains or withholds property of another by deception. A person deceives if he intentionally:

(1) creates or reinforces a false impression, including false impressions as to law, value, intention or other state of mind; but deception as to a person's intention to perform a promise shall not be inferred from the fact alone that he did not subsequently perform the promise;

(2) prevents another from acquiring information which would affect his judgment of a transaction; or

(3) fails to correct a false impression which the deceiver previously created or reinforced, or which the deceiver knows to be influencing another to whom he stands in a fiduciary confidential relationship.

18 Pa.C.S.A. §3922(a).

¶16 Appellant argues that theft by deception is a lesser included offense of unlawful use of computer. He is mistaken. The offense of unlawful use of computer does not have as an element the obtaining or withholding property of another as does theft by deception. The offense of unlawful use of computer is committed where a person accesses a computer network with the intent to devise or execute any scheme or artifice to defraud by means of false or fraudulent pretense, representations, or promises. The actual obtaining or withholding of the property is not an element of unlawful use of a computer. The sentence imposed is a legal one and no merger of sentences is necessary.

¶17 Judgment of sentence affirmed.

List of Adjudicating Officers

For the States

(1) Andhra Pradesh

Secretary, IT&C Department, Government of Andhra Pradesh, Room No.431/A, D-Block, 3rd Floor, Secretariat, Hyderabad Pin: 500022

(2) Arunachal Pradesh

Commissioner (IT), Govt. of Arunachal Pradesh, Civil Secretariat, Itanagar - 791 111, Arunachal Pradesh

(3) Assam

Comm. & Secretary IT,Govt. of Assam, Block D, 3rd Floor, Assam Secretariat, Dispur, Guwahati - 781 006 Assam

(4) Bihar

Principal Secretary, Information Technology Energy Department Sichai Bhawan, Patna, Bihar

(5) Chhattisgarh

Special Secretary, Incharge Secretary, CM Secretariat, Mantralaya, Raipur - 492001, Chhattisgarh

(6) Goa

Secretary IT, New Secreatriat Complex, Porovorim, Bardez, Goa-403521

(7) Gujarat

Secretary IT, Govt. of Gujarat, Block -7, 5th Floor, New Sachivalaya Complex, Gandhinagar - 382010

(8) Haryana

Financial Commissioner & Principal Secretary IT & Industries, R. No. 46, 9th Floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001, Haryana

(9) Himachal Pradesh

Secretary IT,Govt. of Himachal PradeshRoom No. E-112, Armsdale Building, HP Secretariat, Shimla - 171 002, Himachal Pradesh

(10) Jammu & Kashmir

Principal Secretary, Information Tech. Department, Government of Jammu & Kashmir

(11) Jharkhand

Secretary IT, Room No.307, 3rd Floor, Project Building, Dhurwa, Ranchi - 834 001

(12) Karnataka

Prn. Secretary IT, BT and S&T,6th Floor, 5th Stage M.S.Building, Dr. B.R.Ambedkar Veedhi, Bangalore-560 001, Karnataka

Prn Secretarty to Government, Govt. of Karnataka, DPAR(e-Governance), Room No.106, 1st Floor, M.S.Building, Gate No.2, Bangalore-560001

(13) Kerala

Secretary IT, ICT Campus, Vellayambalam Kerala Secretariat Govt. Of Kerala Trivandrum 695 033

(14) Madhya PradeshSecretary IT, Dept. of IT, Room No.533, Mantralaya, Bhopal 462 004

(15) Maharashtra

Secretary IT, Room No. 514, Anex 5th Floor, Mantralaya, Mumbai-400 032, Maharashtra

(16) Manipur

Comm. and Secretary S&T and IT, Room No. 5, North Block, Manipur Secretariat, Imphal-795001, Manipur

(17) Meghalaya

Prn. Secretary IT, Govt. of Meghalaya, Main Secretariat Building Shillong-793 001, Meghalaya

Commissioner & Secretary IT Department Govt. of Meghalaya,Room No. 315Addl. Secretariat Building, Shillong - 793 001

(18) Mizoram

Secretary ICT, Government of Mizoram Civil Secretariat Annex-2, Aizawl-796001, Mizoram

(19) Nagaland

Secretary, Department of Information Technology & Communication, Nagaland Civil Secretariat, Kohima, Nagaland.

(20) Orissa

Comm. & Secretary IT, Information Technology Deptt., Orissa Computer Application Centre Building, Jayadev Vihar, Bhubaneswar-751001, Orissa

(21) Punjab

Secretary IT, Room No. 710, Floor 7, Punjab Mini Civil Secretariat, Sector 9, Chandigarh, Punjab

(22) Rajasthan Room No. 2024, Main Bldg, Secretariat, Jaipur- 302005

(23) Sikkim

Top Floor, Annexe-I Secretariat, Kazi Road, Gangtok-737101 Sikkim

(24) Tamil Nadu Secretary to the Government, IT Deptt. Secretariat, Chennai - 600 009

(25) Tripura Commissioner & Secretary IT,R.No. 144, Ground Floor Secretariat, Agartala-799 001, Tripura (26) Uttar Pradesh

Prn. Secretary IT,1st Floor, Bapu Bhawan, Lucknow- 226 001, Uttar Pradesh

(27) Uttarakhand

Secretary IT,Govt. of Uttarakhand,Uttaranchal Secretariat,Subash Road, Dehradun- 248001, Uttarakhand

(28) West Bengal

Govt. of WB, Deptt. of IT, Advantage Bengal Building, 4, Camac Street, 7 th Floor, Kolkata 700 016

For the Union Territories

(1) Andaman & NicobarSecretary IT, Andaman & Nicobar Admn. Secretariat, Port Blair-744101

(2) Chandigarh

Finance Secretary-cum-Secretary IT, UT Secretariat, Sector 9, Chandigarh UT

(3) Dadra & Nagar HaveliFinance Secretary, 1st Floor, Secretariat, 66 KV Road, Amli, SILVASSA - 396 230, Dadra & Nagar Haveli UT

(4) Daman & DiuFinance Secretary, Secretariat, Fort Area, Moti Daman, DAMAN-396220(UT of Daman & Diu)

(5) Delhi

Secretary IT, Deptt. of IT, Room No. 902, 9th Level, B Wing, Delhi Secretariat, IP Estate, New Delhi- 110002

(6) Lakshadweep

Secretary IT, Department of IT, Secretariat, UT of Lakshadweep, Kavarati - 682 555

Director IT, Department of IT, UT of Lakshadweep, Kavaratti - 682 555, Lakshadweep UT

(7) Puducherry

Special Secretary Transport & IT, Govt. of Puducherry, Gobert Avenue, Chief Secretariat, Puducherry - 605 001