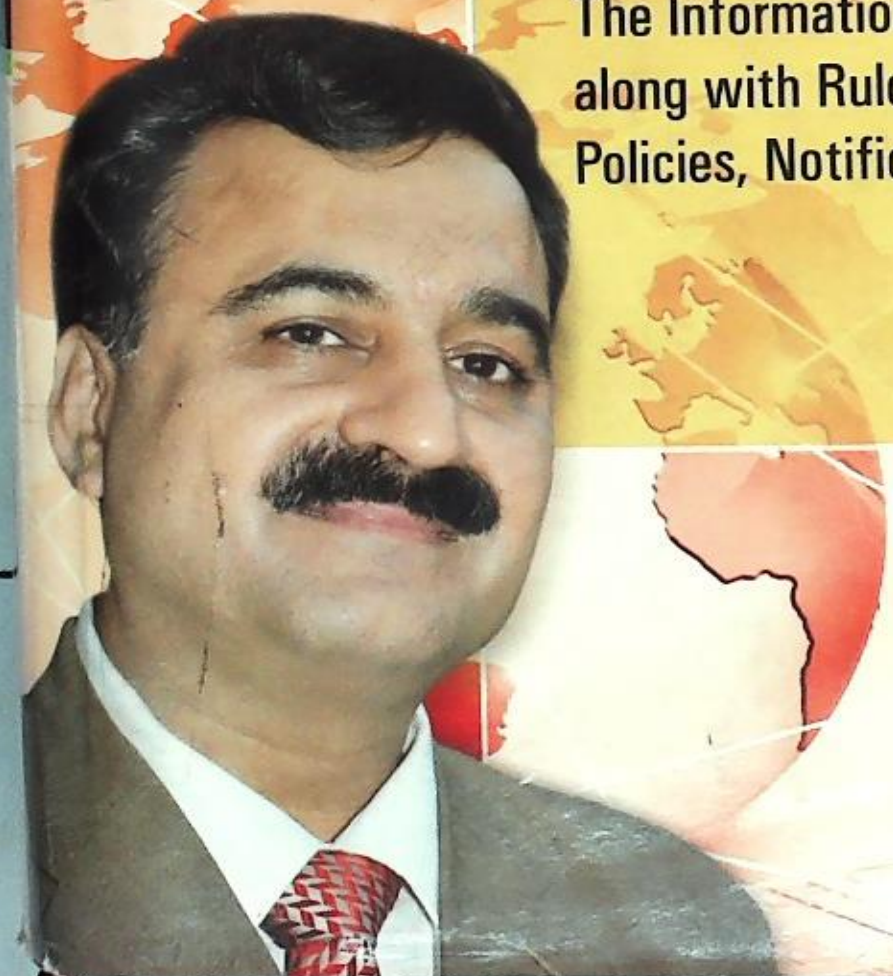
Pavan Duggal

Cyber Law

An exhaustive section wise Commentary on The Information Technology Act along with Rules, Regulations, Policies, Notifications etc.



Universal Law Publishing Co.
NEW DELHI - INDIA

Cyber Law 3.0

An exhaustive section wise commentary on
The Information Technology Act
along with Rules, Regulations,
Policies, Notifications etc.

Pavan Duggal
Advocate, Supreme Court of India

Universal
Law Publishing Co. Pvt. Ltd.
NEW DELHI - INDIA

CONTENTS

Foreword vii
Preface ix
Cyberlaw 3.0 xi
Cyber Law – An Introduction xiii
Table of Cases xxvii

CHAPTER I
PRELIMINARY

Objectives 1
Applicability 1
Jurisdiction 2
Negotiable Instrument 9
Power-of-Attorney 9
Trust 9
Will 10
Conveyance 10
Section 2 – Definitions 13
Section 2(1)(a) – Access 16
Section 2(1)(b) – Addressee 17
Section 2(1)(c) - Adjudicating Officer 17
Section 2(1)(d) – Affixing Electronic Signature 18
Section 2(1)(e) – Appropriate Government 18
Section 2(1)(f) – Asymmetric Crypto System 19
Section 2(1)(ha) – Communication Device 21
Section 2(1)(j) – Computer Network 24
Section 2(1)(k) – Computer Resource 26
Section 2(1)(l) – Computer System 27
Section 2(1)(m) – Controller 28
Section 2(1)(n) – Cyber Appellate Tribunal 28
Section 2(1)(na) – Cyber Cafe 28
Section 2(1)(nb) – Cyber Security 29
Section 2(1)(o) – Data 30
Section 2(1)(p) 30
Section 2(1)(q) – Digital Signature Certificate 31
Section 2(1)(r) – Electronic Form 31
Section 2(1)(s) – Electronic Gazette 32
Section 2(1)(t) – Electronic Record 32
Section 2(1)(ta) – Electronic Signature 32
Section 2(1)(tb) – Electronic Signature Certificate 33
Section 2(1)(u) – Function 33
Section 2(1)(ua) – Indian Computer Emergency Response Team 33
Section 2(1)(v) – Information 34

Section 2(1)(w) – Intermediary 34
Section 2(1)(x) 35
Section 2(1)(y) – Law 35
Section 2(1)(z) – Licence 36
Section 2(1)(za) – Originator 36
Section 2(1)(zb) 37
Section 2(1)(zc) – Private Key 37
Section 2(1)(zd) – Public Key 37
Section 2(1)(ze) – Secure System 37
Section 2(1)(zf) – Security Procedure 38
Section 2(1)(zg) – Subscriber 38
Section 2(1)(zh) – Verify 38
Section 2(2) 39

CHAPTER II

DIGITAL SIGNATURE & ELECTRONIC SIGNATURE

Section 3 – Authentication of Electronic Records 40
Section 3A – Electronic Signature 42

CHAPTER III

ELECTRONIC GOVERNANCE

Section 4 – Legal Recognition of Electronic Records 45
Section 5 – Legal Recognition of [Electronic Signature] 48
Section 6 49
Section 7 – Retention of Electronic Records 53
Section 7A – Audit of Documents, Etc. Maintained In Electronic Form 55
Section 8 – Publication of rule, regulation, etc., in Electronic Gazette 55
Section 10 – Power to Make rules by Central Government in Respect of Electronic Signature 57
Section 10A – Validity of contracts through electronic means 57

CHAPTER IV

ATTRIBUTION, ACKNOWLEDGEMENT AND DISPATCH OF ELECTRONIC RECORDS

Section 11 – Attribution of Electronic Records 61
Section 12 – Acknowledgement of Receipt 62
Section 13 – Time and Place of Despatch and Receipt of Electronic Record 65

CHAPTER V

SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES

Section 14 – Secure Electronic Record 70
Section 15 – Secure Electronic Signature 71
Section 16 – Security Procedures and Practices 72

CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

Section 17 – Appointment of Controller and other Officers 74
Section 18 – Functions of Controller 75
Section 19 – Recognition of foreign Certifying Authorities 77
Section 20 – Controller to Act as Repository 79
Section 21 – Licence to Issue Electronic Signature Certificates 79
Section 22 – Application for Licence 80
Section 23 – Renewal of Licence 82
Section 24 – Procedure for Grant or Rejection of Licence 83
Section 25 – Suspension of Licence 85
Section 26 – Notice of Suspension or Revocation of Licence 88
Section 30 – Certifying Authority to Follow Certain Procedures 95
Section 31 – Certifying Authority to Ensure Compliance of the Act, etc. 97
Section 32 – Display of Licence 97
Section 33 – Surrender of Licence 98
Section 34 – Disclosure 99

CHAPTER VII

ELECTRONIC SIGNATURE CERTIFICATES

Section 35 – Certifying Authority to Issue Electronic Signature Certificate 101
Section 36 – Representations upon Issuance of Digital Signature Certificate 105
Section 37 – Suspension of Digital Signature Certificate 106
Section 38 – Revocation of Digital Signature Certificate 107
Section 39 – Notice of Suspension or Revocation 109

CHAPTER VIII

DUTIES OF SUBSCRIBERS

Section 40 – Generating Key Pair 111
Section 40A – Duties of Subscriber of Electronic Signature Certificate 112
Section 41 – Acceptance of Digital Signature Certificate 112
Section 42 – Control of Private Key 114

CHAPTER IX

PENALTIES, COMPENSATION AND ADJUDICATION

Section 43 – Penalty and compensation for damage to computer, computer system, etc. 116
Section 43A – Compensation for Failure to Protect Data 117
Section 44 – Penalty for Failure to Furnish Information Return, etc. 133
Section 45 – Residuary Penalty 134
Section 46 – Power to Adjudicate 135
Section 47 – Factors to be taken into Account by the Adjudicating Officer 140

CHAPTER X
THE CYBER APPELLATE TRIBUNAL

Section 48 – Establishment of Cyber Appellate Tribunal 142
Section 49 – Composition of Cyber Appellate Tribunal 142
Section 50 – Qualifications for Appointment as Chairperson and Members of Cyber Appellate Tribunal 145
Section 51 – Term of office, conditions of service, etc., of Chairperson and Members 147
Section 52 – Salary, allowances and other terms and conditions of service of Presiding Officer 147
Section 52A – Powers of Superintendence, Direction, etc. 148
Section 52B – Distribution of Business among Benches 148
Section 52C – Powers of the Chairperson to Transfer Cases 149
Section 52D – Decision by Majority 149
Section 53 – Filling-up of Vacancies 150
Section 54 – Resignation and Removal 151
Section 55 – Orders Constituting Appellate Tribunal to be Final and not to Invalidate its Proceedings 152
Section 56 – Staff of the Cyber Appellate Tribunal 153
Section 57 – Appeal to Cyber Appellate Tribunal 153
Section 58 – Procedure and Powers of the Cyber Appellate Tribunal 159
Section 59 – Right to Legal Representation 161
Section 60 – Limitation 161
Section 61 – Civil Court not to have Jurisdiction 162
Section 62 – Appeal to High Court 163
Section 63 – Compounding of Contraventions 164
Section 64 – Recovery of Penalty or Compensation 166

CHAPTER XI
OFFENCES

Introduction 168
Cybercrimes can be basically divided into three major categories 169
Cybercrimes Against Persons 169
Cybercrimes against Property 169
Cybercrimes against Government 170
Cybercrimes – A Turning Point 171
International Cybercrime Treaty 171
Section 65 – Tampering with Computer Source Documents 174
Section 66 – Computer-Related Offences 177
Section 66A – Punishment for Sending Offensive Messages through Communication Service, etc. 183
Section 66B – Punishment for Dishonestly Receiving Stolen Computer Resource or Communication Device 188
Section 66C – Punishment for Identity Theft 189

Section 66D – Punishment for Cheating by Personation by Using Computer Resource 190
Section 66E – Punishment for Violation of Privacy 192
Section 66F – Punishment for Cyber Terrorism 198
Section 67 – Punishment for Publishing or Transmitting Obscene Material in Electronic Form 203
Section 67A – Punishment for Publishing or Transmitting of Material Containing Sexually Explicit act, etc., in Electronic Form 223
Section 67B – Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc., in Electronic Form 227
Section 67C – Preservation and Retention of Information by Intermediaries 232
Section 69 – Power to Issue Directions for Interception or Monitoring or Decryption of any Information through any Computer Resource 235
Section 69A – Power to Issue Directions for Blocking for Public Access of any Information through any Computer Resource 253
Section 69B – Power to Authorize to Monitor and Collect Traffic Data or Information through any Computer Resource for Cyber Security 259
Section 70 – Protected System 266
Definition of National Security 267
Definition of Economy 268
Definition of Public Health or Safety 268
Section 70A – National Nodal Agency 272
Section 70B – Indian Computer Emergency Response Team to Serve as National Agency for Incident Response 273
Section 71 – Penalty for Misrepresentation 276
Section 72 – Penalty for Breach of Confidentiality and Privacy 278
Section 72A – Punishment for Disclosure of Information in Breach of Lawful Contract 281
Section 73 – Penalty for Publishing Electronic Signature Certificate False in Certain Particulars 284
Section 74 – Publication for Fraudulent Purpose 285
Section 75 – Act to Apply for Offence or Contravention Committed Outside India 286
Section 76 – Confiscation 286
Section 77 – Compensation, Penalties or Confiscation not to Interfere with other Punishment 287
Section 77 – Penalties or Confiscation not to Interfere with other Punishments 288
Section 77A – Compounding of Offences 288
Section 77B – Offences with three Years Imprisonment to be Bailable 294
Section 78 – Power to Investigate Offences 296

CHAPTER XII
INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

Section 79 – Exemption from Liability of Intermediary in Certain Cases 297
Harmful 315

Harass 315
Blasphemous 316
Defamatory 316
Obscene 316
Pornography/Pornographic 316
Pedophilia 317
Libellous 318
•Invasion of Privacy 318
Hateful 319
Racially 319
Ethnically 319
Disparaging 320
Money Laundering 320
Gambling 320
Sovereignty 322
Integrity 323
Unity 323
Public Order 324
Security 325
Defence 325
Insult 325
Cognizable Offence 325
Incitement 325

CHAPTER XIIA
EXAMINER OF ELECTRONIC EVIDENCE

Section 79A – Central Government to Notify Examiner of Electronic Evidence 350

CHAPTER XIII
MISCELLANEOUS

Section 80 – Power of Police Officer and Other Officers to Enter, Search, etc. 353
Section 81 – Act to have Overriding Effect 355
Section 81A – Application of the Act to Electronic Cheque and Truncated Cheque 358
Section 82 – Chairperson, Members, Officers and Employees to be Public Servants 360
Section 83 – Power to give Directions 362
Section 84 – Protection of Action Taken in Good Faith 363
Section 84A – Modes or Methods for Encryption 365
Section 84B – Punishment for Abetment of Offences. 367
Section 85 – Offences by Companies 370
Section 86 – Removal of Difficulties 372

Section 87 – Power of Central Government to make Rules 375
Section 88 – Constitution of Advisory Committee 376
Section 89 – Power of Controller to make Regulations 386
Section 90 – Power of State Government to make Rules 387
• The Information Technology (Certifying Authorities) Rules, 2000 391
• The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 393
• The Information Technology (Certifying Authority) Regulations, 2001 439
• The Information Technology (Other Powers of Civil Court Vested in Cyber Appellate Tribunal) Rules, 2003 446
• The Information Technology (Other Standards) Rules, 2003 460
• The Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 461
• The Information Technology (Security Procedure) Rules, 2004 462
• The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 463
• The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 464
• The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 470
• The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 475
• The Information Technology (Intermediaries Guidelines) Rules, 2011 479
• The Information Technology (Guidelines for Cyber Cafe) Rules, 2011 483
• The Information Technology (Electronic Service Delivery) Rules, 2011 486
• The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2009 489
• Interoperability Guidelines for Digital Signature Certificates Issued under Information Technology Act 492
• Report of the Group of Experts on Privacy 497
• Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds 554
• Framework for Delivery of Basic Financial Services Using Mobile Phones 618
• Framework & Guidelines for Use of Social Media for Government Organisations 829
• National Telecom Policy, 2012 869
• National Policy on Information Technology, 2012 889
• National Cyber Security Policy 900
• In Internet Domain Name 905
• Internet Banking in India – Guidelines 917
• Notifications 921

Subject Index 925 928

CHAPTER IX

PENALTIES, COMPENSATION AND ADJUDICATION

India pioneered the Business Process Outsourcing industry, providing a fertile framework for processing of outside information within India.

As time has passed, India has seen the emergence of various legal challenges pertaining to preservation and protection of sensitive personal data and information. It is pertinent to note that India does not have a dedicated legislation on data protection. However, India has put in place, law pertaining to protection and preservation of sensitive personal data and information. This is by virtue of the Information Technology Act, 2000 as amended, which has not only granted legality to data and sensitive personal data and information but has also stipulated parameters for its protection and preservation. As such, the Indian Cyberlaw has various compliance requirements for various entities and body corporates who are dealing, handling, possessing or processing any sensitive personal data or information.

The Government has also notified what all constitutes sensitive personal data and information in India. Given the fact that today large numbers of body corporates are data repositories, having lot of data and sensitive personal data or information on their computer systems, it becomes absolutely imperative for these body corporates to comply with the provisions of Indian Cyberlaw.

We now examine the relevant provision of law pertaining to sensitive personal data or information, being section 43A of the amended Information Technology Act, 2000. This provision states as under:—

Section 43 – Penalty and compensation for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,—

(a) accesses or secures access to such computer, computer system or computer network [4][or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

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

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

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

(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;

(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,

(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;

(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;

he shall be liable to pay damages by way of compensation to the person so affected.

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 database" 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 or 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 rearrange 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.

Section 43A – Compensation for Failure to Protect Data

"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 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."

Section 43A has been enacted with a view to give a fresh look to India's technology dedicated law.

It may be pointed out that for achieving the aforesaid purpose an Expert Committee was set up by the government in January, 2005 under the Chairmanship of the Secretary, Department of Information Technology, Government of India. The Expert Committee comprised various representatives of the Government, legal experts in the areas of Cyber Laws, Service Providers, representatives of IT Industry and apex industry Associations, National

Association for Software Companies (NASSCOM) and Manufacturers Association of Information Technology (MAIT). The mandate of the Expert Committee was to review the provisions of the IT Act, 2000, to consider the feasibility of making the Act technology neutral and recommend necessary amendments to that effect, and to recommend suitable legislation for Data Protection under the Act.

The Information Technology (Amendment) Bill, 2006 was introduced in Lok Sabha on 15th December, 2006 and referred to the Parliamentary Standing Committee for detailed examination and report. After considering and paying due attention to such views/suggestions and clarifications, the Parliamentary Standing Committee attempted, in this Report, to suggest and recommend certain measures to be taken by the Government for making the law more effective and comprehensive.

It is pertinent to point out that the Committee recommended to add the new section 43A for compensation for failure to protect data (Clause 20), as follows:

> *"The Committee notes that under the proposed new section 43A, obligation is cast upon 'body corporate' for paying damages through compensation. The industry representatives are of the view that the obligation to pay damages by way of compensation should also extend to any person operating the information alongwith the body corporate owning or controlling personal information. According to the Department, the issue was extensively debated by the Expert Committee in consultation with industry representatives like NASSCOM and then it was decided to restrict the section to body corporates alone. The Committee appreciating the position recommended that the obligation of paying damage through compensation for the time being be restricted to body corporate only. Extension of the section to individuals may be considered once the system is put in place and experience gained."*

The Committee observed that clause 20 of the Bill proposes to insert a new section 43A which provides to impose a fine not exceeding Rs. 5 crore upon body corporates in case of being negligent in implementing and maintaining reasonable security practices and procedures. The Committee also noted that initially an amount of Rs. 25 crore was suggested as fine, but upon the insistence of the industry it was decreased to Rs. 5 crore. According to the industry, Rs. 5 crore as prescribed under the law, is a sufficient deterrent because certainty of punishment and not necessarily the extent is what matters. The industry further submitted that the Courts of Law generally give the benefit of doubt to the defendant in severe punishment cases where evidence is not completely fool proof. The Committee was in absolute disagreement with the views expressed by the industry in suggesting the fine at Rs. 5 crore. They felt that on the plea of certainty of punishment, the extent of fine should not be on the lower side. Moreover, the Court judgments are perceivably based on fool proof evidences, irrespective of the severity of cases. The Committee, therefore, urged the Department to restore at least the originally suggested amount of Rs. 25 crore as damages by way of compensation to be imposed upon the body corporates for negligence in implementing and maintaining reasonable security practices and procedures. The Committee was hopeful that such an increase commensurate with the magnitude of the IT industry, will send a right message to the stakeholders across the globe.

The Committee also found that as per the existing mechanism for imposition of the damage of Rs. 5 crore, the victim has to go to the Adjudicator, then to the Cyber Tribunal and as a last resort to the High Court and the Supreme Court. The Committee felt that it was too cumbersome a procedure which had been corroborated by the industry when they have stated that in not a single case in the last several years even one rupee damage by way of compensation had been awarded in India. The Committee, therefore, desired that the Department should initiate action in consultation with other appropriate agencies to simplify the complicated adjudication process so that the remedy of providing damages by way of compensation is effectively implemented.

The Committee observed that as of now there is no specific provision in the Bill for protection and retention of data as agreed to by the industry, investigating agencies, legal experts and the Legislative Department, albeit the principal Act draws sustenance in this regard from other enabling laws. In the opinion of the Committee, it is but essential that there should be clear-cut and specific provisions for data protection and retention in the amended Act as the retention of accurately recorded, protected and retrievable research data is of utmost importance for facilitating scientific integrity and investigations.

The Committee also felt that specific provisions prescribing suitable punitive measures for the recipient of stolen data need to be incorporated in this section. This is one field where the intentions of the recipient are not above board in most of the cases and hence the culpability aspect cannot be overlooked or ignored.

As regards the issue of personal privacy, the Committee was not convinced by the logic extended by DIT about non-inclusion of specific provisions in this regard in the Bill as the issue requires a wider debate. Ideally, the Committee would have preferred the inclusion of this important aspect in the draft Bill itself, however, this was not done. Now that the Department have veered towards the view taken by the Committee, they would like the Department to add suitable provisions to define and protect personal privacy.

The Committee further noted that, according to the explanation of the Department, the terms wrongful loss and wrongful gain are being co-opted in the Bill in tune with the IPC where these words are well defined. At the cost of appearing repetitive, the Committee would like to impress upon the Department that in order to make the new law a more comprehensive and user friendly one, these terms ought to be defined unambiguously and definitely in the context of information technology/cyber-related matters/contraventions".

The Government of India accepted the recommendations to enact the new section 43A with some modifications. In the proposed section 43A, damages by way of compensation was limited to 5 crores, but in the amended Information Technology Act, 2000, the damages by way of compensation are unlimited.

Section 43A has been inserted in the Information Technology Act, 2000 by means of the Information Technology (Amendment) Act, 2008. The said section came into effect from 27th October, 2009. Section 43A has been added for the purposes of providing statutory liability to pay damages by way of compensation, in case if the body corporate would fail to protect the sensitive personal data or information of the provider of information. However, Section 43A is slightly different from its scope than section 43 of the Information Technology Act, 2000. While section 43A of the Information Technology Act, 2000 deals with compensation for damages to computers, computer systems and computer networks and for various unauthorised activities as detailed therein, section 43A has a different focus altogether. Section 43A is focused on the civil exposure of legal entities to pay damages by way of compensation for their failure to protect data.

Section 43A is structured in a manner where it actually stipulates the observance of certain mandatory parameters and if in the event of any negligence in the observance of such mandatory parameters, any loss or gain is caused to any person, it becomes the basis for the concerned legal entity to pay damages by way of compensation.

The first thing to note about section 43A is that it is applicable to that body corporate which is possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates. *Explanation (i)* to section 43A provides the body corporate to mean the following:

(a) Any company;
(b) A firm;
(c) Sole proprietorship; or

(d) Other association of individuals engaged in commercial or professional activities.

Thus, the way in which a body corporate has been defined is very vast and its scope applies to all legal entities, barring trusts and associations of individuals engaged in not-for-profit activities.

Since the body corporate includes not just a company but also a firm and sole proprietorship, all intermediaries as defined under section 2(1)(w) of the Information Technology Act, 2000 would also qualify as body corporates. The net effect of that would also be that all intermediaries dealing, handling or processing with sensitive personal data would be required to comply with the mandatory provisions of section 43A of the Information Technology Act, 2000.

It is pertinent to point out here that the Parliamentary Standing Committee submitted its report to the Government. The recommendations from the Parliamentary Standing Committee, headed by Sh. Nikhil Kumar, Member of Parliament, specifically recommended that the term 'intermediary' does not include 'body corporate' as referred to in section 43(A) of the principal Act.

The Parliamentary Standing Committee recommended the definition of the term "intermediary" as below:

'(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 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, but does not include body corporate referred to in section 43A;'.

Despite the Parliamentary Standing Committee recommendation, the Government deliberately included the intermediary within the ambit of 'body corporates' referred to in section 43A.

Further, section 85 of the Information Technology Act, 2000 would be applicable to such body corporates including companies in the event of the company committing a contravention of provisions of the Information Technology Act, 2000, including section 43A. As per section 85, if a person committing a contravention of the provisions of the Information Technology Act, 2000 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 said contravention and shall be liable to be proceeded against and punished accordingly.

Section 43A has got the following salient parameters:

(a) A body corporate must be possessing any sensitive personal data; or
(b) A body corporate must be dealing with any sensitive personal data or information in a computer resource; or
(c) A body corporate must be handling any sensitive personal data and information in a computer resource;
(d) The said computer resource must be owned, controlled or operated by the concerned body corporate;
(e) The body corporate is mandated and required to implement and maintain reasonable security practices and procedures;
(f) The body corporate is mandated not to be negligent in the implementation and maintaining of reasonable security practices and procedures;
(g) And as a cause of negligence of the body corporate in implementing and maintaining reasonable security practices and procedures, the body corporate causes wrongful loss to any person; or
(h) As a result of the negligence of the body corporate in implementing and maintaining reasonable security practices and procedures, the body corporate causes wrongful gain to any person or itself.

If the abovesaid conditions are fulfilled, the said body corporate shall be mandatorily liable to pay damages by way of compensation to the person so affected.

A bare reading of section 43A clearly shows that it has not put a cap on the quantum of damages by way of compensation. Thus, section 43A provides for unlimited damages by way of compensation.

When one examines the structure of section 43A, it is focused on protecting and preserving sensitive personal data or information. *Explanation (iii)* to section 43A defines the term "sensitive personal data or information" to mean such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

The Information Technology Act, 2000 has not defined the term "sensitive personal data or information". Further, this section does not distinguish the "personal information" and sensitive personal data or information". It is pertinent to point out that the term "personal information" and sensitive personal data or information" has been defined and distinguished under the Information Technology Rules, 2011 including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The Government of India notified the Information Technology Rules, 2011 including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The said Rules came into effect from 11th April, 2011. Rule 2(i) has defined "personal information" in the following terms:

"(i) "Personal information" 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."

Further, rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 has given comprehensive clarity on what constitutes sensitive personal data information in India. Rule 3 of the said rules states as follows:

*"**3. Sensitive personal data or information.**—Sensitive personal data or information of a person means such personal information which consists of information relating to;*

(i) password;
(ii) financial information such as bank account or credit card or debit card or other payment instrument details;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules."

The way rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 has been defined is so vast to include not just the parameters defined therein but also include under its ambit all information relating to the parameters defined therein. For example, a password would not only constitute sensitive personal data or information of a person but even information such as password would also qualify as sensitive personal data or information. Thus in a layman's language, his username, his secret question, the answer to the secret question are all information that are relating to the password and hence they would also qualify as sensitive personal data or information. Further, all financial information such as bank account, credit card, debit card or other payment instruction details would qualify as sensitive personal data.

All information relating to physical, physiological and mental health condition of any person would qualify as sensitive personal data. All information relating to sexual orientation as to whether the person concerned is a gay or lesbian, would also qualify as sensitive personal data or information. All medical records and history and information relating thereto, would also qualify as sensitive personal data or information. All biometric information of a person, including his retina, iris scan, thumb impression and information connected therewith including information collected in connection with biometric information would also qualify as sensitive personal data.

Further, all information relating to any detail pertaining to the abovesaid parameters which are provided by the person concerned to a body corporate for providing service would also qualify as personal information. All information that a body corporate receives under the aforesaid parameters for the purposes of processing, storing or handling, under lawful contract or otherwise, would also qualify as sensitive personal data or information. The proviso to rule 3 only provides that any information which is freely available or which is accessible in the public domain shall not be regarded as sensitive personal data or information for the purposes of the said Rules. Also, any information furnished under the Right to Information Act, 2005 or any other law for the time being in force, shall also be not regarded as sensitive personal data or information for the purposes of these Rules.

Thus, the Government of India has provided broad parameters of what would constitute sensitive personal data or information in India. If the aforesaid sensitive personal data or information is being possessed, dealt with or handled by a body corporate, section 43A will come into applicability. The body corporate must be handling, possessing or dealing with such sensitive personal data or information in a computer resource which it either has ownership of or over which it has

complete control or which it actually operates. The Legislature has defined the term "computer resource" under section 2(1)(k), in the widest possible terms, to mean computer, computer system, computer network, data, computer database or software. The sensitive personal data could not only be held in a computer, computer system or computer network, but could also be held as part of a computer database or software or the normal data retained by the body corporate on a computer system. Thus, the ownership, control and operation of the relevant body corporate over its computer resources is essential for the purposes of applicability of section 43A of the amended Information Technology Act, 2000.

In case a body corporate is possessing, dealing or handling with any sensitive personal data or information in a computer resource, which it either does not own or control nor does it operate, then in such a case section 43A of the Information Technology Act, 2000 shall not have any applicability.

One of the main objectives of section 43A of the Information Technology Act, 2000 is to make body corporates more responsible for protecting and preserving the inherent character, authenticity and veracity of sensitive personal data or information that it possesses, deals or handles on its computer resources.

The second portion of section 43A highlights two important parameters. The first important parameter is that the body corporate must implement and maintain reasonable security practices and procedures. The second parameter is that the body corporate is negligent in implementing and maintaining reasonable security practices and procedures.

For the purposes of appreciating this portion of section 43A, let us peruse through *Explanation (ii)* to section 43A. *Explanation (ii)* to section 43A defines reasonable security practices and procedures to mean the following:

(a) security practices and procedures designed to protect sensitive personal data or information from unauthorised access;

(b) security practices and procedures designed to protect sensitive personal data or information from damage.

(c) security practices and procedures designed to protect sensitive personal data or information from unauthorized use;

(d) security practices and procedures designed to protect sensitive personal data or information from unauthorised modification;

(e) security practices and procedures designed to protect sensitive personal data and information from disclosure;

(f) security practices and procedures designed to protect sensitive personal data or information from unauthorised impairment;

All the aforesaid could either be:

(a) specified in an agreement between the parties; or

(b) may be specified in any law for the time being in force; and

(c) In the absence of any such agreement or law, the said reasonable security practices and procedures would mean such reasonable security practices and procedures as may be prescribed by the Central Government in consultation with such professional bodies or associations as it deems fit.

Rule 4 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 mandates body corporates to have in place a privacy policy for handling or dealing with personal information including sensitive personal data or information. It the mandatory responsibility of the body corporate to ensure that the said privacy policies have been made available for view by such providers of information who have provided such information under lawful contract. The privacy policy of body corporate must provide for the following mandatory parameters:

(i) clear and easily accessible statements of its practices and policies;

(ii) type of personal or sensitive personal data or information collected under rule 3;

(iii) purpose of collection and usage of such information;

(iv) disclosure of information including sensitive personal data or information as provided in rule 6;

(v) reasonable security practices and procedures as provided under rule 8.

Further the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 have stipulated a distinct legal regime for protection of sensitive personal data or information.

Sensitive personal data or information can only be collected from the provider of such information by a body corporate after obtaining consent in writing from such provider regarding the purpose of usage before collection of such information. It has been further mandated that any body corporate shall not collect sensitive personal data or information unless the following two conditions are fulfilled:

(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(b) the collection of the sensitive personal data or information is considered necessary for that purpose.

Further, any body corporate while collecting information, has to mandatorily take reasonable steps to ensure that the person concerned is having knowledge of:

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected;

(c) the intended recipients of the information; and

(d) the name and address of—

(i) the agency that is collecting the information; and

(ii) the agency that will retain the information.

The information that is collected, has to be 'mandatorily' used only for the purpose for which has been collected and body corporates are mandated not to retain the information for longer than is required for the purposes, for which the information may lawfully be used or is otherwise required under any law for the time being in force. Body corporates are further mandated to provide an option to

the provider of information, not to provide the data or information sought to be collected. Further, the provider of information has also been given the right to withdraw his consent at any point of time in respect of information that is collected. Body corporates are mandated to ensure that they shall keep the sensitive personal information and data secure.

Further, rule 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 specifically mandates that disclosure of sensitive personal data or information by a body corporate to any third party shall have to mandatorily require the prior permission from the provider of such information. However, there are some exceptions to this general Rule. In case, such disclosure has been agreed to in the contract between the body corporate and provider of information or in case the disclosure is necessary for compliance of the legal obligation, such disclosures can be made, without the prior permission from the provider of such information.

Rule 6(2) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 specifically provides that any sensitive personal data or information shall be disclosed to any third party by an order under the law for the time being in force. The law envisages the fact that there could be potential transfer of information including sensitive personal data or information from one body corporate within India to another body corporate located in any other country. However, in such a case, it is mandated that the body corporate must ensure that the transfer of information only takes to such legal entity that ensures the same level of data protection that is adhered to by the body corporate, as provided by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Further, the law is very clear that the transfer of such sensitive personal data or information shall only be allowed if it is necessary for the performance of a lawful contract between the body corporate or any other person on his behalf and the provider of information has consented to the data transfer. Thus, the law has sought to protect sensitive personal data by way of providing provisions pertaining to transfer of such personal data or information.

It is pertinent to point out that the Government of India has notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Rule 8 of the said Rules has defined reasonable security practices and procedures in the following manner:

"8. Reasonable Security Practices and Procedures.—(1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they

have implemented security control measures as per their documented information security programme and information security policies.

(2) The International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one such standard referred to in sub-Rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-Rule (1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-Rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant upgradation of its process and computer resource."

Rule 8 stipulates the body corporates to implement security practices and standards and also comprehensive documented information security programs and information security policies. The said policies must contain managerial, technical, operational and physical security control measures. These measures need to be commensurate with information assets that have been sought to be protected with the nature of the business.

Rule 8 further stipulates in no unclear terms that in the event of an information security breach, the *onus* of proof shall be upon the body corporate to prove as and when asked to demonstrate that they had implemented security control measures as per their documented information security program and information security policies. The ISO 27001 standard has been recognized as one such standard which is referred to under rule 8(1) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Thus, the perusal of the aforesaid shows that reasonable security practices and procedures can either be specified between the parties in an agreement which is executed by the parties or could also be specified by any law prevailing for the time being in force. In the event that the parties do not specify any reasonable security practices and procedures in their agreement or in the event the law does not specify the same, the reasonable security practices and procedures defined under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 become the *de facto* reasonable security practices and procedures which have to be complied with by all body corporates, who are possessing, dealing or handling sensitive data or information.

Thus, any body corporate, which is possessing, dealing or handling with any sensitive personal data or information, has a choice to make. It can either enter into a contract with another legal entity defining what all reasonable security practices and procedures it is going to apply. Alternatively, in case if it does not do so, it

will be mandated to comply with reasonable security practices and procedures as detailed under Rule 8 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. This becomes all the more relevant since there is no other specific law in this regard which has specified any such reasonable security practices and procedures pertaining to electronic data.

The focus of the law is not only having in place reasonable security practices and procedures but also effectively implementing and maintaining the same. Thus, it is not a one-time exercise but will have to be a continuous exercise of ensuring the security of sensitive personal data or information that is held on the body corporate's computer resource.

For the applicability of section 43A, it is also imperative that the complaining party must show that the body corporate has been negligent in implementing and maintaining reasonable security practices and procedures. The word "negligence" is not defined under section 43A of the Information Technology Act, 2000. However the said word has been adequately defined in the legal jurisprudence.

In "*Jacob Mathew* v. *State of Punjab*, on 5 August, AIR 2005 SC 3180: 2005 Cr LJ 3710: 2005 AIR SCW 3685, 2005 Appeal (Crl) 144-145 of 2004, the Supreme Court held as below:

"Negligence is the breach of a duty caused by omission to do something which a reasonable man guided by those considerations which ordinarily regulate the conduct of human affairs would do, or doing something which a prudent and reasonable man would not do. The definition of negligence as given in Law of Torts, Ratanlal & Dhirajlal (edited by Justice G.P. Singh), referred to hereinabove, holds good. Negligence becomes actionable on account of injury resulting from the act or omission amounting to negligence attributable to the person sued. The essential components of negligence are three: 'duty', 'breach' and 'resulting damage'.

In "*The Municipal Corporation of.....* v. *Laxman Iyer,* " on 27 October, 2003 Appeal (Civil) 8424 of 2003, the Supreme Court held as below:

"Though there is no statutory definition, in common parlance 'negligence' is categorized as either composite or contributory. It is first necessary to find out what is a negligent act. Negligence is omission of duty caused either by an omission to do something which a reasonable man guided upon those considerations who ordinarily by reason of conduct of human affairs would do or obligated to, or by doing something which a prudent or reasonable man would not do. Negligence does not always mean absolute carelessness, but want of such a degree of care as is required in particular circumstances. Negligence is failure to observe, for the protection of the interests of another person, the degree of care, precaution and vigilance which the circumstances justly demand, whereby such other person suffers injury. The idea of negligence and duty are strictly correlative. Negligence means either subjectively a careless state of mind, or objectively careless conduct. Negligence is not an absolute term, but is a relative one; it is rather a comparative term. No absolute standard can be fixed and no mathematically exact formula can be laid down by which negligence or lack of it can be infallibly measured in a given case. What constitutes negligence varies under different conditions and in determining whether negligence exists in a

particular case, or whether a mere act or course of conduct amounts to negligence, all the attending and surrounding facts and circumstances have to be taken into account. It is absence of care according to circumstances. To determine whether an act would be or would not be negligent, it is relevant to determine if any reasonable man would foresee that the act would cause damage or not. The omission to do what the law obligates or even the failure to do anything in a manner, mode or method envisaged by law would equally and per se constitute negligence on the part of such person."

All the parameters, which constitute negligence, will also have to be demonstrated in an action under section 43A of the Information Technology Act, 2000. The said negligence will have to be demonstrated by some cogent evidence, rather than by suggestive averments.

The third portion of section 43A of the Information Technology Act, 2000 deals with the negligence of the body corporate in implementing and maintaining reasonable security practices and procedures causing wrongful loss or wrongful gain to another person. It is pertinent to note that the term "wrongful loss" or "wrongful gain" is not defined by the Information Technology Act, 2000. However, section 23 of the Indian Penal Code, 1860 defines the terms "Wrongful gain" and "Wrongful loss", as follows:

"Wrongful gain" – *"wrongful gain" is gain by unlawful means of property to which the person losing it is legally entitled."*

"Wrongful loss" – *"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled."*

Thus, an overall analysis of section 43A of the Information Technology Act, 2000 clearly shows that this is a comprehensive code in itself. It not only mandates the implementation and maintenance of reasonable security practices and procedures for the purposes of securing sensitive personal data or information, it also mandates civil exposure to body corporates in the form of paying damages by way of compensation for the negligence in implementing and maintaining reasonable security practices and procedures which cause wrongful loss or wrongful gain to another person.

Clearly, no monetary limits have been set up for the damages by way of compensation under section 43A of the Information Technology Act, 2000. It clearly depends upon facts and circumstances of each case. However, technically speaking, unlimited liability to pay damages by way of compensation has been provided under section 43A of the Information Technology Act, 2000 in case its parameters are seen to be duly complied with. It is pertinent to note that any claim under section 43A shall not go to court of law but shall go to the Adjudicating Officer appointed under section 46 of the Information Technology Act, 2000. This is by virtue of section 46(1) of the Information Technology Act, 2000. However, the Adjudicating Officer shall only exercise jurisdiction under section 43A, in case if the claim for damages by way of compensation is upto 5 crore INR. In case the claim for damages by way of compensation under section 43A is beyond 5 crore INR, then the said claim shall have to be filed in a court of competent jurisdiction. Needless to say, by virtue of operation of section 46 of the Information Technology Act, 2000, the proceedings under section 43A are of a summary nature. The

Adjudicating Officer and the competent court have been mandated to give the concerned body corporate reasonable opportunity for making representation in the matter. If on such enquiry, they are satisfied that the body corporate has committed the contravention, the Adjudicating Officer/court of competent jurisdiction has been given the discretion to impose such penalty or award such compensation as they may deem fit in accordance with the provisions of section 43A of the Information Technology Act, 2000.

While the claimant can seek unlimited damages by way of compensation, the *onus* of proving the fact that such wrongful gain or loss occurred, causing damage to the claimant is upon the claimant. The Adjudicating Officer or the court shall also, while granting damages under section 43A of the Information Technology Act, 2000 consider the important factors in this regard including the amount of gain or unfair advantage, whenever quantifiable made as a result of the default, the amount of loss caused to any person as a result of the default and the repetitive nature of default.

At the time of writing, no case has been reported in the public domain which has been decided by any Adjudicating Officer/court of competent jurisdiction under section 43A of the Information Technology Act, 2000.

Seen from a holistic perspective, section 43A provides distinctive code for not just ensuring the protection and preservation of sensitive personal data or information belonging to people but also upon ensuring that body corporates implement and maintain reasonable security practices and procedures to protect the sensitive personal data or information. The negligence in implementing and maintaining the said reasonable security practices and procedures could really cause huge losses for companies. Section 43A does make implementation and maintenance of reasonable security practices as mandatory provision that body corporate handling, dealing or processing with sensitive personal data or information have no choice but to adhere to and comply with implementing and maintaining reasonable security practices and procedures.

While section 43A provides for the civil exposure to pay damages by way of compensation, it also needs to be noted that in case the reasonable security practices and procedures are specified in a contract being lawful agreement and in case if the breach of such lawful agreement or contact, then section 72A of the Information Technology Act, 2000 would also have applicability. Section 72A provides for an offence punishable with imprisonment for a term which may extend to 3 years or with fine which may extend to 5,00,000 INR or with both. section 72A of the Information Technology Act, 2000 states as follows:

"Section 72A – Punishment for Disclosure of information in breach of lawful contract

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished

with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both."

Section 72A makes it an offence when any person including an intermediary, who while providing services under lawful contract, secured access to any material containing personal information about another person. The said access can be secured either with an intention to cause or knowing that it is likely to cause wrongful loss or gain and thereafter, if the said person discloses either without the consent of the person concerned or in breach of lawful contract, such material to any other person, the said act has been declared as an offence under section 72A of the Information Technology Act, 2000. Thus, while section 43A specifically deals with sensitive personal data and information, section 72A is slightly more broader as it also deals with unauthorised disclosure of personal information without the consent of person concerned or in breach of lawful contract.

While some people argue that section 43A along with section 72A provides the data protection regime in India, the fact is that there is no real data protection legal regime in India, in the sense of existing data protection legal regimes in the European Union. For a huge country like India, trying to address the complicated issues pertaining to data protection by means of provisions like section 43A and section 72A alone would not suffice. Further, there are concerns pertaining to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

It is pertinent to note that the Central Government was only authorized by virtue of section 87(2)(ob) to come up with rules and regulations that may provide for reasonable security practices and procedures and sensitive personal data or information under section 43A of the Information Technology Act, 2000. However, a perusal of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 clearly shows that the Central Government has gone far beyond the ambit and scope of powers granted to it. Rather than only specifying the reasonable security practices and procedures and sensitive personal data or information, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 have sought to create a ghost or shadow digital data protection regime by inserting rules 4, 5, 6 and 7 in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

It is pertinent to point out that at a time when the mother legislation, being the Information Technology Act, 2000, has not provided for a distinct data protection legal regime, the said Rules go far beyond the scope of powers granted to the Government in this regard, it clearly could be challenged in a court of law for exceeding the brief given to the Central Government under section 87(2)(ob) of the Information Technology Act, 2000. Further another problem in section 43A of the Information Technology Act, 2000 is that while it only provides for implementation and maintenance of reasonable security practices and procedures, it does not provide for an independent accreditation and evaluation process by means of which such implementation and maintenance of reasonable security practices and procedures by body corporates handling, dealing or possessing sensitive personal

data or information, could be appropriately verified or tested. Further, the said provision does not mandate external independent accreditation agencies for conducting the periodical audits to help ensure compliance.

India does not have a data protection legislation nor a specific privacy legislation. Section 43A seeks to address some of the vacuum existing in this regard. Various aspects pertaining to protection and preservation of sensitive personal data and information have been detailed under the Information Technology Act, 2000.

One of the main criticisms of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 is that these rules are not clear because of huge ambiguities in the manner in which the language therein has been drafted. Further, the words used therein are used in the widest possible sense and the same is likely to affect all kinds of possessing, handling or dealing with information including sensitive personal data or information. Another criticism of section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 is that they do not provide the protection of the data stored in non-electronic medium. Section 43A of the Information Technology Act, 2000 also does not specify distinction between the different levels of security practices or procedures to be made applicable in the context of personal information as also sensitive personal information and data.

The fact that the Information Technology Act, 2000 is silent on defining personal information further complicates the entire scenario. Section 43A of the Information Technology Act, 2000 does not make a distinction between a data controller and data processor in a manner that the distinction existing enough in the UK and Europe. Further, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 do not specify any time frame for retention of sensitive personal data and information. They only stipulate that the body corporate must not retain sensitive personal data or information for longer than is required for the purposes for which the said sensitive personal data may lawfully be used. Given the fact that different laws provide for different retention periods, the said rules further create an Act of confusion.

One of the main problems of section 43A of the amended Information Technology Act, 2000 is that it only deals with sensitive personal data and information and does not deal with protection of personal information which includes 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 the body corporate, is capable of identifying such a person. Thus, personally identifiable information and personal information do not stand on the same pedestal of protection as compared to sensitive personal data and information, thanks to the selective treatment accorded to sensitive personal data and information under section 43A of the Information Technology Act, 2000.

Another major problem in section 43A is that the effect of section 43A has been sought to be watered down thanks to a clarification dated 24th August, 2011. The

said clarification, is published through a press note under the title of "Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under section 43A of the Information Technology ACT, 2000", and states as under:

"The Department of Information Technology had notified Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under section 43A of the Information Technology Act, 2000 on 11.4.2011 vide notification No. G.S.R. 313(E).

These rules are regarding sensitive personal data or information and are applicable to the body corporate or any person located within India. Any such body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India is not subject to the requirement of rules 5 & 6. Body corporate, providing services to the provider of information under a contractual obligation directly with them, as the case may be, however, is subject to rules 5 & 6. Providers of information, as referred to in these Rules, are those natural persons who provide sensitive personal data or information to a body corporate. It is also clarified that privacy policy, as prescribed in rule 4, relates to the body corporate and is not with respect to any particular obligation under any contract. Further, in rule 5(1) consent includes consent given by any mode of electronic communication".

The net effect of the said clarification is that all outsourcing companies, who are outsourcing work to India, are brought outside the scope of section 43A. The net effect also is that all companies who are providing outsourcing services to clients outside India shall also fall outside the scope of section 43A of the amended Information Technology Act, 2000.

The said clarification apparently has been given by the Government so as to give a boost to the outsourcing sector. The net effect of the said clarification is that any such body corporate providing any services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligations whether any legal entity located within or outside India is not subject to the requirements of rules 5 and 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Further, body corporate providing services to the provider of information under contractual obligation directly with them, however, is subject to rules 5 and 6. I am of the opinion that the said clarification is *per se* not legally tenable. This is so as section 43A has been enacted by the Parliament of India and only the Parliament is authorized to exempt certain categories of operators from the applicability of section 43A of the Information Technology Act, 2000. It is important to note that the clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under section 43A of the Information Technology Act, 2000 has been done by means of a Press Note. It has neither been done by means of rules to be made by the Government as authorized under section 87(2)(ob) of the Information Technology Act, 2000, nor does this Press Note have the sanction of Parliament

behind the same. At the time of writing, the legal validity of the said Press Note has not been challenged. However, since the Press Note has been issued in contravention of the stated objectives of section 43A of the Information Technology Act, 2000, it is only a question of time that when a challenge to such clarification could come across, the court would be besieged about the legality of such a Press Note. I am very clear that no Press Note can outreach the scope of the provisions stipulated by the Parliament being section 43A of the Information Technology Act, 2000.

Seen from an overall perspective section 43A of the Information Technology Act, 2000 is a quantum leap forward in terms of stipulating the Indian law relating to sensitive personal data or information. It is still not India's answer for having a separate or distinct data protection legislation. However, it does seek to have in place adequate legal mechanisms for the purposes of getting and preserving the sanctity, veracity and authenticity of sensitive personal data or information in the electronic form in India. There are huge ambiguities in the way section 43A has been defined and when read in conjunction with the Information Technology Act, 2000, there is lot of jurisprudence that has yet to evolve on this subject. As time passes by, the evolution of such jurisprudence will determine the direction in which section 43A of the Information Technology Act, 2000 gravitates for the protection and preservation of sensitive personal data or information in India.

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

(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."

Various penalties have been provided under section 44 if there is non-compliance of certain specified conditions. Section 44(1) states that if any person fails to furnish any document, return or report to the Controller of Certifying Authorities which that person is required under the Information Technology Act, Rules or Regulations made thereunder, to furnish, that person shall be liable for a penalty not exceeding Rs. 1,50,000 for each such failure.

Further, if the Certifying Authority fails to furnish any documents, report or return to the Controller which the Certifying Authority is required under the Information Technology Act, Rules or Regulations made thereunder, to furnish, the Certifying Authority shall be liable to pay penalty not exceeding Rs. 1, 50,000 for

each such failure. Penalties are liable to be recovered as an arrear of land revenue under section 64 of the Information Technology Act, 2000 and in case of failure of any party or the Certifying Authority to pay any penalty, the Digital Signature Certificate or the licence, as the case may be, can be suspended till the time the penalty is paid.

If a person who is mandated by the Information Technology Act, Rules or Regulations made thereunder, to file any return or furnish any information, books or other documents within a specified time, and if the said person fails to file or furnish the same within the time specified, he shall be liable to pay penalty not exceeding Rs. 5,000 for each day, during which such failure continues.

Similarly, if any person is mandated by the Information Technology Act, 2000, Rules or Regulations made thereunder, to maintain books of account or records and if that person fails to maintain the same, that act attracts penalty. The penalty in such a case amounts to Rs. 10,000 for each day, during which the failure continues.

The rationale behind enacting section 44 is basically to ensure that people comply with the provisions of the Information Technology Act, Rules or Regulations made thereunder. Any failure to comply with the provisions would meet with steep economic penalty and in many cases, penalty would be continuing on a day to day basis till the time such failure continues or subsists. The Adjudicating Officer under section 46 of the Information Technology Act, 2000, shall levy these penalties.

Section 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."

Three kinds of penalties have been defined under section 44. The Act further envisages that there may be other residuary cases of contravention of the provisions of the Indian Cyberlaw where the Information Technology Act, 2000 has not specified any penalty. In such a case, section 45 comes into play. Section 45 specifically provides that where no penalty has been separately provided for the contravention of any Rules or Regulations made under the Information Technology Act, 2000, if any person contravenes such Rules and Regulations, then he shall be liable to pay compensation not exceeding Rs. 25,000 or a residuary penalty of a sum not exceeding Rs. 25,000. This penalty, by way of compensation, has been imposed to provide monetary relief that would go to the person affected by such contravention.

Section 45 is distinguished from section 44 inasmuch as section 44 imposes penalty, the amount of which would go only to the exchequer. Section 45 provides for penalty, both in the form of a levy accruing to the exchequer as also by way of compensation. In case of compensation, the amount of penalty in question would not go to the Government but to the person affected by such contravention, which may or may not necessarily be the Government.

Section 46 – Power to Adjudicate

Section 46 has been amended by the Information Technology (Amendment) Act, 2008. In section 46(1), in place of the earlier words, "direction or order made thereunder", the words "direction or order made thereunder which renders him liable to pay the penalty or compensation" have been inserted. Further by virtue of the Information Technology (Amendment) Act, 2008 section 46 (1A) has been added. Further section 46(5c) has been added by the Information Technology (Amendment) Act, 2008. Section 46 of the amended Information Technology Act, 2000 reads as follows:

"(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, 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.*

(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 claim for injury or damage exceeding rupees five crore shall vest with the competent court.

(2) *The Adjudicating Officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for 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 as he thinks fit in accordance with the provisions of that section.*

(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.*

(4) *Where more than one Adjudicating Officer 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 sections 193 and 228 of the Indian Penal Code (45 of 1860);

(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1973).

(c) shall be deemed to be a Civil Court for purposes of Order XXI of the Civil Procedure Code, 1908 (5 of 1908)."

Section 46 talks of a statutory authority called the Adjudicating Officer. In the IT Act, 2000, the Adjudicating Officer is the third statutory authority that finds mention after the Controller of Certifying Authorities and the Certifying Authorities. Adjudicating Officers shall be appointed for the purpose of adjudication under Chapter IX of the IT Act, 2000.

The Adjudicating Officers shall be appointed by the Central Government for the purpose of adjudging under Chapter IX whether any person has committed a contravention of any of the provisions of the Information Technology Act, 2000 or of any Rule, Regulations, direction or order made thereunder which renders him liable to pay the penalty or compensation. Thus, an Adjudicating Officer will adjudicate a contravention and violation of the provisions of the Information Technology Act, 2000, IT Rules, 2000, Information Technology (Certifying Authority) Regulations, 2001, other directions or orders. The Adjudicating Officer shall be an Officer, not below the rank of a Director to the Government of India or an equivalent Officer of the State Government. It may be pertinent to note that the Adjudicating Officer is the first level of redress under the Information Technology Act.

The main role of the Adjudicating Officer is to hold an inquiry in the manner, which may be prescribed by the Central Government. What is of importance is to note that the Adjudicating Officer has been given the power to adjudicate whether any person has committed a contravention of any of the provisions of the Information Technology Act, 2000, IT Rules, 2000, Information Technology (Certifying Authority) Regulations, 2001 or other directions or orders made thereunder which renders him liable to pay the penalty or compensation. Therefore, the ambit and jurisdiction of the Adjudicating Officer is to adjudicate the contravention of provisions of the Information Technology Act, Rules, Regulations, directions or orders made thereunder which renders him liable to pay the penalty or compensation. For the purpose of adjudging, the Adjudicating Officer has to hold an enquiry in the manner, as stipulated by the Central Government.

It is important to note that the Central Government has been mandated to appoint an Adjudicating Officer for adjudging the commission of any contravention of the provisions of the Indian Cyberlaw. The Central Government has no discretion in the matter of appointment of the Adjudicating Officer. The Central Government has not been granted the role of a filtering authority to filter the complaints for adjudication under Chapter IX and as such, it cannot, at any point of time, refuse to appoint an Adjudicating Officer, as the word used by section 46(1) is 'shall'.

As per new added section 46(1A), the Adjudicating Officer shall mandatorily exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed 5,00,00,000 INR. Thus, all claims for damages by way of compensation upto 5,00,00,000 INR can be filed with the Adjudicating Officer. The proviso to section 46(1A) clearly shows that, in case, if the claim for injury or damages exceed 5,00,00,000 INR, then the jurisdiction to entertain such agreement shall vest with the court of competent jurisdiction. Thus, the net result is that, if

any person who is aggrieved by the various acts detailed under section 43 of the Information Technology Act, 2000, wants to file damages upto 5,00,00,000 INR, he can do so by filing it before the Adjudicating Officer. For claims beyond amount of 5,00,00,000 INR, the said claims will have to be filed in court of competent jurisdiction.

Section 46(2) mandates that the Adjudicating Officer must follow the principles of natural justice and give opportunity of being heard to the concerned person whose contravention is being adjudged. The concerned person has to be given a reasonable opportunity for making representation in the matter. The Adjudicating Officer is also mandated to carry out the said inquiry and if, after the conclusion of such inquiry, the Adjudicating Officer is satisfied that the concerned person has committed the contravention, then the Adjudicating Officer has been given the discretion to impose penalty or award compensation. He may impose such penalty or award such compensation as he thinks fit in accordance with the provision of the section 46. This discretion has to be exercised according to well-established principles of law.

A perusal of section 46 shows that a lot of discretion has been given to the Adjudicating Officer. However, no standards or parameters have been laid down to guide the exercise of discretion of the Adjudicating Officer. It is expected that the discretion shall be exercised in accordance with the well-established principles of law. Further, the Act has not specified the manner in which the adjudication has to be conducted by the Adjudicating Officer. The Act has also not detailed the exhaustive scope of territorial jurisdiction of the Adjudicating Officer.

The qualifications of Adjudicating Officer are dealt with in section 46(3). It is stated that the Central Government would not appoint any person as an Adjudicating Officer unless he has such experience in the field of Information Technology and legal or judicial experience as may be prescribed.

The Information Technology Act stipulates that there would be many Adjudicating Officers. If more than one Adjudicating Officer is appointed, it has been mandated that the Central Government shall specify the subject-matters over which the Adjudicating Officers will have jurisdiction as also their territorial jurisdiction.

Under section 46(5) the Adjudicating Officers have been given the power of a Civil Court as conferred upon the Cyber Appellate Tribunal under section 58(2). It is important to note that section 61 of the Information Technology Act, 2000 bars the jurisdiction of civil courts. An Adjudicating Officer shall have the same powers as are vested in Civil Court under the Code of Civil Procedure, 1908, while trying a suit in respect of the following matters:—

(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.

Further, an Adjudicating Officer shall be deemed to be a Civil Court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973. The effect of this would be that when any such offence as is described in sections 175, 178, 179, 180 or 228 of the Indian Penal Code is committed in the view or presence of the Adjudicating Officer, the Adjudicating Officers shall be deemed to be a Civil Court. The Adjudicating Officer may cause the offender to be detained in custody and may, at any time before the rising of the Adjudicating Officer on the same day, take cognizance of the offence and, after giving the offender a reasonable opportunity to show cause why he should not be punished under section 345, sentence the offender to a 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.

In every such case, the Adjudicating Officer shall be deemed to be a Civil Court, which implies that it shall record the facts constituting the offence with the statement, if any, made by the offender, as well as impose a fine or sentence.

If any offence is under section 228 of the Indian Penal Code, the record shall show the nature and stage of the judicial proceeding in which, the Adjudicating Officer interrupted or insulted, was sitting, and the nature of the interruption or insult.

Further, the Adjudicating Officer is deemed to be a Civil Court for the purposes of section 346 Cr. P.C. As such, the practical working of the same would possibly evolve in the manner detailed herein below. If the Adjudicating Officer in any case considers that a person accused of any of the offences referred to in section 345 Cr. P.C. and committed in its view or presence should be imprisoned otherwise in default of payment of fine, or that a fine exceeding two hundred rupees should be imposed upon him, or if such Adjudicating Officer is for any other reason of the opinion that the case should not be disposed of under section 345, such Adjudicating Officer, 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 he may further require security to be given for the appearance of such person before such Magistrate, or if such sufficient security is not given, shall forward such person in custody to such Magistrate. Also, the Magistrate to whom any case is forwarded under the section, shall proceed to deal with, as far as may be, as if it were instituted on a police report.

Further, all proceedings before the Adjudicating Officer shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of Indian Penal Code. Thus, if any person, intentionally gives false evidence in any stage of the proceedings before the Adjudicating Officer, or fabricates false evidence for the purpose of being used in any stage of the proceedings before the Adjudicating Officer, he shall be punished, for the offence of false evidence, which shall be imprisonment of either description for a term which may extend to seven years and shall also be liable to fine. Further, whoever, intentionally offers any insult or

causes any interruption to the Adjudicating Officer, while such Adjudicating Officer being a public servant is sitting, in any stage of the judicial proceedings, he shall be punished with simple imprisonment for a term which may extend up to six months or with fine which may extend to one thousand rupees or with both.

The Adjudicating Officer has been given very comprehensive powers *i.e.* of a Civil Court, the proceedings before him shall be deemed to be judicial proceedings and he has been given the single most important job of adjudging the violations of the provisions of the Information Technology Act, 2000, Rules, Regulations, directions or orders made thereunder.

However, in the absence of specific parameters being stipulated by the Information Technology Act, 2000, there are numerous challenges that are likely to arise in the said scenario. It may be pertinent to note that the Controller of Certifying Authorities under section 28(1) or any officer authorized by him, shall take up for investigation any contravention of the provisions of this Act, Rules and Regulations made thereunder. It may be submitted that the same powers have been conferred on an Adjudicating Officer under section 46 and there is likelihood of conflict that may arise between the two statutory authorities. The power of the Adjudicating Officer to adjudicate whether any person has committed a contravention of any of the provisions of the Information Technology Act, 2000 or any Rule, Regulation, direction or order made thereunder is very wide and includes not just power to investigate as is given to the Controller under section 28(1), but also the power to hold an inquiry under section 46(1). Such conflicting provisions are likely to create problems for the smooth functioning of the Information Technology Act, 2000.

The Information Technology Act, 2000 has been made applicable under section 1(2) not only to the whole of India, as also to any offence or contravention thereunder committed outside India by any person. It is not clear how the Adjudicating Officer shall adjudicate if any contravention of the provisions of the Information Technology Act, any Rule, Regulation, direction or order made thereunder has been committed outside India. Further, cyber crimes and other illegal activities take place in cyberspace. In cyberspace, it is very difficult to come to a conclusion as to from what particular place does a particular act or violation or contravention takes place. In such a scenario, it is not clear how the Adjudicating Officer would decide as to where a particular contravention took place, and how he will adjudicate upon it. Such provisions are also likely to lead to conflict of jurisdiction with other authorities in other nations, who are duly authorized to deal with such scenarios.

Section 46 is in the nature of an absolute statement without any clarification. The words "contravention of any of the provisions of this Act" makes it clear that any contravention of any section would attract the jurisdiction of the Adjudicating Officer.

However, the wordings of section 46 have to be harmoniously constructed and interpreted, keeping in mind the scheme and other provisions of the Information Technology Act, 2000.

A close scrutiny of the section reveals that the Adjudicating Officer has been empowered only to determine contraventions under sections 43, 44 and 45 of the Act. Chapter XI of the Act deals with "offences" and provides for punishment of fine and/or imprisonment for committing offences like tampering with computer source documents, hacking and other offences prescribed therein. The trial of these offences would not fall within the jurisdiction of Adjudicating Officer as the Adjudicating Officer has been conferred with the powers of a Civil Court under section 46(5) of the Information Technology Act, 2000. The trial of offences committed under Chapter XI of the Information Technology Act, 2000 would therefore still be within the jurisdiction of the relevant criminal courts, be it those of the Metropolitan Magistrate or the Additional Sessions Judge under the provisions of the Code of Criminal Procedure. (For more details, kindly see the commentary on Chapter XI)

Further, section 46(5c) has been added by the Information Technology (Amendment) Act, 2008. The net effect of this is that every Adjudicating Officer shall be deemed to be a Civil Court for the purposes of Order XXI CPC. Order XXI CPC deals with execution of decrees and orders. Thus, the net effect of section 46(5c) is that all the orders passed by the Adjudicating Officers shall be deemed to be decree which are liable to be executed and hence the Adjudicating Officer shall be deemed to be a civil court for the purposes of Order XXI CPC.

Section 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"

Section 47 is the only pointer that the Legislature has given to Adjudicating Officers. There are only three factors the Adjudicating Officers have to take into account while deciding the quantum of compensation. It is mandatory for the Adjudicating Officer to give due regard to the three factors enumerated in section 47.

The first factor to be considered by the Adjudicating Officer, while dealing with the quantum of compensation, is the amount of gain or unfair addition, whether quantifiable, made as a result of the default. The Adjudicating Officer has to judge as to how much gain or unfair addition was obtained by the respondent by indulging in any of the eight acts stipulated in section 43 of the Information Technology Act. If the amount of gain or unfair addition can be quantified in monetary terms, that gives a substantial economic indicator of the quantum of compensation to be granted.

The second factor to be considered while adjudging the total amount of compensation is the amount of loss caused to any person as a result of the default. If the loss, incurred by a particular person, due to any of the acts of the respondent stipulated in section 43, can be quantified in monetary terms, that also gives a

substantial basis for determining the quantum of damages, since the damages have to include that element as specified in section 47(b).

The third factor to be considered by the Adjudicating Officer, while adjudicating the quantum of compensation, is the repetitive nature of the default. If someone has been repeatedly doing any of the illegal acts detailed in section 43(a) to (h), it gives a ground to award enhanced compensation against the offender compared with any other case of solitary acts. If any person repeatedly does the illegal acts detailed in section 43(a) to (h), that not only indicates a continuing intention to do the illegal acts, but also displays an attitude of impunity and defiance of law of the alleged offender. In such a case, it is important that higher quantum of compensation be awarded so that the same acts as a deterrent to all potential future offenders. The main idea in granting compensation up to five crore rupees under section 43 is that such compensation acts as an economic deterrent for potential mischief mongers and offenders, from doing the acts detailed in section 43(a) to (h) of the Information Technology Act, 2000.

CHAPTER X

THE CYBER APPELLATE TRIBUNAL

Section 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."

Section 48 of the Information Technology Act, 2000 has been amended by the Information Technology (Amendment) Act, 2008 whereby the term "Regulations" has been omitted. Now the "The Cyber Regulation Appellate Tribunal" has become "The Cyber Appellate Tribunal".

Section 48 of the amended Information Technology Act, 2000 stipulates the establishment of a statutory authority called The Cyber Appellate Tribunal. This is the first appellate statutory body that has been envisaged under the Information Technology Act, 2000. The Cyber Appellate Tribunal shall hear appeals filed by persons aggrieved from any of the orders passed by the Controller of Certifying Authorities and an Adjudicating Officer. Section 48(1) states that there will be one or more Cyber Appellate Tribunals and they shall only be established by the Central Government by an appropriate notification in the Official Gazette.

Section 48(2) further stipulates that the Central Government shall also elaborate and detail the territorial jurisdiction of the Cyber Appellate Tribunal. Further, the subject matters over which the Cyber Appellate Tribunal shall have jurisdiction shall also be stipulated in the notification providing for the establishment of the Cyber Appellate Tribunal.

Since India is a large country, it is expected that the Government shall constitute various Cyber Appellate Tribunals, preferably one in each State. Further, the Act provides that all appeals against the orders passed by the Cyber Appellate Tribunal shall lie to the High Court. As such, it will be logical and prudent to have at least one Cyber Appellate Tribunal for each High Court so as to do justice to the objects of the legislation.

Section 57 of the Information Technology Act, 2000 states that any person aggrieved by an order made by the Controller or an Adjudicating Officer may prefer an appeal to the Cyber Appellate Tribunal, having jurisdiction over the matter.

Section 49 – Composition of Cyber Appellate Tribunal

"(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 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."

Section 49 of the Information Technology Act, 2000 has been inserted in the said legislation by virtue of the Information Technology (Amendment) Act, 2008. This provision provides for the composition of the Cyber Appellate Tribunal. Earlier, the Cyber Appellate Tribunal used to consist of single member Tribunal who was the Presiding Officer of the Cyber Appellate Tribunal. Now, after the amendments, the law has stipulated that the Cyber Appellate Tribunal shall be a multi-member Tribunal. It shall be headed by a Chairperson and it will have such number of other members as may be appointed by the Central Government after notification in the Official Gazette.

The proviso to section 49(1) provides that if any person was earlier appointed as the Presiding Officer of the Cyber Appellate Tribunal under the Information Technology Act, 2000 before the commencement of the Information Technology (Amendment) Act, 2008, he shall be deemed to have been appointed as the Chairperson of the Cyber Appellate Tribunal under the provisions of the amended Information Technology Act, 2000.

Given the fact that the Cyber Appellate Tribunal will deal with legal and judicial issues concerning electronic form and the digital space, section 49(2) mandates that the Chief Justice of India shall be consulted by the Central Government before making the selection of the Chairperson and members of the Cyber Appellate Tribunal.

Earlier, the Cyber Appellate Tribunal was established for being located in Delhi only. However, the amendments have now come up with the concept of Benches of the Cyber Appellate Tribunal. Section 49(3) provides that the jurisdiction, powers and authorities of the Cyber Appellate Tribunal may be exercised by the various Benches of Cyber Appellate Tribunal in different parts of the country. Discretion has been provided to Chairperson of the Cyber Appellate Tribunal to constitute any Bench. The Chairperson of the Cyber Appellate Tribunal may constitute the Bench with either one or two members of the Tribunal as per the discretion and choice of the Chairperson.

Section 49(3) further stipulates that the Benches of the Cyber Appellate Tribunal shall sit primarily at New Delhi. The said Benches may also sit at such other places as may be notified by the Central Government by notification in the Official Gazette. However, the Central Government can specify such other places where the Benches of Cyber Appellate Tribunal can sit in consultation with the Chairperson of the Cyber Appellate Tribunal.

The Central Government is further mandated that it shall by notification in the Official Gazette specify the areas of jurisdiction of each Bench of the Cyber Appellate Tribunal. This would be essential to determine the specific areas in relation to which each Bench of the Cyber Appellate Tribunal exercises its territorial jurisdiction. Such an exercise is further required to avoid potential overlap of jurisdiction amongst various Benches of the Cyber Appellate Tribunal.

While the constitution of the Benches, place of sitting and the jurisdiction may be specified by the Central Government, the Chairperson of the Cyber Appellate Tribunal has been given the discretion to transfer a member of the Cyber Appellate Tribunal from one Bench to the other. Such power has been given on the Chairperson notwithstanding anything else contained in section 49(3) of the Information Technology Act, 2000.

The law has been alive to the fact that there may come, before the Cyber Appellate Tribunal, very complex issues concerning technical nuances of various aspects and interpretation of different clauses. As such, discretion has been given to the Chairperson or member of the Cyber Appellate Tribunal that they could determine as to whether at any stage of the hearing of any case or any matter that the said matter is of such a nature that it needs to be heard by a Bench consisting of more members. In such a case, the discretion has been given to the Chairperson of the Cyber Appellate Tribunal to transfer the said case or matter to such a Bench as the Chairperson may deem fit. Thus, large amount of flexibility has been given to the Chairperson in order to take such administrative decisions so as to effectively ensure the efficient functioning of the Cyber Appellate Tribunal and its various Benches across the country.

Section 50 – Qualifications for Appointment as Chairperson and Members of Cyber Appellate Tribunal

"(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 years or Joint 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."

Section 50 prescribes the mandatory qualifications for any person to be appointed as a Chairperson and Members of Cyber Appellate Tribunal. Section 50 is couched in mandatory terms and conditions. Unless the mandatory terms and conditions of section 50 are satisfied, the appointment of the Chairperson and Members would be illegal and shall be subject to scrutiny in a court of law.

Section 50(1) stipulates that the minimum qualification for appointment as a Chairperson of the Cyber Appellate Tribunal is that the said person either has been or is qualified to be a Judge of the High Court. This will be done so as to ensure that senior level people who are qualified or qualified to become Judges of the High Court only, can be appointed to the post of the Chairperson of the Cyber Appellate Tribunal.

The law stipulates for two kinds of members in the Cyber Appellate Tribunal. There will be a Judicial Member and there will be other members of the Cyber Appellate Tribunal. The power to appoint the general members of the Cyber Appellate Tribunal has been conferred on the Central Government. The Central Government shall appoint such members of the Cyber Appellate Tribunal from amongst persons who could have special knowledge of and professional experience in any of the following areas:

(a) Information Technology
(b) Telecommunication
(c) Industry
(d) Management; or
(e) Consumer affairs.

The proviso to section 50(2) provides that there has to be seniority of service in respect of the person to be appointed as member of the Cyber Appellate Tribunal. The proviso mandates that only a person who is or has been in the service of the Central Government or State Government and has held any of the following posts for the stipulated period shall be appointed as member of the Cyber Appellate Tribunal:

(a) Has held the post of Additional Secretary to the Government of India, for period of not less than one year;

(b) Has held any equivalent post in the Central Government to the post of Additional Secretary, for the period of not less than one year;

(c) Held any equivalent post of Additional Secretary to the State Government, for the period of not less than one year.

(d) Has held the post of Joint Secretary to the Government of India, for a period of not less than seven years;

(e) Has held any equivalent post in the Central Government equivalent to the Joint Secretary to the Government of India, for a period of not less than seven years; or

(f) Has held any equivalent post in the State Government equivalent to the Joint Secretary to the Government of India, for a period of not less than seven years.

Thus, the law seems to take adequate protection to ensure that the persons who are appointed as members of the Cyber Appellate Tribunal have fairly high level of seniority and experience in the Central or State Governments.

As regards Judicial Members of the Cyber Appellate Tribunal, the parameters for appointment are different. Judicial Members of the Cyber Appellate Tribunal also shall be appointed by the Central Government. These Judicial Members can be appointed from any of the following persons:

(a) A person who is or has been a member of Indian Legal Service;

(b) Has held the post of Additional Secretary for a period of not less than one year;

(c) Has held a Grade 1 post of Indian Legal Service for a period of not less than five years.

Thus, section 50(3) made substantial precautions to ensure that senior level persons who qualify minimum standards stipulated under section 50(3) of the Information Technology Act, 2000, are inducted as Judicial Members of the Cyber Appellate Tribunal.

The rationale of the Legislature is very clear inasmuch as the Legislature wants a judicial person with a judicial mind and training to become a Chairperson and Members of the Cyber Appellate Tribunal. This is important because the Adjudicating Officer is not envisaged under the law and rules to be a judicial officer. As such, there is a need for having a judicial person at the helm at the appellate stage for listening to all appeals *i.e.* at the level of the Chairperson and Members of the Cyber Appellate Tribunal. Also, since the Appellate Tribunal is

envisaged to have a Chairperson and other special knowledged and also professional experienced Members including the judicial members, it is imperative that they must be well trained in the legalities and technicalities of law so as to render full justice to the appellants.

Section 51 – Term of office, conditions of service, etc., of Chairperson and Members

"(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."

Section 51 deals with the terms of office and conditions of service of the Chairperson and Members of the Cyber Appellate Tribunal.

Section 51(1) stipulates that the term of the Chairperson or member of the Cyber Appellate Tribunal shall be for a period of five years. The holding of the office for a term of five years shall be from the date on which the relevant person enters upon his office or until he attains the age of 65 years whichever is earlier. Thus, the cap in terms of retirement of Chairperson or members of Cyber Appellate Tribunal is 65 years. The Chairperson and members of Cyber Appellate Tribunal can either have a term for five years or can continue to work till attaining the age of 65 years, whichever is earlier.

The Central Government has been straddled with the mandatory responsibility of doing appropriate due diligence before appointing any person as the Chairperson or member of the Cyber Appellate Tribunal. The Central Government has been straddled with the duty to satisfy itself that the said person does not have any financial or other interest as is likely to prejudicially impact its functions as such Chairperson or member of the Cyber Appellate Tribunal.

Further, in order to ensure the independence of the Cyber Appellate Tribunal, section 50(1)(3) provides for the specific scheme of things. It is provided that in case an officer of the Central or State Government is selected to be the Chairperson or member of the Cyber Appellate Tribunal, he shall have to mandatorily retire from service of the Central Government or State Government before being the Chairperson of member of the Cyber Appellate Tribunal. Such provision has been made so to insulate the Cyber Appellate Tribunal and to ensure its judicial independence and functions.

Section 52 – *Salary, allowances and other terms and conditions of service of Presiding Officer*

"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."

Section 52 of the Information Technology Act, 2000 deals with salary, allowances and other terms and conditions of service of the Chairperson or a member of the Cyber Appellate Tribunal. Section 52 provides that the salary, allowances payable to, other terms and conditions of service including pension, gratuity and other benefits of the Chairperson and members of Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government. As such in this regard, the Central Government has been given the power under section 87(2)(r) of the Information Technology Act, 2000 to come up with rules pertaining to the salary, allowances and other terms and conditions of the Chairperson and members of the Cyber Appellate Tribunal under section 52 of the amended Information Technology Act, 2000.

It is pertinent to point out that the Central Government has already notified the Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Member) Rules, 2009 which elaborated upon the salary, allowances and other terms and conditions of service of Chairperson and Members of the Cyber Appellate Tribunal.

Section 52A – Powers of Superintendence, Direction, etc.

"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."

Section 52A deals with the specific powers of superintendence of the Chairperson of Cyber Appellate Tribunal. The Chairperson has been given the mandatory powers of general superintendence and directions in the conduct and affairs of the Cyber Appellate Tribunal. He has been given the power to preside over meetings of the Cyber Appellate Tribunal. He has been given the mandatory obligations to exercise and discharge such other powers and functions of the Cyber Appellate Tribunal as may be prescribed. The said powers of superintendence and directions have been given to this Chairperson of the Cyber Appellate Tribunal to ensure that there is uniformity of approach adopted by the Cyber Appellate Tribunal and there are no problems and hurdles in the day to day running and functioning of the Cyber Appellate Tribunal.

Section 52B – Distribution of Business among Benches

"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."

The Chairperson of the Cyber Appellate Tribunal has also been given the discretion to distribute business between different Benches of the Cyber Appellate Tribunal. As and when Benches are constituted, discretion has been given to the Chairperson of Cyber Appellate Tribunal that he may by order distribute the business of the Cyber Appellate Tribunal amongst the Benches. Further, he nas been given the discretion to distribute the matters being dealt with by each Bench of the Cyber Appellate Tribunal.

Section 52C – Powers of the Chairperson to Transfer Cases

"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."

Since the Chairperson of the Cyber Appellate Tribunal has been given the general powers of superintendence and directions in the conduct of the affairs of the Cyber Appellate Tribunal, he has also been given the specific power to transfer cases. Under the said power, he can transfer cases pending before one Bench for the disposal to another Bench. However, the said power about transfer of cases can be exercised by the Chairperson in any of the two circumstances:

(a) when an application is moved by one of the parties and after notice to the parties and after hearing them as he may deem proper to be heard; or

(b) *suo motu* by the Chairperson without such notice.

The said power has been granted to the Chairperson so as to ensure that there is smooth conducting of business in the Cyber Appellate Tribunal and further that all administrative issues are dealt with by the Chairperson of Cyber Appellate Tribunal in terms of transferring cases from one Bench to another Bench. In that sense, the powers granted to the Chairperson of the Cyber Appellate Tribunal is the powers granted to the Chief Justice of High Court to transfer cases from one Bench for the disposal to any other Bench of the High Court.

Section 52D – Decision by Majority

"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."

Section 52D of the Information Technology Act, 2000 recognizes the fact that there could be difference of judicial opinion on legal propositions. As such, it could be possible that different members of the Bench could take different legal stands on particular issues. The matter is likely to become more complicated when there are only two-member Benches and both the members of Bench can take different viewpoints in terms of their opinion on legal issues. In such a case, section 52D provides a simple way to proceed forward. Section 52D stipulates that if two-member Bench is hearing the matter and members differ in opinion on any point, the members are mandated to take their own point by points on which they differ and then make a reference to the Chairperson of the Cyber Appellate Tribunal. Once the reference is made to the Chairperson of Cyber Appellate Tribunal, he is authorized to hear the point by point issues himself and also decide. In such a scenario, such point by point issues shall be meant to be decided according to the opinion of the majority of the members who have heard including the members who heard for the first time. As such, the majority of vote would be the majority decision deemed to be taken by the Cyber Appellate Tribunal. Normally if the two-member Benches of the Cyber Appellate Tribunal have different viewpoints, the point of difference could be referred to the larger Bench and then normally the

larger Bench would have to decide the entire matter which then would be applicable upon the smaller Bench. However, section 52D of the Information Technology Act, 2000 adopts innovative approach of not constituting the larger Bench. Instead, section 52D stipulates that point of difference will be made to the Chairperson who independently decides the points himself and then on the basis of his decision, the matter would be decided by majority amongst the other members. Such a principle goes against the entire philosophy of referring matter to the larger Bench and instead tends to make mockery of the entire system of a decision by majority in the Cyber Appellate Tribunal. It would have been far better if the lawmakers would have adopted the same approach as is adopted in the Supreme Court of India and in different High Courts of the country. If two member-Bench of the Cyber Appellate Tribunal differ at a point, they could refer the matter to the larger bench who would then decide in totality and then the decision of the larger Bench of the Cyber Appellate Tribunal should have been binding on all other Benches. Instead, section 52D has a different approach which is currently unknown in the history of Indian jurisprudence. It will be interesting to see how this interesting innovative approach of decision by majority, in the context of Cyber Appellate Tribunal will work in the times to come.

Section 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 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."

Section 53 provides for the procedure for filling-up of vacancies in the office of the Chairperson and members of the Cyber Appellate Tribunal. Other than temporary if there is any vacancy which occurs in the office of the Chairperson or members of the Cyber Appellate Tribunal, then mandatory responsibility has been given to the Central Government to appoint any other person to the said office. That appointment has to be in accordance with the provisions as are detailed under Chapter X of the Information Technology Act, 2000 to fill the vacancy. Further, section 53 provides that the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

Section 53 of the Information Technology Act, 2000 has also been amended by the Information Technology (Amendment) Act, 2008, whereby in place of the term "Presiding Officer", the term "Chairperson or Member" has been inserted.

Section 53 empowers the Central Government to fill a vacancy that has been caused in the office of the Chairperson or Member as the case may be of the Cyber Appellate Tribunal. However, the vacancy to be filled has to be for reasons other than temporary absence. In the case of all vacancies other than temporary absence, it has been made mandatory for the Central Government to appoint another person as Chairperson or Member in accordance with the Information Technology Act, 2000 to fill the vacancy.

In that event, the proceedings may be continued before the Cyber Appellate Tribunal from the same stage from which the vacancy is filled. This provision

ensures a continuation of the office of the Chairperson or Member and envisages that in case of any disruption, the Government is empowered to fill the vacancy to ensure continuous and smooth working of the Cyber Appellate Tribunal. This provision has been enacted in order to ensure that appeals are heard expeditiously and are not kept pending due, to the existence of a vacancy in the office of the Chairperson or Member of a Cyber Appellate Tribunal.

Section 54 – Resignation and Removal

(1) The Chairperson or Member of the Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Provided that the said Chairperson or Member 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 Member 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 Chairperson or Member 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."

Section 54 stipulates the procedure in case of resignation and removal of the Chairperson or Member of the Cyber Appellate Tribunal. It has been provided that the Chairperson or Member of the Cyber Appellate Tribunal may resign from his office by giving a notice in writing under his own hand addressed to the Central Government. In the event of the Chairperson or Member resigning, he shall continue to hold office until the expiry of a period of 3 months from the date of the receipt of notice of his resignation or until his successor enters upon his office or until the expiry of his term, whichever is the earliest. However, discretion has been vested in the Central Government to permit the Chairperson or Member to relinquish his office sooner.

A very complicated procedure has been stipulated for the removal of the Chairperson of the Cyber Appellate Tribunal under section 54(2). Under section 50 of the IT Act, 2000 a person, in order to be qualified as the Chairperson, must be or has been or is qualified to be a judge of the High Court. Given the high qualifications required for the post of the Chairperson, it has been stipulated that the Chairperson can only be removed after an inquiry is conducted against him.

A Judge of the Supreme Court shall conduct the inquiry. In the inquiry, the Chairperson has to be informed of all the charges against him. Also, a reasonable opportunity of being heard in respect of all the charges in question has to be given to the Chairperson. These provisions ensure compliance with the principles of natural justice, good conscience, fair play and equity.

If, on inquiry, it is found that the Chairperson is guilty of proven misbehaviour or incapacity, then the report of the inquiry has to be forwarded to the Central Government and then, the Central Government may, by order, direct the Presiding Officer to be removed from his office.

The Chairperson can only be removed on two grounds:—

1. Proven misbehaviour,
2. Proven incapacity.

It is clear that barring the above grounds, the Chairperson cannot be removed from his office on any other charge whatsoever.

The Information Technology Act, 2000 has also stipulated that the Government may regulate and elaborate the details of the procedure for the investigation of misbehaviour or incapacity of the Chairperson. This may be done by the Central Government by enacting appropriate rules under section 87(2)(o) of the Information Technology Act, 2000.

Section 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 of a Cyber Appellate 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 a Cyber Appellate Tribunal."

Section 55 seeks to grant finality to the orders for constitution of the Cyber Appellate Tribunal and its proceedings. Section 55 states that on no condition can an order of the Central Government appointing any person as the Chairperson or the Member of a Cyber Appellate Tribunal be called into question in any manner.

The first part of section 55 has been couched in mandatory form and it rules out any challenge to the order of appointment of the Chairperson or the Member of a Cyber Appellate Tribunal. This provision, in my opinion is absolutely contrary to established principles of law.

In India, the Constitution of India governs us. The Constitution of India has been held to be sacrosanct. It has got its own basic structure, which cannot be altered. Judicial review has been held to be an integral part of the basic structure of the Constitution by the Supreme Court. No law can exclude judicial review. Section 55 purports to make the appointment of Chairperson or Member of the Cyber Appellate Tribunal outside the ambit of judicial review, which is not permissible, and as such, the present provision is likely to be struck down as *null* and *void* by the courts.

Further, it has also been stated in section 55 that no act or proceeding before the Cyber Appellate Tribunal shall be called in question on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal. This provision is again violative of the rule of law and the jurisprudence that we know in India.

It is common parlance that if a Tribunal has to be constituted, it has to be constituted as per the law and, if it is not constituted as per law, then the Tribunal is no Tribunal in the eyes of law and is a nullity. If there is a defect in the constitution of a Cyber Appellate Tribunal, that goes to the root of the entire matter. As such, in such a case, the entire constitution of the Cyber Appellate Tribunal is defective as per law and a defectively constituted Tribunal is no Cyber Appellate Tribunal in the eyes of law. As such, all proceedings before a defective Cyber Appellate Tribunal would have no relevance or validity in the eyes of law and would not stand the scrutiny of law.

Hence, the second part of section 55 excluding the challenge on the ground of defect in the constitution of the Cyber Appellate Tribunal is not legally tenable. Also, it is violative of the principles of law laid down by the Constitution of India and also by different judgments delivered by the Supreme Court.

Section 56 – Staff of the Cyber Appellate Tribunal

"(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as the Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Chairperson.

(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."

Section 56 provides for the staff of Cyber Appellate Tribunal. It has been left to the Central Government to provide such officers and employees to the Cyber Appellate Tribunal as it may deem fit. It has been provided that all the officers and employees of the Cyber Appellate Tribunal shall discharge their functions under the general control, supervision and superintendence of the Chairperson.

The salary of the officers and employees and their allowances and other terms and conditions of service may be prescribed by the Central Government under section 87(2)(t) of the Information Technology Act, 2000. Such officers and employees of the Cyber Appellate Tribunal shall assist the Tribunal in conducting its business and would be necessary for the smooth working of the same.

Section 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 tor 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 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."

Section 57 provides for the procedure for filing and disposing of the appeal before the Cyber Appellate Tribunal. It has been stated that the Cyber Appellate Tribunal shall hear all appeals from all orders passed by the Controller or an Adjudicating Officer. The only exception provided is that where the Adjudicating Officer with the consent of both the parties has passed any order, no appeal shall lie with the Cyber Appellate Tribunal.

The words used in section 57(1) are "any person aggrieved by an order made by the Controller or an Adjudicating Officer under this Act may prefer an appeal". Such appeal may not only be preferred by the party against whom the order has been passed, but it can also be preferred by any other person or legal entity which, though it has not been a party before the Controller or an Adjudicating Officer, is affected or aggrieved by the operation of the order of the Controller or Adjudicating Officer. Thus, even persons, who are strangers to the proceedings before the Controller or Adjudicating Officer, can challenge the order of the Controller or Adjudicating Officer before the Cyber Appellate Tribunal.

Further, it has been specified that the period of limitation of filing any appeal to the Cyber Appellate Tribunal shall be 45 days from the date on which a copy of the order, made by the Controller or the Adjudicating Officer, is received by the aggrieved person. Therefore, the period of limitation starts on the date of receipt of order and not from the date of the passing of the impugned order.

The appeal has to be in such form and accompanied by such fees as may be prescribed by the Central Government. At this stage, it is prudent to refer to the following provisions of The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000:—

"Rule 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.

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 authorizing 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 'vakalatnama'.

The proviso of section 57(3) gives power to the Cyber Appellate Tribunal to entertain an appeal filed much beyond the prescribed period of limitation of forty-five days. However, the appeal can be entertained after the expiry of the period of limitation, if the Cyber Appellate Tribunal is satisfied that there was "sufficient

cause" for not filing it within that period. The words used are "sufficient cause" and since the words have not been defined under the IT Act, 2000, we would have to rely upon the meaning of the words "sufficient cause" as has been defined and elaborated within the context of section 5 of the Limitation Act, 1963.

The Supreme Court has, in numerous decisions, explained the ambit of the words "sufficient cause". The interpretation of the words "sufficient cause" is very necessary for condonation of delay in filing the appeal before the Cyber Appellate Tribunal. The Supreme Court has had various occasions to interpret the words "sufficient cause" as appearing in section 5 of the Limitation Act. In *Sitaram Ramcharan* v. *M.N. Nagrashana*[1], the Supreme Court held as follows:-

In dealing with the question of condoning delay under section 5 of the Limitation Act, the party has to satisfy the court that he had sufficient cause for not preferring the appeal or making the application within the prescribed time, and this has always been understood to mean that the explanation has to cover the whole of the period of delay. The contention that once it is shown that there was sufficient cause for not making the application within the prescribed time then the application can be made any time thereafter is not correct.

The Supreme Court in *Sarpanch, Lonand Gram Panchayat* v. *Ramgiri Gosavi*[2], held as under:—

"The words "sufficient cause" should receive a liberal construction so as to advance substantial justice when no negligence nor inaction nor want of bona fides is imputable to the appellant...

...The Authority has a discretion to condone the delay in presenting the application provided sufficient cause for the entire delay is shown to its satisfaction. This discretion like other judicial discretion must be exercised with vigilance and circumspection according to the justice, common sense, and sound judgment. The discretion is to know through law what is just."

In *Shakuntala Devi Jain* v. *Kuntal Kumari*,[3] the Supreme Court held that section 5 of the Limitation Act has to be properly interpreted. It was held that:—

"Section 5 gives the courts a discretion which in respect of jurisdiction is to be exercised in the way in which judicial power and discretion ought to be exercised upon principles which are well understood; the words 'sufficient cause' receiving a liberal construction so as to advance substantial justice when no negligence nor inaction nor want of bona fides *is imputable to the appellant."*

The Supreme Court further elaborated upon the scope and ambit of the words 'sufficient cause' in the case entitled *State of Haryana* v. *Chandra Mani*.[4] In the said case it was held as under:—

"The expression "sufficient cause" should, therefore, be considered with pragmatism in justice-oriented approach rather than the technical detection of

1. AIR 1960 SC 260: (1960) 1 SCR 875: 1960 SCJ 183.
2. AIR 1968 SC 575.
3. AIR 1969 SC 575: (1969) 1 SCR 1006.
4. (1996) 3 SCC 132: AIR 1996 SC 1623: 1996 AIR SCW 1672.

sufficient cause for explaining every day's delay. The factors, which are peculiar to, and characteristic of the functioning of the governmental conditions would be cognizant to and requires adoption of pragmatic approach in justice-oriented process. The court should decide the matters on merits unless the case is hopelessly without merit. No separate standards to determine the cause laid by the State vis-a vis private litigant could be laid to prove strict standards of sufficient cause. "

Finally, the Supreme Court once again had an opportunity to discuss the ambit and scope of the words 'sufficient cause' and also stated various guidelines that need to be adopted by court exercising the power of condonation of delay. In the case entitled *N. Balakrishnan* v. *M. Krishnamurty*,[5] the Supreme Court has held as under:—

"Condonation of delay is a matter of discretion of the court. section 5 of the Limitation Act does not say that such discretion can be exercised only if the delay is within a certain limit. Length of delay is no matter, acceptability of the explanation is the only criterion. Sometimes delay of the shortest range may be uncondonable due to a want of acceptable explanation whereas in certain other cases, delay of a very long range can be condoned, as the explanation thereof is satisfactory. In every case of delay, there can be some lapse on the part of the litigant concerned. That alone is not enough to turn down his plea and to shut the door against him. If the explanation does not smack of mala fides *or it is not put forth as part of a dilatory strategy, the court must show utmost consideration to the suitor. But when there is reasonable ground to think that the delay was occasioned by the party deliberately to gain time, then the court should lean against acceptance of the explanation. A court knows that refusal to condone delay would result in foreclosing a suitor from putting forth his cause. There is no presumption that delay in approaching the court is always deliberate. The words "sufficient cause" under section 5 of the Limitation Act should receive a liberal construction so as to advance substantial justice.*

Once the court accepts the explanation as sufficient, it is the result of positive exercise of discretion and normally the superior court should not disturb such finding, much less in revisional jurisdiction, unless the exercise of discretion was on wholly untenable grounds or arbitrary or perverse. But it is a different matter when the first court refuses to condone the delay. In such cases, the superior court would be free to consider the cause shown for the delay afresh and it is open to such superior court to come to its own finding even untrammelled by the conclusion of the lower court.

However, while condoning the delay, the court should not forget the opposite party altogether. It must be borne in mind that he is a loser and he too would have incurred quite large litigation expenses. It would be a salutary guideline that when courts condone the delay due to laches on the part of the applicant, the court shall compensate the opposite part for his loss."

Thus, the present law is crystal clear. It is also pertinent to note that section 5 of the Limitation Act uses the word "within such period" whereas section 57(3) of the IT Act uses the word "within that period". The import and underlying

5. (1998) 7 SCC 123: AIR 1998 SC 3222: 1998 AIR SCW 3139.

meaning of both the phrases is the same. The Supreme Court in *Ramlal* v. *Rewa Coal Fields Ltd.*[6] has categorically held as below:—

> *"…. "Within such period" means within the period, which ends with the last day of limitation prescribed. In other words, in all cases falling under section 5 what the party has to show is why he did not file an appeal on the last day of limitation prescribed. That may inevitably mean that the party will have to show sufficient cause not only for not filing the appeal on the last day but to explain the delay made thereafter day by day. In other words, in showing sufficient cause for condoning the delay the party may be called upon to explain for the whole of the delay covered by the period between the last day prescribed for filing the appeal and the day on which the appeal is filed. To hold that the expression "within such period" means "during such period" would be repugnant in the context."*

Thus, the various principles of law as enunciated by the Supreme Court as detailed above would be fully applicable to the provisions of section 57(3) of the Information Technology Act, 2000.

The Tribunal possesses discretionary power to entertain an appeal even after the prescribed period. Since the decision of the Tribunal affects the rights of the parties, it is required by the rule of law that it adheres to the notions of fairness and reasonability. It was held in *Mahabir Auto Stores* v. *Indian Oil Corporation*,[7] that

> *"every act of a public authority is subject to the rule of law and must be supported by reasons and it should meet the test of article 14 of the Constitution".*

Section 57(4) stipulates that the provisions of natural justice have to be duly complied with by the Cyber Appellate Tribunal, while adjudicating any appeal. On the receipt of any appeal, the Tribunal has to grant, the parties to the appeal, an opportunity of being heard. After hearing both the parties, the Tribunal is empowered to pass such orders as it thinks fit. The Tribunal can confirm, modify or set aside the order appealed against. It is expected that the Tribunal shall pass a written and detailed order, giving details of the reasons and grounds on the basis of which, it has made its decision or order.

The appellant may either appear in person or may authorize any legal practitioner on his behalf before the Cyber Appellate Tribunal as per the provisions of the section 59 of the IT Act, 2000.

After the Cyber Appellate Tribunal has passed its order, it has been mandated that the Tribunal must send a copy of the order so passed to all the parties of the appeal as also to the concerned Adjudicating Officer who passed the impugned order, challenged in appeal before the Tribunal. It is pertinent to mention that the limitation for filing an appeal against the order of the Cyber Appellate Tribunal starts from the date of receipt of the copy of the order from the Cyber Appellate Tribunal.

It is important to note that the jurisdiction of civil courts has been totally excluded from the Information Technology Act, 2000, on all matters that are within

6. AIR 1962 SC 361: 1961 (2) SCJ 556: (1962) 2 SCR 762.
7. (1999) 69 Comp Cas 746.

the purview of an Adjudicating Officer or the Cyber Appellate Tribunal, as per section 61 of the Information Technology Act, 2000.

Section 57(6) has been enacted, keeping in mind the requirements of expeditious disposal of appeals by the Cyber Appellate Tribunal. The Legislature was well aware of the huge pendency of cases and appeals in different courts and tribunals in the country. In addition, the Legislature was also aware of the fact that in the age of Information Technology, speed is of essence. As such, the Legislature has inserted section 57(6).

There is no absolute mandatory time frame within which an appeal has to be disposed of by the Cyber Appellate Tribunal. However, section 57(6) mandates that the Cyber Appellate Tribunal shall deal with the appeal, filed before it, as expeditious as possible. Thus, the discretion to decide the appeal within a specific time frame has been vested with the Cyber Appellate Tribunal, though the Tribunal is mandated to deal with the appeal as expeditiously as possible.

It has further mandated that the Cyber Appellate Tribunal must make all endeavours to dispose of the appeal finally within 6 months from the date of receipt of the appeal. It is important to note that though the Cyber Appellate Tribunal is expected to dispose of any appeal within a period of 6 months, it does not mean that in case if an appeal is not disposed of within 6 months, the same would amount to a contravention of section 57(6). Section 57(6) only requires that all endeavours shall be made to dispose of the appeal finally within 6 months.

The approach adopted by section 57(6) is indeed a prudent approach, inasmuch as in the context of Internet and the electronic environment, litigants would not want to wait for endless period of time before getting their appeal disposed of. It is also pertinent to note that appeals to the Cyber Appellate Tribunal would be made by entities conversant in or utilizing Information Technology. As such, the class of litigants filing appeals to the Cyber Appellate Tribunal would indeed be computer and net savvy. It is to address the specific requirements of this new class of litigants that section 57(6) has been enacted. In any case, the same is a wonderful step ahead as it reiterates the intention of the Legislature for expeditious disposal of appeals so that there is no pendency of cases.

Section 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 (5 of 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.*
>
> *(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 (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.

(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 (45 of 1860) 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 (2 of 1974)."

Section 58 stipulates the powers and procedures of the Cyber Appellate Tribunal. Since, the Legislature desires that the Tribunal has to dispose of the appeal finally within six months from the date of its filing, it is imperative that the Tribunal be not caught in procedural and legal tangles.

With that purpose in mind, the law states that the Cyber Appellate Tribunal shall not be bound by the procedure laid down by Code of Civil Procedure, 1908. The Cyber Appellate Tribunal shall be bound by principles of natural justice. The Tribunal has also been given the powers to regulate and streamline its own procedures, including the power to decide the place where it shall have its sittings.

In addition, the Cyber Appellate Tribunal has been vested with the same powers as vested in a civil court under the Code of Civil Procedure, 1908 in respect of various matters. These include the power of summoning and enforcing the attendance of any person and examining him on oath, the power of discovery and production of documents or other electronic records, receiving evidence by way of affidavit and issuing commissions for recording evidence of witnesses or for examining documents, reviewing its decisions, dismissing applications for default or deciding them *ex-parte*.

Section 58(2)(g) uses the words "any other matter which may be prescribed". Any other matter may be prescribed by the Central Government by notification in the Official Gazette. This is a wide clause that can be used effectively and innovatively to ensure the effective discharge of the functions of the Cyber Appellate Tribunal.

These powers granted to the Cyber Appellate Tribunal are likely to lead to some practical difficulties. These practical difficulties would be in the sense while the Cyber Regulations Appellate Tribunal have the power of dismissing an application for default or deciding it *ex-parte* under section 58(2)(f), it does not have the power of setting aside any order of dismissal of any application for default or the power of setting aside any order passed by it *ex-parte*. The Cyber Regulations Appellate Tribunal does not have the specific power of granting interim relief.

All proceedings before the Cyber Appellate Tribunal shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of Indian Penal Code. Thus, if any person, intentionally gives false evidence in any stage of the

proceedings before the Cyber Appellate Tribunal, or fabricates false evidence for the purpose of being used in any stage of the judicial proceeding before the Cyber Appellate Tribunal, he shall be punished, for the offence of false evidence, which shall be imprisonment of either description for a term which may extend to seven years and shall also be liable to fine. Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding for the purposes of section 196 IPC. Thus, whoever consciously 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 as detailed hereinabove.

Further, whoever, intentionally offers any insult or causes any interruption to the Cyber Appellate Tribunal, while the Chairperson of such Tribunal being a public servant is sitting, in any stage of the judicial proceedings, shall be punished with simple imprisonment for a term which may extend up to six months or with fine which may extend to one thousand rupees or with both.

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. Section 195 Cr. P.C. details about the prosecution for contempt of lawful authority of public servant, for offences against public justice and for offences relating to documents given in evidence. Chapter XXVI of Cr. P.C. elaborates on the various provisions as to offences affecting the administration of justice.

Section 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."

This provision deals with the issue relating to the right to legal representation. Since the Cyber Appellate Tribunal has been made the first tier of appeal, the Legislature has appreciated the fact that questions likely to be raised before the tribunal would involve substantial legal issues. Section 59 has allowed the appellant to appear before the Tribunal either in person or through one or more legal practitioners or advocates. Further, the appellant has the discretion to authorize any of his or its officers to present his or its case before the Cyber Appellate Tribunal.

This is a welcome provision since Cyberlaw is a new area and companies as well as individual entities, cannot be expected to know all the intricacies of law of this newly emerging field. Lawyers are trained in law; therefore they have a much better chance of putting across the complicated legal issues to the Tribunal than a person with non-legal background.

Section 60 – Limitation

"The provisions of the Limitation Act, 1963, (36 of 1963), shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal."

Section 60 states that the provisions of the Limitation Act, 1963 shall be applicable to an appeal made to the Cyber Appellate Tribunal. This means that the Limitation Act, as far as may be, applies to the proceedings before the Cyber Appellate Tribunal.

Thus, the principles enshrined in section 5 of the Limitation Act would also apply in cases of appeals filed before the Cyber Appellate Tribunal. This really means that any appeal may be admitted by the Cyber Appellate Tribunal after the prescribed period of limitation if the appellant satisfies the Cyber Appellate Tribunal that he had sufficient cause for not preferring the appeal within such time, thereby supplementing the provisions of section 57 of the Information Technology Act, 2000. As such, the entire principles of law laid down by the Supreme Court to interpret the meaning of the words "sufficient cause" in section 5 of the Limitation Act, 1963, shall be directly applicable to the Cyber Appellate Tribunal.

Section 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."

Section 61 has specifically excluded the jurisdiction of all civil courts in mandatory terms. The jurisdiction of the civil court has been barred in respect of any and all matters, which an Adjudicating Officer or the Cyber Appellate Tribunal, provided for under the Information Technology Act, 2000, are empowered to determine and decide.

Under section 46, the Adjudicating Officer has been given the power to hold an inquiry and to adjudge whether any person has committed a contravention of any of the provisions of the Information Technology Act, 2000. Thus, all the issues relating to the inquiry of contravention of any provisions of the Information Technology Act, 2000 would be outside the ambit of the jurisdiction of the civil court. Similarly, it is mandatory that all matters decided by an Adjudicating Officer under section 46 of the Information Technology Act, 2000 be appealed before the Cyber Appellate Tribunal and as such, the jurisdiction of the civil court cannot be invoked in these cases.

Cyber Appellate Tribunal has been given the power of making orders in appeals, confirming, modifying or setting aside the orders appealed against.

If any person, without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, gains access to such computer, computer system or computer network and downloads, copies or extracts any computer database or information, or introduces or causes to be introduced any computer contaminant or damages or disrupts or denies access to any person of any computer, computer system or computer network or causes to do the same, then also the only remedy available under the Information Technology Act, 2000 is to approach the Adjudicating Officer and the civil court would have no jurisdiction to adjudicate the matters falling within the exclusive jurisdiction of the Adjudicating Officer.

It is important to note that since the jurisdiction of the civil courts is barred under section 61 of the Information Technology Act, 2000, the Legislature has conferred upon the Adjudicating Officer and the Cyber Appellate Tribunal the

same powers as are vested in a civil court under the Code of Civil Procedure, 1908. These powers conferred are in respect of all matters including summoning and enforcing the attendance of any person, examination on oath, discovery and production of documents and other electronic records, receiving evidence by affidavit, issuing summons for the examination of witnesses or documents, reviewing decisions and dismissing applications and any other matter which may be prescribed.

Section 61 also ensures and makes it mandatory that no court of any jurisdiction or other authority shall grant an injunction in respect of any action taken or to be taken in pursuance of any power conferred by or under the Information Technology Act, 2000. The rationale of this is to ensure that there is no disturbance in the performance of statutory duties by various statutory bodies under the Information Technology Act, 2000 and that the grant of an injunction may not hijack the working and procedures of different authorities under the Information Technology Act, 2000.

It is important to note that though no court will have jurisdiction over a matter which an Adjudicating Officer is empowered to determine, the power of granting damages up to five crore rupees has been given under section 43 of the Information Technology Act, 2000. The power has to be exercised by the Adjudicating Officer under section 43(2) of the Information Technology Act, 2000.

A claim in excess of five crore rupees can be filed in a civil court of competent jurisdiction.

Section 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 be filed within a further period not exceeding sixty days."

Section 62 provides the second tier of appeal under the Information Technology Act, 2000. The first tier of appeal is the Cyber Appellate Tribunal. The second tier is the High Court. If anyone is not satisfied by any decision or order passed by the Cyber Appellate Tribunal, he may file an appeal to the concerned High Court.

The period of limitation for filing an appeal under section 62 has been specified as 60 days from the date of communication of the decision or order of the Cyber Appellate Tribunal to the appellant. The ground of appeal can be either on question of facts or law arising out of such order.

Normally, in civil jurisprudence, a second appeal can be preferred on any question of law. The Information Technology Act, 2000 makes a departure in this regard. Due to the provision of the first appeal to the Cyber Appellate Tribunal, any matter under the IT Act, 2000 reaches the High Court for the first time only in second appeal. As such, the right has been given to the appellant to file an appeal on any question of fact or law arising out of the impugned order.

The proviso to section 62 empowers the High Court to extend the period of limitation by a period of 60 days. However, the extension of the period of limitation has only to be done on the discretion of the High Court, exercised on well-established judicial principles. This discretion can be exercised if and only if the High Court is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the limitation period of 60 days from the date of communication of the decision or order of the Cyber Appellate Tribunal.

For the import, meaning and interpretation of the words "sufficient cause", kindly see the commentary under section 57 of the Information Technology Act, 2000.

Section 63 – Compounding of Contraventions

"(1) Any contravention under this Act 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.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from 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 (1), 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."

Section 63 of the Information Technology Act provides for a provision relating to compounding of contraventions or violations of different provisions of this Act. It specifically states that the Controller or any officer authorized by him in this regard or the Adjudicating Officers shall have the powers of compounding any contravention made under the provisions of this Act either before or after the institution of adjudication proceedings. The idea of inserting the present section seems to be that violations of the provisions of the Information Technology Act, 2000 would not be totally penal in nature and that no useful purpose would be solved to take adjudication proceedings to the fullest extent and so, the power of compounding of contravention has been given. However, this power may be exercised according to the discretion of the Controller or any other officer authorized by him. The law further states that such power may be exercised subject to such conditions as the Controller or such other officer or the Adjudicating Officer may specify.

The proviso to section 63(1) categorically states that the sum for compounding shall not in any case exceed the maximum amount of prescribed penalty under the Act for the contravention so compounded. The rationale of the legislation seems to be that a person should not be penalized beyond the penalty as detailed in the respective penalties prescribed under the Information Technology Act, 2000.

Section 63(2) is aimed at preventing the misuse of the above provision. It is aimed at preventing the misuse of the provision of compounding by habitual offenders. It is mandatory in nature and categorically states that it is not applicable to any person who commits the same contravention as done by him previously within a period of three years from the date on which the first contravention committed by him was compounded.

By incorporating the power of compounding, the legislation has played a lenient role in dealing with first time violators of the provisions of this Act. However, this approach is not available to the offender in case he repeats the same offence within the period of three years from the date when the first offence was compounded.

The *Explanation* to section 63(2) explains that a second or subsequent contravention committed after the expiry of three years from the first date of compounding would mandatorily be deemed to be the first contravention and as such, the power of compounding of such contravention can be exercised as in the case of the first contravention. The logic behind this seems to be that the Legislature wants to have a minimum deterrence period of 3 years should anyone want to take the benefit of exercise of the power of compounding of contravention.

Section 63(3) makes a logical step forward by stating that when a contravention has been compounded, there shall be double jeopardy and no proceedings shall be taken against the person guilty of such contravention in respect of the contravention so compounded. The rationale behind this is to prevent a person from being prosecuted twice for the same contravention and also to minimize proceedings from the administrative point of view.

However there are practical difficulties that section 63 poses. *Firstly*, compounding of contravention is based upon the principle of condoning a specific contravention, penal or otherwise, for a consideration, normally monetary in character. Section 63(1) only talks about "any contravention under this chapter". Section 63 appears in Chapter X of the Information Technology Act. Thus, only contraventions under this Act of the Information Technology Act can be compounded by the Controller or his authorized officer. The perusal of Chapter X of Information Technology Act shows that it is Chapter which provides for the establishment, composition and functions of the Cyber Appellate Tribunal. The provisions of this Chapter are largely regulatory or procedural in character. Another possible consequence of the wordings of section 63 is that the present section concerning compounding of offences is made applicable to provision of the Information Technology Act, which are capable of being compounded. Consequently this section is a provision inserted as a result of careless drafting.

Section 64 – Recovery of Penalty or Compensation

"A penalty imposed or compensation awarded under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Electronic Signature Certificate, as the case may be, shall be suspended till the penalty is paid."

Section 64 outlines the procedure for recovery of penalty imposed or compensation awarded under the Information Technology Act, 2000. If the said penalty and/or compensation are not paid, it shall be recovered as an arrear of land revenue. The law further aims to put a person not paying a penalty and/or compensation under some liability, till the time the penalty and/or compensation are not paid, the licence of the Certifying Authority, shall be suspended. Similarly, if the penalty has been imposed or compensation has been awarded on an individual who is a subscriber of an Electronic Signature Certificate, then till the time the individual does not pay the penalty or compensation, his Electronic Signature Certificate shall be suspended.

However, one question that comes up for consideration is how to enforce an order passed under section 43 by the Adjudicating Officer. Section 64 of the Information Technology Act states that a penalty or compensation including a penalty or compensation imposed under section 43 of the Information Technology Act, if it is not paid, shall be recovered as an arrear of land revenue. Since land revenue is a state subject under List II in the Seventh Schedule to the Constitution, different States have enacted different laws relating to land revenue and the recovery of its arrears.

By way of illustration, we can take the example of Delhi, which has enacted the Delhi Land Reforms Act, 1954.

Section 136 of the Delhi Land Reforms Act, 1954 provides the procedure for recovery of arrears of land revenue. Section 136 states as follows:—

"An arrear of land revenue may be recovered by any one or more of the following processes—

(h) by serving a writ of demand or a citation to appear on any defaulter,

(i) by arrest and detention of his person,

(j) by attachment or sale of his movable property including produce,

(k) by attachment of the holding in respect of which the arrear is due,

(l) by sale of the holding in respect of which the arrear is due, or

(m) by attachment or sale of other immovable property of the defaulter."

The administrative machinery under the land revenue legislations of different States can recover the arrears of land revenue. In the context of the IT Act, 2000, once the Adjudicating Officer awards compensation or penalty by way of damages, the party, against whom such damages are awarded, is duty bound to pay the penalty unless the same has been set aside in appeal. If that party fails to pay the penalty or compensation by way of damages, then the applicant/complainant can move an application before the Adjudicating Officer for recovery of the same. In that case, the Adjudicating Officer can direct the said penalty or compensation to be recovered as arrears of land revenue. The Adjudicating Officer can pass an order directing the Tahsildar/Collector of the concerned area to recover the penalty as an arrear of land revenue.

However, the law does not state what would be the liability for an offender who is neither a Certifying Authority nor a subscriber of an Digital Signature Certificate, but who is a mere netizen. Further, how the arrear of land revenue shall be recovered has not been specified under the Information Technology Act, 2000 and it will have to be *per se* recovered as per the provisions of the Code of Civil Procedure in a Civil Court of a competent jurisdiction. This is so because the Information Technology Act, 2000 shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. This however, does not inhibit or restrict the application of the other laws which are consistent with the Information Technology Act, 2000.

CHAPTER XI
OFFENCES

INTRODUCTION

Chapter XI of the Information Technology Act, 2000 has been entitled "Offences". Broadly speaking, it deals with various offences done in the electronic format as also those offences concerning computers, computer systems and computer networks, (computer crimes) as also those which come within the ambit of cybercrimes.

It is pertinent to mention that "computer crimes" refer to all crimes done through, involving or impacting any computer, computer system or computer network. There is a large area of overlap between "computer crimes" and "cybercrimes". As such, a lot of people use both the terms "computer crimes" and "cybercrimes" interchangeably. The Information Technology Act, 2000 does not propose to be a comprehensive code on all offences concerning the electronic format or concerning computers, computer systems and computer networks or cybercrimes. Before we proceed further to examine each specific cybercrime and offence that the new law has defined, let us examine the brief background of cybercrimes.

The real power of today's Internet is that it is available to anyone with a computer and a telephone line. Internet places in an individual's hands the power of information and communication. It is this very power which is being misused by devious minds for criminal purposes, thereby leading to the growth of cybercrimes. Cybercrimes constitute one of the most important challenges facing cyberspace today.

When Internet was developed, the founding fathers of Internet hardly had any idea that Internet could also be misused for criminal activities. Today, there are many disturbing things happening in cyberspace.

Cybercrime has no one exhaustive definition. At this juncture, I refer to the definition of Cybercrime that I had coined in the nineties. ***Cybercrime refers to all the activities done with criminal intent in cyberspace or using the medium of Internet. These could be either the criminal activities in the conventional sense or activities, newly evolved with the growth of the new medium. Any activity, which basically offends human sensibilities, can be included in the ambit of Cybercrimes.***

Because of the anonymous nature of Internet, it is possible to engage in a variety of criminal activities with impunity, and people with intelligence, have been grossly misusing this aspect of the Internet to commit criminal activities in cyberspace. The field of Cybercrime is just emerging and new forms of criminal

activities in cyberspace are coming to the forefront each day. For example, child pornography on Internet constitutes one serious Cybercrime. Similarly, online pedophiles, using Internet to induce minor children into sex, are as much cybercriminals as any others.

Cybercrimes can be basically divided into three major categories:—

1. **Cybercrimes against persons;**
2. **Cybercrimes against property; and**
3. **Cybercrimes against Government.**

Cybercrimes Against Persons

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer and cyber-stalking.

The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important cybercrimes known today. The potential harm of such a crime to humanity can hardly be overstated. This is one cybercrime, which threatens to undermine the growth of the younger generation and also leave irreparable scars on the minds of the younger generation, if not controlled.

Similarly, cyber harassment is a distinct cybercrime. Various kinds of harassments can and do occur in cyberspace, or through the use of cyberspace. Harassment can be sexual, racial, religious, or of any other nature. Persons committing such harassment are also guilty of cybercrimes. Cyber harassment as a crime also brings us to another related area of violation of privacy of netizens. Violation of privacy of online citizens is a cybercrime of a grave nature. No netizen likes any other person invading the extremely sensitive area of his or her own privacy.

Another cybercrime against persons is that of Cyber stalking. The Internet is a wonderful place to work, play and study. The Net is merely a mirror of the real world, and that means it also contains electronic versions of real life problems. Stalking and harassment are problems that many persons especially women, are familiar with in real life. These problems also occur on the Internet, in the form of "Cyber stalking" or "on-line harassment"

Cybercrimes against Property

The second category of cybercrimes is cybercrimes against all forms of property. These crimes include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

Hacking and cracking are amongst the gravest cybercrimes known till date. It is a dreadful feeling to know that someone has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Coupled with this, the actuality is that no computer system in the world is hacking proof. Any system in the world can be hacked. Using one's own programming abilities, as also various programmes,

with malicious intent to gain unauthorized access to a computer or network are very serious crimes. Similarly, the creation and dissemination of harmful computer programs or virii, which do irreparable damage to computer systems, is another kind of cybercrime. Software piracy is also another distinct kind of cybercrime, which is perpetrated by many people online, who distribute illegal and unauthorized pirated copies of software.

Cybercrimes against Government

The third category of cybercrimes is cybercrimes against Government. Cyber Terrorism is one distinct kind of crime in this category. The growth of Internet has shown that the medium of cyberspace is being used by individuals and groups to threaten international governments as also to terrorize the citizens of a country. This crime manifests itself into cyber terrorism when an individual "cracks" into a government or military maintained website.

Since cybercrime is a newly specialized field, a great deal of development has to take place in terms of putting into place the relevant legal mechanism for controlling and preventing cybercrime. The courts in United States of America have already begun taking cognizance of various kinds of fraud and cybercrimes being perpetrated in cyberspace. However, much work has to be done in this field. Just as the human mind is ingenious enough to devise new ways for perpetrating crime, similarly, human ingenuity needs to be channelized into developing effective legal and regulatory mechanisms to control and prevent cybercrimes. A criminal mind can assume very powerful manifestations if it is used on a network, given the reachability and size of the network.

Internet and cyberspace present various technical hurdles for law enforcement agencies that aim to regulate and investigate cyber crimes. There is a need for law enforcement agencies to prove an electronic trail (e-trail) to link the offender to the cyber crime. For example, in the actual world, fingerprints link an accused to a crime, similarly in cyber space, an e-trail links a cyber criminal to a cybercrime. Given the inherent nature of Internet, a cyber offender in cyber space can be anywhere in the actual world and thus, this global nature of cybercrime poses a big challenge for governments all across the world.

A further challenge relating to cybercrimes is the collection of electronic evidence. The adoption of the latest techniques of cyber forensics is absolutely essential in order to ensure successful investigation and prosecution of a cyber crime. Collection of electronic evidence is another important challenge as information is intangible in nature and the electronic information, in the legally stipulated format, has to be captured in order to be duly produced and proved in court. There are also big challenges in the collection of electronic evidence, given the fact that every time a computer is booted, there is a change, even though slight, in the information residing in the said computer.

Law enforcement agencies have to be well-equipped in data recovery skills and mechanisms. Apart from this, there is an urgent need for the judiciary *per se* to be well-equipped and well-versed with the provisions of Cyberlaw and cybercrime, especially given the fact that cybercrime is increasing at a very fast pace in our country and all over the world. Law enforcement agencies have to understand that cybercriminals are always a step ahead. There is a need for pro-active approach in regulating and preventing cyber crimes.

Since the beginning of Internet, cybercrime has been emerging as a major source of headaches for governments all across the world. The absence of any international law on cybercrime further complicates the matter with different countries assuming distinct national approaches for controlling, regulating and preventing cybercrime.

Cybercrimes – A Turning Point

September 11th, 2001 saw the turning point in the history of the World Wide Web and the Internet. The attacks on World Trade Center's Twin Towers were an example of how terrorist acts had been conceived, planned and committed using the means of Internet. That singular instance of September 11th changed the way we use the Internet and the way Internet is going to be regulated.

International Cybercrime Treaty

The scenario emerging post September 11th, 2001 saw the adoption of the International Cybercrime Treaty. This international treaty, being a creation of the European Union, was adopted after 29 drafts and more than 4 years of work. At the time of writing, more than 40 members of the European Union apart from the United States, Canada, South Africa and Japan have signed the International Cybercrime Treaty.

The International Cybercrime Treaty is the first international benchmark for controlling and regulating cybercrime and for ensuring cooperation amongst different signatory nations for exchanging information concerning cybercrime and cybercriminals. Almost single handedly, the treaty promises to fill-up the void about the need for having an international regulatory mechanism for controlling cybercrime that has existed since the beginning of Internet.

The International Cybercrime Treaty also becomes the first international treaty to be in place for any issue concerning Cyberlaw. The treaty may not be perfect, and no treaty is perfect. However it does give a very strong starting point for international efforts to regulate and control cybercrime. This treaty also promises to possibly change the way cybercrimes would be investigated, regulated and punished in a global scenario, in the context of increasing cooperation and exchange of information between signatory member countries on the issue of regulating cybercrime.

Coming specifically to Chapter XI of the Information Technology Act, 2000, the said chapter raises numerous issues, which need to be discussed, before embarking upon a section by section analysis.

A school of thought exists which states that in all crimes, where a computer is used, only the Information Technology Act, 2000 should be invoked and not the Indian Penal Code, 1860. This argument can be dealt with by saying that the Information Technology Act, 2000 does not comprehensively deal with all kinds of cybercrimes and has only listed certain broad categories of cybercrimes. In the event of a cybercrime happening, which is not specifically covered under the Information Technology Act, 2000, it does not mean that the police and the society

should watch as helpless spectators. The provisions of the Indian Penal Code, 1860 are duly invoked given the non-comprehensive nature of coverage of cybercrimes under the Information Technology Act, 2000.

The Information Technology Act, 2000 remains completely silent on the issue of territorial jurisdiction for the trial of the various offences prescribed under Chapter XI. The provisions of Chapter XIII of Cr. P.C. also do not offer much help given the intrinsic nature of the cybercrimes, which are committed over a network and which are basically technical in character. This flaw of the Information Technology Act has left open vistas for huge litigation in the future.

In addition, the Information Technology Act, 2000 does not display a uniform approach in prescribing punishment. The various provisions of Chapter XI show an imbalance between the degree of culpability and the prescribed punishment. At many instances the law appears to be unjust and not in tune with other established principles of criminal jurisprudence.

It is interesting to note that the Information Technology Act, 2000 is completely silent on the issue of limitation for taking cognizance of any offence. As such, one has no option but to fall back upon section 468 of Cr. P.C. Under section 468(1) Cr. P.C., no court shall take cognizance of any offence of the category specified under 468(2) Cr. P.C. after the expiry of the period of limitation. The period of limitation is prescribed under section 468(2). Most of the offences detailed under Chapter XI of the Information Technology Act fall in the category specified under section 468(2) Cr. P.C.. It is true that section 81 of the Information Technology Act states that the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. Since the provisions relating to limitation for taking cognizance under section 468 Cr. P.C. are not inconsistent with the provisions of the Information Technology Act, the same shall apply for the purposes of calculating limitation.

Classification of Offences Detailed under The IT Act, 2000

Sections	Offence	Cognizable/ Non-Cognizable	Bailable/ Non-Bailable	By What Court Triable
Section 65	Tampering with computer source code and documents	Cognizable	Bailable	Magistrate of the First Class
Section 66	Computer Related Offences	Cognizable	Bailable	Magistrate of the First Class
Section 66A	Punishment for sending offensive messages through communication service, etc.	Cognizable	Bailable	Magistrate of the First Class
Section 66B	Punishment for dishonestly receiving stolen computer resource or communication device	Cognizable	Bailable	Magistrate of the First Class

1	2	3	4	5
Section 66C	Punishment for identity theft.	Cognizable	Bailable	Magistrate of the First Class
Section 66D	Punishment for cheating by personation by using computer resource.	Cognizable	Bailable	Magistrate of the First Class
Section 66E	Punishment for violation of privacy	Cognizable	Bailable	Magistrate of the First Class
Section 66F	Punishment for cyber terrorism	Cognizable	Non-Bailable	Court of Session
Section 67	Punishment for publishing or transmitting obscene material in electronic form.	Cognizable	Bailable, in case of first conviction but in case of second and subsequent conviction Non-Bailable	Magistrate of the First Class
Section 67A	Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.	Cognizable	Non-Bailable	Magistrate of the First Class
Section 67B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.	Cognizable	Non-Bailable	Magistrate of the First Class
Section 67C	Preservation and retention of information by intermediaries.	Cognizable	Bailable	Magistrate of the First Class
Section 68	Failure of comply with the directions of Controller	Non-Cognizable	Bailable	Any Magistrate
Section 69	Power to issue directions for interception or monitoring or decryption of anyInformation through any computer resource.	Cognizable	Non-Bailable	Magistrate of the First Class

1	2	3	4	5
Section 69A	Power to issue directions for blocking for public access of any information through any computer resource.	Cognizable	Non-Bailable	Magistrate of the First Class
Section 69B	Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.	Cognizable	Bailable	Magistrate of the First Class
Section 70	Securing Access to a protected system	Cognizable	Non-Bailable	Court of Session
Section 70B	Indian Computer Emergency Response Team to serve as national agency for incident response.	Non-Cognizable	Bailable	Any Magistrate
Section 71	Penalty for misrepresentation	Non-Cognizable	Bailable	Any Magistrate
Section 72	Breach of confidentiality	Non-Cognizable	Bailable	Any Magistrate
Section 72A	Punishment for disclosure of information in breach of lawful contract.	Cognizable	Bailable	Magistrate of the First Class
Section 73	Penalty for publishing Digital Signature Certificate false in certain particulars	Non-Cognizable	Bailable	Any Magistrate
Section 74	Publication for fraudulent purpose	Non-cognizable	Bailable	Any Magistrate

Section 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."*

Section 65 is the first provision that appears in Chapter XI entitled "Offences" under the Information Technology Act, 2000. This Chapter specifies various kinds of cyber crimes, which have been made penal offences punishable with imprisonment or fine, or both. These are new offences, which have been declared as penal offences, over and above the offences, which are already covered under the Indian Penal Code, 1860.

Section 65 declares tampering with 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, as a penal offence.

The *Explanation* to section 65 defines "computer source code" as the listing of programmes, computer commands, design and layout and the programme analysis of computer resource in any form. Further, section 2(k) defines "computer resource" to mean computer, computer system, computer network, data, computer database or software.

Section 65 defines a new kind of computer crime, which has assumed tremendous relevance across the country. The essential ingredients of section 65 are as follows:-

1. An accused must knowingly or intentionally do the acts specified in this section. Thus, *mens rea* or intention is the basic requirement of the offence under section 65.
2. The acts specified include concealing, destroying, altering or intentionally causing another to conceal, destroy or alter any computer source code.
3. The computer source code must be used for a computer, computer programme, computer system or network.
4. The computer source code must be required to be kept or maintained by the law for the time being in force.

Once the essential ingredients are satisfied, that constitutes an offence under section 65. The offence has been made punishable with imprisonment up to 3 years or with fine, which may extend up to Rs. 2 lakhs, or both.

It is important to note that this entire offence would only be constituted when the computer source code is required to be kept or maintained by any existing law for the time being in force. If any law for the time being in force does not require the computer source code to be kept or maintained, the mandatory ingredients of section 65 will not be satisfied. In that case, even if someone intentionally conceals, destroys or alters or intentionally causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, then also, the same shall not be an offence under section 65.

The words "knowingly or intentionally" are not defined under the Information Technology Act, 2000. Therefore, by necessary implication, we will have to fall back upon the meaning of these words as they occur in the Indian Penal Code.

Similarly, the word "conceal" has not been defined under section 65 of the Information Technology Act, 2000. Webster's New World Dictionary defines the word "conceal" to mean to put out of sight, hide, to keep secret. The word "conceal", used in section 65 Information Technology Act, 2000, has a direct nexus with a computer source code. What would tantamount to concealment in the context of a computer source code cannot be defined exhaustively and has to be determined on a case to case basis or on the peculiar facts and circumstances of each case.

Also, the word "alter" has also not been defined. According to Webster's New World Dictionary, the word "alter" means to make different in details, modify, to become different, to change. The usage of the word 'alter' is likely to throw up numerous challenges in the coming times. Would just superficial altering attract the present offence or has it to be material altering that would be covered by section 65 of the Information Technology Act? The law on section 65 of the Information Technology Act, 2000 is likely to develop over a period of time.

The important question that arises for consideration is whether server logs can be brought within the ambit of the words "computer source code". This question has become more pertinent today, as we have begun to see various criminal activities on the Net, which are aimed at altering, deleting and diminishing the value of computer server logs.

The server logs are not defined in any law of our country. However, if one goes to the internet, one finds that the term "server logs" has been defined as follows:—

> *"Server log files are records of Web server activity (or server activity for any digital medium). They provide details about file requests to a server and the server response to those requests. Collecting and analyzing these files can provide information about who is coming to your Web site; what information they're requesting; their navigation and behaviour"*[1].

Server logs refer to all the logs, logistics and other details that are generated, maintained and preserved by a computer or computer system, which acts as a server. The said logistic data contains details of all activities that have been done on the computer and is the comprehensive source of information for monitoring any activity or for documenting any act done on the server, including any change or alteration, deletion, preservation or saving of any electronic record or information.

Server logs are basically details of various computer commands, whether they exist in the electronic format or the printed format. As such, server logs would come within the broad definition of the terms "computer source code" as given in *Explanation* to section 65 of the IT Act, 2000. Thus, server logs are a listing of computer commands. In any case, they can be seen to be the listings of programme analysis of computer resource in any form. As such, whenever someone intentionally conceals, destroys or alters the server logs used for a computer, computer programme, computer system or network, when such computer source code is required to be kept or maintained by law for the time being in force, it also comes within the ambit of the offence defined under section 65 of the IT Act.

1. www.usability.gov

As per section 77B of the amended Information Technology Act, 2000, the offence under section 65 is a cognizable, non-bailable offence, which can be triable by a Magistrate of the First Class. We now examine some important cases in this regard based on information made available in the public domain.

State of Maharashtra v. *Anand Ashok Khare*

As reported, in July, 2001, the website of Mumbai Police Cyber Cell was broken into. Consequently, the Mumbai police reportedly registered a case under sections 43, 65 and 67 of the IT Act, 2000 along with sections 465, 467, 468, 120B, 34 and 201 IPC. In the said case, after investigations, the police arrested a 23-year-old telecom engineer, Anand Ashok Khare from Mumbai who had posed as the famous hacker Dr Neuker. According to reports, Khare reportedly made several attempts to hack into Mumbai Police Cyber Cell's website and succeeded by using port scan technology to gain the web host's user name "Vijay".

Khare also guessed the password, which also was "Vijay". Khare allegedly hacked the Mumbai Police Cyber Cell website from a cyber cafe in Dadar, Mumbai. In addition, Khare had his own website called www.maharaja.web-jump.com where he called himself "Rudra Analyzer". The said website also had his photograph along with the motto, "we hack, we teach, we make history...." The police were able to trace the alleged cyber criminals with the help of a team of computer experts. Another accomplice of Anand Ashok Khare, namely, Mahesh Mahatre *alias* Da Libran was also arrested.

State of Uttar Pradesh v. *Saket Singhania*

The Noida police reportedly registered a case against Saket Singhania under section 65, IT Act, 2000 on the complaint made by Noida Export Promotion Zone's Software Moguls Industries Ltd. (SIMPL). The crux of the complaint is that SIMPL sent its engineer Saket Singhania to America along with his wife to develop a software programme for the company. The company also bore the couple's expenses in America, but Singhania, instead of working for SIMPL, allegedly sold the concept of the programme to an American client of SIMPL, namely, Fifty Below, consequent to which SIMPL lost its American client.

On investigation, the police found that Saket Singhania had indeed made minor alterations in the programme to sell it. Earlier, it was a C++ programme which was then converted into an ASP programme before being sold. Saket Singhania is alleged to have deposited the money he got from the American company in his wife's account. Consequently, as reported, the police registered a case against Saket Singhania under sections 65, 72 and 75 of the IT Act and sections 406, 408, 465, 469, 471, 474 and 120B of the Indian Penal Code.

Section 66 – Computer-Related Offences

One of the most significant and predominant provisions of the Indian Cyberlaw, is section 66 of the Information Technology Act, 2000. In its earlier avatar, it was one of the most significant provisions of India's first e-commerce legislation. The author had since the year 2000, referred to the said section, as the Mother India provision of the Indian Cyberlaw.

Section 66 has been dramatically amended by the Information Technology (Amendment) Act, 2008, which has completely replaced the language of the earlier section 66 of the Information Technology Act, 2000.

Earlier section 66 of the Information Technology Act, 2000 referred to the offence of hacking in the following terms:

"(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 upto two lakh rupees, or with both."

The offence of hacking defined under the earlier section 66, was extremely wide as to incorporate a variety of acts, which did not amount to hacking, but it was still an offence under section 66 of the earlier Information Technology Act, 2000.

The Information Technology (Amendment) Act, 2008 has inserted a completely new language under section 66. Section 66 of the amended Information Technology Act, 2000 states as follows:

"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 (45 of 1860);

(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860)."

The first important feature that appears from the perusal of section 66 is that the ambit and scope of section 66 of the amended Information Technology Act, 2000, has been expanded even beyond the scope of the earlier section 66. As such, from a mere provision on hacking, section 66 is now addressing various computer-related offences. It is pertinent to point out, that Legislature has already defined various activities which tantamount to misuse of computers, computer systems and computer networks under section 43 of the amended Information Technology Act, 2000, on the basis of which damages by way of compensation can be awarded.

Section 66 stipulates that if, any person dishonestly or fraudulently commits any act referred from section 43(a) to 43(j) of the amended Information Technology Act, 2000, the same has been declared as an offence. The said offence is 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.

For the purposes of understanding the scope, ambit and applicability of the relevant clauses of section 43 of the amended Information Technology Act, 2000, it is relevant to reproduce hereinbelow section 43 of the amended Information Technology Act, 2000, which is as follow:

Section 43 - Penalty and Compensation for damage to computer, computer system, etc.

"If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network—

(a) accesses or secures access to such computer, computer system or computer network or computer resource

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

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

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

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

(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,

(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,

(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

(j) Steals, 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,

he shall be liable to pay damages by way of compensation to the person so affected.

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 Database" 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 or 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."

For the detailed commentary on the ten grounds elaborated under section 43 of the amended Information Technology Act, 2000, kindly refer to the commentary under section 43 of the amended Information Technology Act, 2000 in this Book.

It is pertinent to point out that the said activities and acts, as detailed from section 43(a) to 43(j) committed *per se* themselves, do not become offences. The acts done as detailed under section 43 only continue to be grounds for seeking damages by way of compensation. It is only when the said acts, are done, dishonestly or fraudulently, does the said acts transform themselves into various crimes, as detailed under section 66 of the amended Information Technology Act, 2000.

It is pertinent to point out that the *Explanation* to section 66 of the amended Information Technology Act, 2000 explains that the words "dishonestly" and "fraudulently" shall have the same meanings assigned to them under section 24 and 25 of the Indian Penal Code, respectively.

Section 24 of the Indian Penal Code provides the legal definition of the term "dishonestly".

Section 24 of the Indian Penal Code provides as follows:

"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 24 stipulates that if any person does anything with the intention of causing wrongful gain to another person or wrongful loss to another person, that person does, the said thing dishonestly. The entire definition of the term "dishonestly" is dependent upon causing wrongful gain or wrongful loss to another. It is pertinent to point out that section 23 of the Indian Penal Code, defines the terms "wrongful loss" and "wrongful gain" in the following manner:

Section 23:

"Wrongful gain" is gain by unlawful means of property which the person gaining is not legally entitled.

"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.

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".

In "*Kishan Kumar* v. *Union of India*"[2], the Supreme Court held that, the expression

"wrongful gain includes wrongful retention and wrongful loss includes being kept out of the property as well as being wrongfully deprived of property".

The judiciary has over the years evolved detailed case-law on the concept of "Dishonestly".

In "*Abdul Fazal Siddiqui* v. *Fatehchand Hirawat*",[3] the Hon'ble Supreme Court reiterated the, definitions of "dishonestly" and "fraudulently" as detailed in sections 24 and 25 of the Indian Penal Code respectively.

In "*B. Suresh Yadav* v. *Sharifa Bee,*[4]", the Hon'ble Supreme Court held that regarding the expression "dishonestly" as contained in section 24 thereof in terms whereof something must be done with an intention of causing wrongful gain to one person or wrongful loss to another.

In "*Charanjit Singh Chadha* v. *Sudhir Mehra,*[5]", the Hon'ble Supreme Court held that the element of 'dishonest intention' which is an essential element to constitute the offence of theft, cannot be attributed to a person exercising his right under an agreement entered into between the parties as he may not have an intention of causing wrongful gain or to cause wrongful loss to the hirer.

In "*R.R. Diwakar* v. *V.B. Guttal,*"[6] the Hon'ble Karnataka High Court held that, the word dishonestly is defined by section 24 of Penal Code. A person who 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'

In "*Raju Jha* v. *Emperor,*"[7] the Hon'ble Patna High Court held that, the section does not say that the word "dishonestly" is applicable only when there is an intention of causing wrongful loss to another person but properly construed means that cases of intention of causing such wrongful gain to one person or wrongful loss to another person but properly coming with wider class of dishonest actions.

It is pertinent to note to that the *Explanation* to section 66 of the amended Information Technology Act, 2000 stipulates that the term "fraudulently" for the purposes of section 66 of the amended Information Technology Act, 2000 shall have the meanings assigned to it under section 25 of Indian Penal Code.

Section 25 of the Indian Penal Code gives the legal definition of the term "fraudulently". Section 25 of the Indian Penal Code provides as follows:—

"A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise."

---

2. AIR 1959 SC 1390: (1960) 1 SCR 452: 1959 Cr LJ 1508.
3. (1996) 6 SCC 32.
4. 2007 AIR SCW 6592: AIR 2008 SC 210: 2008 Cr LJ 431.
5. 2001 AIR SCW 3487: AIR 2001 SC 3721: 2001 Cr LJ 4255.
6. 1975 Cr LJ 90: (1974) 1 Kant LJ 323: ILR 1975 Kant 102.
7. AIR 1943 Pat 60 (63).

As per the provisions of section 25, if a person does a particular thing with intention to defraud but not otherwise, that person is set to do a thing fraudulently. The foundation of the legal definition of the term "fraudulently" is dependent on the phrase "intend to fraud".

It is important to note that the terms "fraud" and 'defraud" are not defined in the Indian Penal Code. The word "defraud" is of double meaning in the sense that it either may or may not, imply deprivation, and as it is not defined, its meaning must be sought by consideration of the context in which the word "fraudulently" is found.[8]

Over the years the Judiciary has evolved distinctive case law on the aforesaid words.

In "*S.P. Chengalvaraya Naidu* v. *Jagannath*"[9] the Hon'ble Supreme Court held in the context of, non-disclosure of relevant material and material documents in the court in a partition suit with a view to obtain advantage, that the word "fraud" was defined as an act of deliberate deception with a design of securing something by taking unfair advantage of another.

In "*Dr. Vimla* v. *Delhi Administration*,"[10] the Hon'ble Supreme Court held that, the expression "defraud" involves two elements, namely, deceit and injury to the person deceived. The injury may even comprise a non-economic or non-pecuniary loss. Even in those rare cases where the benefit to the deceiver does not cause corresponding loss to the deceived, the second condition is satisfied.

In "*Abdul Fazal Siddiqui* v. *Fatehchand Hirawat*,"[11] the Hon'ble Supreme Court reiterated the definition of "fraudulently" defined in section 25 of the Indian Penal Code.

Thus, a cumulative examination of section 66 of the amended Information Technology Act, 2000 entails that the acts referred to under section 43 of the amended Information Technology Act, 2000, must be done either dishonestly or fraudulently. If any of the two elements namely dishonestly or fraudulently is missing, the said acts do not become cyber crimes under section 66 of the amended Information Technology Act, 2000. Given the fact that section 66 provides for imprisonment for a term which may extend to three years, computer-related offences under section 66 of the amended Information Technology Act, 2000 are clearly bailable offences and hence, lack the teeth that the people and users of computer systems, expect the law to have. Consequently, despite the broad ambit, scope and applicability of section 66 of the amended Information Technology Act, 2000, the said provision belies the expectations of the users and victims of computer related offences as the same does not provide adequate deterrent quantum of punishment to cyber criminals, who perpetuate various kinds of computer-related offences.

8. *Abas Ali*, supra.
9. JT 1993 (6) SC 331: (1994) 1 SCC 1: AIR 1994 SC 853.
10. AIR 1963 SC 1572: (1963) 33 Com Cas 279: (1963) 2 Cr LJ 484.
11. (1996) 6 SCC 32.

Section 66A – Punishment for Sending Offensive Messages through Communication Service, etc.

"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 makes 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 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."*

The Information Technology Act, 2000 has been amended to incorporate a new provision, being section 66A. This section provides for the offence of sending offensive messages through communication devices or computer resources. However, people utilize computers, computer systems, computer networks, computer resources and communication devices for a variety of purposes for expressing their opinions, frustrations, emotions, thought processes, perspectives and views.

Lot of times, the said expressions may not be in compliance with the requirements of public decency, morality or other standards existing in the contemporary society at the relevant time. This misuse of computers and communication devices have resulted in targeting of individuals and therefore, causing a lot of anguish, harassment, anxiety to the victims. Earlier, the law did not have teeth, with regard to misuse of computers and communication devices. However, the Information Technology Act, 2000 has now been amended to incorporate section 66A. Section 66A applies to any information that is sent, either by means of a computer resource or a communication device.

The Government of India has been aware of the manner in which, computers and communication devices have been continuously misused, not only for the purposes of causing harassment of the target but also generally creating lot of nuisance in that regard. Initially meant to be a means of communicating, today computers and communication devices have become a source of nuisance.

If any person uses any computers and communication devices used for communicating, sending or transmitting any text, video, audio or image, for the various activities listed under section 66A(a) to (c), he shall be guilty of an offence, which is punishable with imprisonment for a term which may extend to three years and with fine.

Any person who sends, by means of his computers and communication devices, any information that is grossly offensive or has menacing character commits an offence under section 66A of the amended Information Technology Act, 2000.

The words "grossly offensive" and "menacing character" has not yet been defined under the Information Technology Act, 2000 and the same has been left to the subjective interpretation of the law-enforcement agencies and the courts. For the reason of understanding, it is feasible to break the words and go by their dictionary meaning so that the usage of the words is clearer.

The following definitions give more clarity to the meaning of the following words:—

1. OFFENSIVE

   Violating or tending to violate or offend against; "violative of the principles of liberty"; "considered such depravity offensive against all laws of humanity"[12]

2. MENACING

   Menace - a perceived threat or danger; the act of threatening; a dangerous person; to make threats (against someone); to intimidate; to endanger someone or something; to imperil or jeopardize.[13]

Thus, any information of any nature which is transmitted using computers and communication devices, which is grossly offensive would qualify as an offence. The said information could be offensive to person's moral standards, his privacy, his standing, stature, credibility, goodwill or even position in society. Further, if any information sent using a computers and communication devices has, got a menacing character in the sense of it threatening to harm the character, personality, standing, stature of any person, it shall also be deemed to be an offence under section 66A of the amended Information Technology Act, 2000.

Today, a large number of people misuse the computers and communication devices for the purposes of sending information, which they know is false, but which they send for vested interests. These vested interests can either be for the purposes of annoying someone, or causing inconvenience, danger or obstruction to them. A large number of times, these informations are sent by computers and communication devices, with a purpose to insult the recipient, as also to cause injury and criminal intimidation to the concerned person. It is amazing how computers and communication devices can be used to intimidate people and to bring them into submission. Further, if any person uses a computer and communication device and sends information, which he knows to be false which is sent for the purposes of causing enmity, hatred or ill-will and the said acts are normally done persistently, by making use of the concerned computers and communication devices, then those activities also come within the ambit of the offence defined under section 66A(b) of the amended Information Technology

12. wordnetweb.princeton.edu/perl/webwn
13. en.wiktionary.org/wiki/menace

Act, 2000. The said offence will also be punishable with three years' imprisonment and fine.

A lot of people use computers and communication devices for the purposes of accessing the internet as also sending, receiving, transmitting and forwarding e-mails and electronic mail messages. The law has today made it illegal for any person to send, by means of using computers and communication devices, any e-mail or electronic mail messages for the purposes of causing annoyance or inconvenience to the recipient. Such acts have been brought within the ambit of criminal penalty. In that sense, cyber stalking using electronic mail messages through computers and communication devices, has been sought to be specifically covered by the provisions of the amended section 66A of the Information Technology Act, 2000. Further, if any person sends, by means of computers and communication devices, any electronic mail or electronic mail message to mislead the addressee or recipient about the origin of such message, that is also deemed to be an offence punishable with three years imprisonment and fine.

It is important to note that section 66A(c) tries to cover slightly the phenomenon of spam. However, the entire issue of spam, cannot be effectively tackled only with just having one provision in place. This is all though more so, because the said provision only makes the said offence as a bailable offence. This provision lacks effective teeth and is a mere paper tiger provision. India has not come up with any dedicated anti-cyber spam legislation in this regard. However, limited level of protection has been sought to be given under section 66A of the amended Information Technology Act, 2000.

It is important to point out that the *Explanation* to section 66A of the amended Information Technology Act, 2000 defines the terms "electronic mail" and "electronic mail messages". These terms are defined to mean a message or information created, transmitted, or received on computers, computer systems, computer networks, computer resources and communication devices. This definition is very wide and includes all attachments in text, image, audio, video or other electronic record, which may be transmitted with a message. This definition of the terms "electronic mail" and "electronic mail message" is indeed very broad and comprehensive and is likely to be used, in the cases of misuse of computers and communication devices by victims, as also the law-enforcement agencies. However, since section 66A is only a bailable offence, it still does not put much deterrence in the minds of potential cyber criminals.

All computers and communication devices users in India need to be aware of three broad categories of activities which have been declared as criminal act. Broadly three kinds of activities have been brought within the ambit of criminal penalty under the new amended section 66A of the amended Information Technology Act, 2000. If any person sends by means of a computer resource or communication device, any information that is grossly offensive or has menacing character, then the same is an offence under the amended section 66A. This is a very broad section as it includes not just information sent through computers, computer systems, computer networks and computer resources but also all kinds of communication devices. Thus, if any person sends information to any computer

or communication device which is grossly offensive and has menacing character, he is exposed to potential punishment with imprisonment for a term which may extend to three years and with fine.

It also needs to be appreciated that what is offensive and menacing has to be understood in the context of the relevant society of India at the relevant time. Thus, something, which may not be offensive a decade ago or earlier, could now be deemed to be offensive. Thus, the Legislature has given the discretion to the law enforcement agencies and the court shall decide as to what is offensive or grossly offensive or has menacing character. Thus, when people use their computers or mobile phones for the purposes of threatening a person by e-mail or SMS or MMS, they need to be now careful as the said activities have been brought within the ambit of criminal penalty.

In case, sexually explicit content is sent by computers and communication devices to recipients on their computers and communication devices, the same could also be deemed to be grossly offensive and having menacing character. Everything will depend upon the facts and circumstances of each case and each case has to be tested on the strength of merits of the facts stated therein.

Further, if any person sends by means of a computer resource or communication device any information which he knows to be false but which is sent for the purposes of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will persistently by making use of such computer resource or communication device, the same will also be deemed to be an offence punishable under section 66A of the amended Information Technology Act, 2000 with the term which may extend to three years and with fine. Thus, offences like cyber stalking, cyber nuisance, cyber harassment and cyber defamation are all brought within the ambit of section 66A of the amended Information Technology Act, 2000. However, the beauty of new section 66A is that it also incorporates within its ambit all the aforesaid activities done using mobile phones, cell phones, smart phones, blackberries and personal digital assistants. Thus, spreading malicious defamation campaigns using computers and communication devices is specifically covered within the ambit of section 66A. Further, sending threatening information by e-mail or SMS would also be covered within the ambit of the said provision. Cyber nuisance, Cyber harassment and other related offences would be now covered within the ambit of section 66 of Information Technology Act, 2000. However, for this section to be applicable it is necessary to prove the persistent usage of a computer resource or communication device to do the aforesaid acts. The said acts must be done persistently by making use of such computer resource or communication device.

Another third category of activities brought within the ambit of criminal liability are when a person sends by means of a computer resource or communication device, any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages. If the aforesaid activities are done, the same are also punishable with imprisonment for a term which may extend to three years and also with fine. This is possibly a very wide section and

incorporates therein almost a variety of offences. The Legislature intended to target in a limitted manner computer, spam by enacting the said section. This is so because, spam or unsolicited commercial e-mail are electronic mail messages which are sent either to create annoyance or inconvenience or to deceive or to mislead the addressee or the recipient about the origin of such messages. To some extent, the said section could also incorporate therein the phenomenon of the newly emerging mobile spam.

To some extent, this provision would also cover elements pertaining to spam. However, when one examines in detail the said provision, one realizes that the said provision is not at all adequate to deal with the menace of spam, whether on computers or communication devices. This is so because, spammers today take extraordinary care and precaution to ensure that their steps cannot be traced and that they cannot be identified. Thus, in a majority of cases, the identity of spammers itself cannot be known since they are using a number of proxy servers and other devices and technologies so as to hide their real identities. Further, they deliberately create landmines on the way so that the law enforcement agencies cannot track up their spam related activities to them. Since, that is the accepted norm of the day, section 66A(c) does not provide an effective legal remedy in the practical terms. This is so because, in a number of cases, it is impossible to find out the real identity of the spammer.

Further, it needs to be appreciated that spam is such a complicated subject that it cannot be addressed very simplistic by section 66A(c). Countries across the world have applied their collective wisdom and have come to the conclusion that spam needs to be distinctly regulated by detailed legislations. That is why different countries have had different legislations aimed dedicatedly at spam. These spam related legislations include the CAN Spam Act of the United States of America, Anti-Spam Law of Australia and the Anti-Spam Law of New Zealand of 2007.

Cleary, even in those countries, despite having these comprehensive legal provisions in the form of special dedicated legislations and statutes to spam, spam has still not yet been brought fully within the blanket of regulation. India cannot afford to achieve much by a singular provision being section 66A(c) which in any case has very limited applicability. To that extent, one does realize that Indian Legislature has failed the expectations of the nation in this regard. Today, India has emerged as one of the top originators of spam across the world. This has happened primarily because of the absence of regulation in this regard. Even, when the Government of India legislated the amended Information Technology Act, 2000, it still has not given any detailed provisions relating to spam. India has missed a tremendous opportunity to regulate spam by providing for specific detailed legal provisions in this regard. Because of the severe limitations of section 66A which presupposes the identity of the spammer being known, even instances pertaining to mobile spam are not likely to be effectively covered under the new legislation.

While section 66A has made some advancement, it still does not provide any effective remedy in the event of spam emerging from unknown destinations. India has lost the window of opportunity in legislating a detailed legal regime to

regulate spam and this is likely to be further assisting spammers who can continue to go ahead and indulge in spamming activities, without any fear of law or any deterrent effect upon them.

Thus, now e-mail does not need to be only sent by a computer system or laptop. It can even be sent by a blackberry, smart phone, personal digital assistants and all the activities pertaining to same are also now brought within the ambit of the legality, as stipulated under the amended Information Technology Act, 2000. It is expected that with the passage of time, more and more people are likely to adopt the usage of mobile technologies as well as mobile devices. That being so, increasingly people would use computers and communication devices for accessing their electronic records as also electronic mail messages. The propensity to commit the crime using these digital communication devices are likely to increase with the passage of time. Section 66A is expected to be applicable to all such activities using any computers, mobile devices or communication devices pertaining to electronic mail messages.

Section 66B – Punishment for Dishonestly Receiving Stolen Computer Resource or Communication Device

"Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both."

In today's world, people are using computers and communication devices as a disposable item. Once computer or communication device is used for a long period of time, it is either disposed off or just thrown in the wastepaper basket. However, because of the propensity to use such computers and mobiles very frequently a lot of cases have arisen pertaining to theft of computers and communication devices. Traditionally, a computer or communication device is a movable property and the theft of computer or communication device is covered within the standard offence of theft defined under section 379 of the Indian Penal Code. However, Legislature also required that people should be further deterred from retaining stolen computers and communication devices.

Therefore, the Parliament has introduced section 66B of the amended Information Technology Act, 2000. Section 66B clearly makes dishonest receiving or retaining of any stolen computers and communication devices knowing or having the reason to believe that same to be stolen computers and communication devices, as a punishable offence. This offence is punishable with imprisonment of either description for a term, which may extend to 3 years or fine, which may extend to rupees one lakh or with both. This is a bailable offence, by virtue of the provisions of the amended Information Technology Act, 2000. This provision is also particularly helpful for all corporate and legal entities, who give computers and communication devices to their employees for the purposes of efficiently and effectively performing their day to day official functions and operations These computers and communication devices have a large amount of confidential data and information belonging to the concerned companies. However, rogue

employees often resign without giving notice and often do not return back these communication devices. Such kind of scenarios will also be covered within the ambit of section 66A of the amended Information Technology Act, 2000. Further, specifically the act of dishonest receiving and retention of stolen computer resource or communication devices either with the knowledge that the same is stolen or having reason to believe the same to be stolen, has thus now been brought within the ambit of the criminal penalty. This provision is likely to provide effective remedy to people, whose computers and communication devices often get stolen by different persons and who further continue to retain, use or sell the same, to the detriment of the original owner of the computers and communication devices. Such an exercise is now brought specifically within the ambit of section 66B of the amended Information Technology Act, 2000.

Section 66C – Punishment for Identity Theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh."

Today, identity theft has emerged as major headache for nations, especially in the western world. "Identity Theft", in common man's parlance, means the phenomenon of stealing another person's identity.

Wikipedia states that Identity theft is a form of fraud in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. The victim of identity theft (here meaning the person whose identity has been assumed by the identity thief) can suffer adverse consequences if he or she is held accountable for the perpetrator's actions. Organizations and individuals who are duped or defrauded by the identity thief can also suffer adverse consequences and losses, and to that extent are also victims. The term identity theft was coined in 1964 and is actually a misnomer, since it is not literally possible to steal an identity as such - more accurate terms would be identity fraud or impersonation or identity cloning but identity theft has become commonplace.

Section 66C has provided for the offence of identity theft. The said provision has been drafted in very generic and broad terms and incorporates therein the fraudulent or dishonest making use of the digital signature, password or any other unique identification feature of any person. While, the said provision has not specifically mentioned communication devices therein yet the said provision is equally applicable in the context of communication devices. Today, therein a large number of computers and communication devices use passwords for accessing the same. In case a person comes to know about a password of another and then misuses it on the computers and communication devices of other person, such an act would also come within the ambit of the section 66C of the amended Information Technology Act, 2000.

Further, if any person fraudulently or dishonestly, makes use of any other unique identification feature of any person on any computers and communication devices, that act is also brought within the ambit of criminal penalty. Such an act

is punishable under section 66C of the amended Information Technology Act, 2000.

It is pertinent to point out that section 66 C does not give the definition of the term unique identification feature. Further, section 2 of the amended Information Technology Act, 2000 also does not give the definition of the term "unique identification feature".

Let us examine the individual definition of the term in the phrase "unique identification feature"

Illustrated Oxford Dictionary defines *"Unique as unequalled; having no like, equal or parallel".*

The said Dictionary defines *"identification as the act or an instance of identifying."*

Illustrated Oxford Dictionary defines *"features as a distinctive or characteristic part of the thing"*

However, it is important to note that the words any other "unique identification feature" are very vast, comprehensive and futuristic in their approach and perspective. Thus, even though technology may change and continuously evolve, any unique identification feature of any person in any new technology could also come within the ambit of section 66C of the amended Information Technology Act, 2000. The said section makes the offence punishable with imprisonment of either description for a term, which may extend to 3 years and shall also be liable to fine, which may extend to rupees one lakh.

While, the Legislature has to be complimented for introducing section 66C, which has dealt with the offence of identity theft for the first time and has made it the basis for criminal punishment and fine, yet the disappointing feature is that the said section is only a bailable offence. The said offence is a bailable offence where the accused, even if arrested, would be entitled to bail as a matter of right. Such bailability of the offence of identity theft clearly makes the said provision a paper tiger provision and does not provide an effective deterrent effect on, people not to indulge in identity theft. Further, such a provision also fails to give effective remedy to victims of identity theft, perpetuated through any ambit or usage of technology. In that sense, the addition of section 66C is two steps forward and one-step backward. The law needs to be made far more stringent in terms of its deterrent effect and in terms of it providing effective remedies to victims of identity theft.

Section 66D – Punishment for Cheating by Personation by Using Computer Resource

"Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees."

Another major advancement done by the amended Information Technology Act, 2000 is providing for the offence under section 66D therein. The said section provides for the offence of cheating by personation by using computer resource or communication device.

It is pertinent to point out that the offence of cheating by personation is defined under section 416 of the Indian Penal Code (45 of 1860).

Section 416 of Indian Penal Code reads as under:—

"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."

The punishment for cheating by personation is given under section 419 of the Indian Penal Code (45 of 1860). In the following terms:-

"Section 419. Punishment for cheating by personation

Whoever cheats by personation shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both."

The main essential ingredients of the offence of cheating by personation is when a person cheats by pretending to be some other person. The essential ingredients of section 416 are that a person is said to cheat by personation if he cheats:

(a) by pretending to be some other person, or

(b) by knowingly substituting one person from another person, or

(c) representing that he is a person other than he really is, or

(d) representing that any other person is a person other than such other person really is.

The *explanation* to section 416 clearly provides that the offence of cheating by personation is committed whether the individual personated is a real or imaginary person.

It is pertinent to now refer to the *Illustrations* given under section 416 Indian Penal Code which are as detailed below:

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.

Having now examined the concept of the offence of cheating by personation, we have noted that in today's world people are increasingly resorting to cheating by personation using technology and technology tools. Such cheating by personation is done by computers, computer systems, computer networks and computer resources. Further, such cheating by personation is also done by people using the computers and communication devices. The Legislature has now provided for section 66D which has stipulated that cheating by personation, by means of any communication device or computer resource, is an offence punishable 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. Thus, if any person cheats by pretending to be some other person, by using a

computer, computer system, computer network, communication device or computer resource, he is deemed to have committed the offence under section 66D of the amended Information Technology Act, 2000.

Further, if a person cheats by pretending to be another person, who is already deceased, by using any communication devices or computers, or computer systems, computer networks, or computer resources, he is also deemed to have committed the offence under section 66D of the amended Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act, 2008.

Section 66D assumes significance as it incorporates all instances of cheating by personation, by using computers and communication devices. Further, cheating done by personation by using computer resources including computers, computer systems, and computer networks as also data and information resident therein are also brought within the ambit of criminal penalty under section 66D of the amended Information Technology Act, .

Section 66D is likely to now be utilized on a far wider scale since people are misusing the computer resources and communication devices and are indulging in cheating by personation using computer resources and mobile devices. However since the said section provides only for a bailable offence, the deterrent effect of the offence is missing.

Section 66E – Punishment for Violation of Privacy

"Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation.—*For the purposes of this section—*

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

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

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

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

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that—

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

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

The Legislature has sought to protect the privacy of individuals in the electronic ecosystem. Section 66E has been added to provide for the offence of violation of privacy.

The essential ingredients of section 66E is that a person has to intentionally or knowingly capture, publish or transmit the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person.

It is important to point out that the following essential acts need to be performed:

(a) Capturing

(b) Publishing, or

(c) Transmitting.

All the said three acts need to be done either intentionally or knowingly.

All these three acts must relate to the image of a private area of any person.

It is pertinent to point out that word "transmit" has been defined by the *Explanation* (a) to mean to electronically send a visual image with the intent that it be viewed by a person or persons. This incorporates, within its ambit, transmission done using computers, computer networks, computer systems, computer resources as well as transmission done using the communication devices. This is so because transmission is done by computer resources and communication devices by electronically sending the concerned images over computer networks.

Further, the word "capture" has been explained by *Explanation* to section 66E with respect to any image to mean a video tape, photograph, film or records by any means. It is today the given norm to capture images using computers and communication devices. Hence, misuse of computers and communication devices for the purpose of violating a person's privacy is on the rise.

It is further pertinent to note that *Explanation* to section 66E defines the term "private area" to mean the naked or undergarment clad genitals, pubic area, buttocks or female breast. Thus, the law has only taken a very small restrictive definition of the term "private area of any person" to mean the aforesaid. Further, it is imperative that the said capturing, publishing or transmitting the image of a private area of any person has to be, without his or her consent. Further, it is essential that the said acts must be done under circumstances violating the privacy of that person. Explanation (e) to section 66E provides as under:

"(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."

The said *Explanation* states that "under circumstances violating privacy" refers to the reasonable expectation of a person of the circumstances within which he or she could disrobe in privacy, without ever being concerned that an image of his/her private area was being captured. Further, the said term also includes therein circumstances where a person could have a reasonable expectation that any part

of his or her private area would not be visible to the public. This is regardless or whether, the said person is in a public or private place. The said provision is indeed broad to cover all aspects pertaining to the female and male organs. This provision also extremely relevant, given the huge number of MMS controversies that have happened in India, beginning with the reporting of the famous DPS MMS case or Baazee.com case. In this case, mobile phone was used for the purposes of creating or publishing an MMS wherein oral sex was being administered by a school girl to a school boy.

Thus, if any person now makes an MMS, of any person regarding his private areas under circumstances violating his or her privacy, such an act is an offence punishable with imprisonment which may extend to three years or with fine which may extend to two lakh rupees or with both. This provision would also aim to act as a deterrent against the peeping toms, spy-cameras and web cameras which are installed without permission of concerned persons, so as to invade their privacy. Such an act would now be brought within the ambit of criminal penalty and would be punished under section 66E of the amended Information Technology Act, 2000.

While, the said advancement is indeed appreciable, it is indeed also disappointing to see that the law has itself not made much progress in the direction of protecting and preserving privacy. The concept of privacy is a very large, ever expanding concept. It does not just include the private areas of persons. People have a reasonable expectation of privacy pertaining to their persons as also relating to data privacy. Unfortunately, the law has not touched anything on the concept of data privacy. Further, such provision only takes a very restrictive narrow interpretation of the concept of privacy.

There is a need to amend the Indian Information Technology Act, 2000, to bring within its ambit, more instances of violations of data privacy of persons and legal entities using computers and communication devices. Thus, while some misuse by communication devices, which violate the privacy of others has been sought to be made criminally liable under section 66E of the amended Information Technology Act, 2000, there are still a large number of areas pertaining to violation of data privacy, which still have not been legislated upon by the amended Information Technology Act, 2000 and which require urgent, immediate and proactive attention of and action by the Government of India.

Section 66E has chosen to address certain limited aspects pertaining to individual's privacy and its violation. Over the last one decade, India has seen various instances where the privacy of individuals has been violated and the said acts have been reproduced in the digital format. A few years back, we had the Bangaru Lakshman spy camera scandal where the former chief of a political party was seen on camera accepting bribe. We also have instance where Trisha, a Tamil film actress suddenly discovered that her nude scenes showing her bathing in her bathroom was released on the Internet. This was thanks to a spy camera being installed in her bathroom. In the DPS MMS case, we also saw how the MMS making capabilities of the mobile phones had been misused to capture a girl giving oral sex to the boy, a co-student, in a prominent school in Delhi, India. We have

also seen a number of cases being reported where mobile phones with cameras, have been used, without authorization to capture the private parts as well as private moments of individuals, thereby invading the privacy of that concerned individuals.

By and large the aforesaid instances are occurring in India because of the inherent defect under the existing law of India. One of the biggest tragedies as far as the legislations in independent India is concerned, is that India does not have dedicated law to protect privacy. Possibly a need for a same never arose earlier. However, the judge-made law in India has made some advances in this regard.

The Supreme Court of India has held that the fundamental rights of life includes the right of privacy and thus if any State action contravenes the privacy of any individual, the same can be challenged in the writ jurisdiction of any relevant court. However, the biggest problem still continues to be that instances of violation of privacy of individuals by other private entities are not yet brought within the ambit of specific legislation. Further, in India, the concept of data privacy does not exist. To a large extent, the historical reasons in India are responsible for this. This is so because India has emerged out of the joint family set up. As such, children from the very beginning were encouraged to share their information and as such the concept of private space for individuals did not exist. Consequently, it was but natural to expect that there would be no dedicated legislation to protect privacy in India. However, with video voyeurism becoming more and more popular, the Government of India decided to enact a special provision being section 66E of the amended Information Technology Act, 2000.

It is important to note that the term "privacy" has still not been defined under the amended Information Technology Act, 2000. It is important to now consider the various judicial pronouncements by the Supreme Court on the subject of privacy:

In *R. Rajagopal* v. *State of Tamil Nadu*,[14] the Supreme Court held as follows:—

> *"The right of privacy to be implicit in the right to life and liberty guaranteed to the citizens of India by article 21. "It is the right to be let alone". Every citizen has a right to safeguard the privacy of his own."*

In *Sunkara Satyanarayana* v. *State of Andhra Pradesh, Home*,[15] the Andhra Pradesh High Court held as follows:

> *"The right to privacy as an independent and distinctive concept originated in the field to Tort Law, under which a new cause of action for damages resulting from unlawful (invasion) of privacy was recognised. This right has two aspects which are but two faces of the same coin: (1) the General Law of privacy which affords a tort action for damages resulting from an unlawful invasion of privacy and (2) the constitutional recognition given to the right to privacy which protects personal privacy against unlawful governmental invasion. The first aspect of this right must be said to have been violated where, for example, a person's name or likeness is used,*

14. JT 1994 (6) SC 514: AIR 1995 SC 264: 1994 AIR SCW 4420.
15. 2000 (1) Ald (Cri) 117: 2000 Cr LJ 1297: 1999 (6) Andh LT 249.

without his consent, for advertising or non-advertising purposes or for that matter, his life-story is written-whether laudatory or otherwise-and published without his consent as explained hereinafter. In recent times, however, this right has acquired a constitutional status."

44. Therefore, right to privacy though not an enumerated fundamental right, is constitutionally recognised enforceable right flowing from article 21 of the Constitution. Invasion of this right gives cause of action for tortious liability besides right to enforce through Constitutional Courts. In this context the principle laid down by the Supreme Court in Kharak Singh's *case (supra),* Govind's *case (supra) and* Malak Singh's *case (supra) with reference to police surveillance and violation of right to privacy may be noticed.*

45. In Kharak Singh's *case (supra) the Supreme Court held that unless specifically authorized by law, it is constitutionally impermissible to invade the privacy of an individual violating article 21 of the Constitution. The Supreme Court held as follows:*

"The position therefore is that if the action of the police which is the arm of Executive State is found to have infringed any of the freedoms guaranteed to the petitioner, the petitioner would be entitled to the relief of mandamus *which he seeks to restrain the State from taking action under the regulations."*

In *Directorate of Revenue* v. *Mohammed Nisar Holia,*[16] the Supreme Court held as follows:

"An authority cannot be given an untrammeled power to infringe the right of privacy of any person. Even if a statute confers such power upon an authority to make search and seizure of a person at all hours and at all places, the same may be held to be ultra vires *unless the restrictions imposed are reasonable ones."*

In *Kharak Singh* v. *State of Uttar Pradesh,*[17] the apex court held as follows:

"The appellant was being harassed by police under Regulation 236(b) of U.P. Police Regulation, which permits domiciliary visits at night. The Supreme Court held that the Regulation 236 is unconstitutional and violative of article 21. It concluded that the article 21 of the Constitution includes "right to privacy" as a part of the right to "protection of life and personal liberty". The Court equated 'personal liberty' with 'privacy', and observed, that "the concept of liberty in article 21 was comprehensive enough to include privacy and that a person's house, where he lives with his family is his 'castle' and that nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy".

In *People's Union for Civil Liberties (PUCL)* v. *Union of India,*[18] the Supreme Court held as follows:

"The telephone tapping by Government under section 5(2) of Telegraph Act, 1885 amounts infraction of article 21 of the Constitution of India. Right to privacy is a part of the right to "life" and "personal liberty" enshrined under article 21 of the

16. (2008) 2 SCC 370: 2007 AIR SCW 7864: (2007) 12 SCR 906.
17. AIR 1963 SC 1295.
18. (1997) 1 SCC 301: AIR 1997 SC 568: 1997 AIR SCW 113.

Constitution. The said right cannot be curtailed "except according to procedure established by law".

Govind v. *State of Madhya Pradesh,*[19] the Supreme Court laid down that *".....privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling State interest test....."*

The focus of the entire provision under discussion is upon the relevant circumstances, in which any person can have a reasonable expectation of privacy. Thus, for example, a person can have a reasonable expectation of privacy in his or her own bathroom or her own bedroom, without ever being concerned that an image of his or her private area was being captured. Further, wherever a person has a reasonable expectation that any part of his or her private area would not be visible to the public, regardless of whether that person is in the public or private place, that expectation is now sought to be protected by the provisions of the amended section 66E of the Information Technology Act, 2000 as amended.

Further, examination and analysis of the *Explanations* (a) to (e) given to section 66E of the amended Information Technology Act, 2000 clearly shows that the focus of the section is on video voyeurism.

Explanation (a) to section 66E explains the term "transmit" to mean to electronically sent visual image with the intent that it will be viewed by person or persons. All kinds of transmissions of images of the private areas of any person, would be brought within the ambit of section 66E of the amended Information Technology Act, 2000. It is pertinent to point out that *Explanation* (b) to section 66E explains the word "capture" with respect to any image to mean to videotape, photograph, film or record by any means. Thus, whether the videotaping is being done by a video camera recorder, digital recorder, cell phone with camera, or any other similar device or any other communication device, all such activities will now be covered within the ambit of the amended Information Technology Act, 2000. Thus, if any person captures a photograph or films or videos the private area of any other person, without that person's knowledge and under circumstances violating the privacy of a person, his actions come within the ambit of section 66E of the amended Information Technology Act, 2000.

It is important to now analyze as to what is the legal definition of the term "private areas". *Explanation* (c) to section 66E defines the term "private area" to mean the naked or undergarment clad genitals, pubic area, buttocks or female breast. The perusal of the said provision clearly shows that the same is primarily meant to target the private areas of individuals, both, males and females. However, particular significant are the words "undergarment clad genitals". This is one area that is likely to provide confusion as we go long. Can it be said that the model, modeling for the bikini when being recorded by another person, the said act could also be brought within the ambit of section 66E of the amended Information Technology Act, 2000? I think there will be problems in overall applicability of the aforesaid provisions of law.

19. (1975) 2 SCC 148: AIR 1975 SC 1378: 1975 Cr LJ 1111.

Further, *Explanation* (d) to section 66E defines the term "publishes" to mean the reproduction in the printed or electronic form and making it available to public. Thus, all kinds of electronic publishing are also brought within the ambit of the section 66E of the amended Information Technology Act, 2000.

It is pertinent to point out that section 66E does not specify the mode by means of which the said violation of privacy takes place. Thus, whether the said acts were done either using a computer, computer systems, computer network, computer resources as also any other form of communication device, which are used to send, receive or transmit in any form, audio, video, text or image, all have been brought within the ambit of section 66E of the Information Technology Act, 2000.

Thus, if any person uses the camera in his/her mobile phone for the purposes of violating the privacy of individual under the parameters detailed under section 66E of the amended Information Technology Act, 2000, such an act also comes within the ambit of criminal penalty as described under section 66E of the Information Technology Act, 2000. The sending of an MMS capturing the private area of any person thereby violating of his privacy under the parameters detailed under section 66E of the amended Information Technology Act, 2000, would also be now brought within the ambit of penalty and be punished with imprisonment for a term which may extend to three years or with fine which may extend to two lakh rupees or with both. Thus, it is expected that instances pertaining to video voyeurism, especially mobile video voyeurism, are likely to be specifically covered within the ambit of section 66E of the amended Information Technology Act, 2000.

Section 66F – Punishment for Cyber Terrorism

"(1) Whoever,—

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding 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 access to information, data or computer database that is restricted for reasons for 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."

The offence of cyber terrorism was introduced for the first time in the history of independent India in the form of an amendment to the Information Technology Act, 2000. India, for the last few years, has been seeing the tremendous increase in the amount of activities that tantamount to terrorism. India has also discovered, on the way, that terrorists are extremely technology savvy and are invariably a couple of steps ahead of the law enforcement agencies. Further, the advent of the Internet and new tools including tools for encryption, data masking, proxy server hopping and other related tools, have made sure that terrorists are indeed using cyber space in a big way. That is the reason, why in repeated terrorist attacks in India, there was increasingly more and more evidence that was being discovered of tremendous reliance on technology by terrorists. That is the reason, why the Government of India had been thinking of amending the law to put up a provision for cyber terrorism.

The author himself testified before the Parliamentary Standing Committee of the Indian Parliament and underlined and stressed the need for incorporating cyber terrorism as an offence under the amendments to the Information Technology Act, 2000. The catalyst in this direction happened to be the 26/11 Mumbai attacks. The Mumbai attacks left no doubt in anybody's mind that cyber terrorism was here to stay and unless the same is handled by a strong hand, it is likely to go out of control and impact India prejudicially as time passes by. Therefore, the new offence of cyber terrorism was incorporated under the amended Information Technology Act, 2000.

This provision is incorporated under section 66F of the amended Information Technology Act, 2000. A perusal of the entire section clearly shows that it is talking about computer resources as also data, information and computer databases.

The term "computer" has been defined in a very vast term under section 2(1)(i) as under:—

"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."

A perusal of the said definition clearly shows that this is vast enough to include any kind of high-speed data processing device or system which performs logical, arithmetic and memory functions, by manipulations of electric, magnetic or optical impulses and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to a computer in a computer system or computer network. The said definition is so vast so as to specifically include all communication devices as well.

A broad analysis of the offence of cyber terrorism defined under section 66F(1) shows that it is broadly classified into two major categories of activities. The first thing that strikes any person about the said definition is the huge, comprehensive and extremely wide ambit, scope, applicability and nature as also character of the offence of cyber terrorism. It is possibly been defined in the widest possible terms as known across the world and to that extent, the Indian Legislature needs to be duly complemented for its thought leadership in this direction. The first major category of activities covered by cyber terrorism would include the following essential ingredients:

A person must have an intention to threaten the following:

- The unity of India
- Integrity of India
- Security of India
- Sovereignty of India
- To strike terror in the people
- To strike terror in any section of the people

The aforesaid intention must be followed by doing the following acts:

- Denying or causing the denial of access to any person authorised to access computer resource; or
- Attempting to penetrate or access a computer resource without authorization or exceeding authorised access; or
- Introducing or causing to be introduced any computer contaminant.
- Thereafter by means of such conduct;
- The person either causes or is likely to cause death or injuries to persons or;
- The person concerned causes damage to or the destruction of property or;
- The said person disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community, or;
- It adversely affects the critical information infrastructure specified under section 70 of the Information Technology Act, 2000.

By doing the aforesaid acts, the person commits the offence of cyber terrorism.

A broad analysis of the aforesaid section would therefore show that there has to be an intention to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people.

The second essential ingredient is that there must be a cogent act of either denying or causing the denial of access to any person authorised to access the computer resource or attempting to penetrate or access a computer resource without authorization cr exceeding unauthorised access or introducing or causing to be introduced any computer contaminant.

The third essential element is that the aforesaid intention and acts must either cause or are likely to cause death or injuries to persons. Further, the said acts must either cause damage or destruction of property or disruption of the same or disruption of supplies essential to the life of the community or either result in the adversely affecting the critical information infrastructure specified under the Information Technology Act, 2000. The net result is that any act, which has got any connection, association, nexus or relationship with terror, is covered under this section. Thus, a perusal of the said section would show that this is the widest possible characterization of the offence of cyber terrorism. However, a perusal of section 66F shows that this is only the first sub-set of the offence of cyber terrorism.

We now proceed to examine the second category of activities which are classified as cyber terrorism. The second set of activities postulate that any person must knowingly or intentionally penetrate or access a computer resource without authorization or exceeding authorised access. Further, by means of doing such an act the said person obtains access to information and data or computer database, that is restricted. The said restrictions can be for any of the reasons including the following:

- Security of the State,
- Foreign relations, or
- The said information could be any restricted information, data or computer database. The aforesaid acts must be done with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause an injury. The said injury could be caused to any of the following:
- Interests of sovereignty and integrity of India,
- Security of State,
- Friendly relations with foreign States,
- Public order,
- Decency,
- Morality,
- 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.

If the acts fulfil the aforesaid parameters, they also fall within the ambit of the offence of "cyber terrorism".

The said offence is indeed very broad and includes not just people who directly use computers, computer resources, data and information as also computer databases in the electronic form to cause detriment to the cause of the sovereignty and integrity of India but also all those people who assist such people in their various illegal activities aimed to strike terror in the hearts of people at large.

As per section 66F(2), has been categorically provided that whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment, which may extend to imprisonment for life.

Thus, clearly the ambit of such offence is very wide and includes within itself, all offences of cyber terrorism committed using computer resources including communication devices, and any other device which is used to communicate any text, video, audio or image. Thus, the usage of computers and communication devices for the purposes of either planning, discussing, analyzing, executing terror attacks or other terror plans itself comes within the ambit of the offence of cyber terrorism. Almost any and every technological device that terrorists use today can be brought within the ambit of a computer since the same are invariably electronic, magnetic, optical or other high-speed data processing devices or systems which perform logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses. The said addition of section 66F into the law book has clearly strengthened the hands of the law enforcement and the Indian nation at large in its fight against cyber terrorism. Apart from the applicability of existing laws pertaining to terror and terrorism, section 66F now becomes an immensely valuable weapon added in the arsenal of the nation, in its fight against cyber terrorism.

At the time of writing, the section has not been very extensively utilised. However as time passes by, it is but natural to expect that this provision is likely to be used more and more, not only in cases pertaining to committing acts of terror using computer systems and computer networks but also in the context of usage of communication devices.

Section 66F clearly represents one of the crowning glories of the amended Information Technology Act, 2000. Its relevance in the fight against terrorism in cyber space as also mobile terrorism and terrorism executed using mobile phones and devices is immense. However, what is currently required is a far more proactive and flexible interpretation of the said provision.

While India needs to be duly complemented for coming up with its detailed provisions pertaining to cyber terrorism, on a more objective analysis, one realizes that the fight against cyber terrorism by any nation cannot be won by one single provision alone. Clearly, India requires far more detailed legal provisions to assist the effective implementation and the applicability of section 66F of the amended Information Technology Act, 2000. Further, comprehensive procedures, processes and presumptions in relation to cyber terrorism need to be more elaborately detailed, whether in the Information Technology Act, 2000 or by means of secondary legislation which can help provide the platform for expeditious trial of cyber terror related cases.

Because of the application of section 81 of the amended Information Technology Act, 2000, the provisions of section 66F related to cyber terrorism shall prevail notwithstanding anything contrary contained therewith in any other law for the time being in force. The Information Technology Act, 2000 being a special legislation, its provisions pertaining to cyber terrorism prevail over anything inconsistent therewith in any other law including the existing anti-terror laws of India.

The author believes that certain presumptions need to be drawn up in cyber terrorism related cases. There is need for creating secondary legislation with regard

to practices and procedures to be followed, in the context of cyber terrorism. This is because as in the times to come, terrorism is going to shift completely to mobile and communication devices and the hands of law enforcements agencies need to be duly strengthened in their fight against cyber terrorists. The author personally believes that the sovereignty and integrity of India is paramount and no forces or terrorist groups can ever be allowed to subvert the sovereignty and integrity of India or the security of the State, friendly relations with other nations, public order, decency or morality. As time passes by, as more and more cases pertaining to cyber terrorism are likely to occur, there would be a need for distinct cyber terror courts who would need to be duly trained in this regard and who can provide far more effective expeditious platform for expeditious trial of cyber terror related cases.

Section 67 – Punishment for Publishing or Transmitting Obscene Material in Electronic Form

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

Section 67 of the Information Technology Act, 2000 represents India's legal position in respect of obscene and pornographic content on computers, computer systems, computer networks, computer resources and communication devices. This section was incorporated in the amended Information Technology Act, 2000. Initially, section 67 of the Information Technology Act, 2000 was made punishable on first conviction with imprisonment of either description for a term which may extend to 5 years and with fine which may extend to 1,00,000 INR. In the event of the second or subsequent conviction, the said offence was made punishable with imprisonment of either description for a term which may extend to 10 years and also with fine which may extend to 2,00,000 INR. This was the position that existed under section 67 of the Information Technology Act, 2000 from 17th October, 2000 till 27th October, 2009 when the amendments to the Information Technology Act, 2000 by virtue of the Information Technology (Amendment) Act, 2008 came into force.

It is pertinent to note that the Information Technology (Amendment) Act, 2008 amended the section 67 of the Information Technology Act, 2000 in terms of varying the quantum of punishment and fine. By virtue of the new amendments, the offence under section 67 which was earlier a non-bailable offence, has now been converted into a bailable offence since the quantum of punishment has been decreased. As per the new amendments, an offence under section 67 of the Information Technology Act, 2000 as amended, is punishable on first conviction with imprisonment of either description for a term which may extend to 3 years

and with fine which may extend to 5,00,000 INR and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to 5 years and also with fine which may extend to 10,00,000 INR. The net effect of the new amendments is that the quantum of punishment under section 67 has been reduced from earlier periods of 5 years and 10 years for first and second convictions, to 3 and 5 years for the said first and second conviction respectively. However, by virtue of the new amendments, the quantum of fine has been sought to be increased. On first conviction, the person could also be fined with fine which may extend to 5,00,000 INR. In the event of second or subsequent conviction, the person could also be fined with fine which may extend to 10,00,000 INR. The Information Technology (Amendment) Act, 2008 did not make any other changes in the language of the offence under section 67 of the Information Technology Act, 2000.

Further the Information Technology (Amendment) Act, 2008 has amended the title of section 67. Earlier section 67 was titled *"Publishing Of Information Which Is Obscene In The Electronic Form"*. The said title has now been replaced by virtue of the new amendments to *"Punishment For Publishing Or Transmitting Obscene Material In Electronic Form"*. Whereas the original section 67 only talked about publishing, transmitting or causing to be published in the electronic form, the relevant material, under the new amendments, the law now brings in its ambit, all acts of publishing, transmission as well as causing to be published or transmitted in the electronic form, the said content.

It is pertinent to point out that the words "causing to be transmitted" are very broad and include within their ambit all activities which would have an association, connection, nexus or relationship of any kind whatsoever pertaining to transmission of any obscene electronic content. Thus, section 67 is far more broader in its ambit, it not only covers the entire issue pertaining to transmission of obscene electronic records but also the act of causing the same to be transmitted.

It is apparent that the Information Technology Act, 2000 does not give legal definition of the term "transmission".

According to Wikipedia in telecommunications, transmission is the process of sending and propagating an analogue or digital information signal over a physical point-to-point or point-to-multipoint transmission medium, either wired, optical fiber or wireless. Transmission of a digital message, or of a digitized analog signal, is known as data transmission or digital communication. One transmission is the sending of a signal with limited duration, for example a block or packet of data, a phone call, or an e-mail.[20]

According to the freedictionary.com, transmission means (a) The act or process of transmitting (b) The fact of being transmitted. (c) Something, such as a message, that is transmitted. (d) The sending of a signal, picture, or other information from a transmitter.[21]

---

20. http://en.wikipedia.org/wiki/Transmission_(telecommunications)
21. http://www. thefreedictionary.com/transmission

According to Oxford dictionary *verb (transmits, transmitting, transmitted)[with object]* cause (something) to pass on from one person or place to another, communicate or be a medium for (an idea or emotion), broadcast or send out (an electrical signal or a radio or television programme), allow (heat, light, sound, electricity, or other energy) to pass through a medium.

Thus seen from one angle, any person who has got any connection with either publishing, transmitting or with causing to be published or transmitted obscene electronic content, comes within the ambit of the language of section 67 of the amended Information Technology Act, 2000.

Given the fact that section 67 is very broadly and widely defined, there has been a consistent criticism of section 67 of the Information Technology Act, 2000. Critics have stated that the said section only contains broad generic terms and does not specifically deal with the specific challenges in pornography including child pornography and electronic record containing sexually explicit records. Keeping that criticism in mind, the Legislature has added two new positions under the amended Information Technology Act, 2000, being section 67A and 67B. More about the said sections is discussed in the commentary of the relevant sections.

The main object behind enacting the section 67 of Information Technology Act is to prevent the publishing and transmitting the obscene contents on the internet, which create/cause or disturb the public order and morality.

It is relevant to point out that sex has always been an inspiring subject for mankind from the very beginning. This is one subject that has generated immense debate, discussion and controversy during each succeeding period of history in all civilizations of the world. The obsession for sex and its related acts have resulted in the origin of pornography. According to Webster's New World Dictionary, "pornography" means writings, pictures etc., intended primarily to arouse sexual desire.

Pornography has been a subject of contentious and controversial legal regulation in history. Lawmakers all across the world have always felt the need to curtail the exhibition, display and impact of pornographic materials, pornography and obscenity on the minds of the public at large in different societies. However, laws of different nations have adopted various methods to regulate pornography especially Child pornography.

Section 67 deals with the penal offence of publishing or transmitting of information or material, which is obscene in the electronic form. Section 67 of the Information Technology Act, 2000 is modeled on the basis of section 292 IPC. As such, before examining section 67 of the Information Technology Act, 2000, it would be prudent to examine briefly section 292 IPC.

In India, the offence of obscenity is dealt with under the Indian Penal Code. Section 292 IPC deals with the offence of obscenity.

Section 292 IPC states as follows:—

"292. (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 effects, or (where

it comprises 2 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 persons 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 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.—This section does not extend to—

(a) any book, pamphlet, paper, writing, drawing, painting, representation or figure—

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

(ii) which is kept or used bona fide for religious purposes;

(b) any representation sculptured, engraved, painted or otherwise represented on or in—

(i) any ancient monument within the meaning of the Ancient Monuments and Archaeological Sites and Remains Act, 1958, or

(ii) any temple, or on any car used for the conveyance of idols, or kept or used for any religious purpose."

Interestingly the Indian Penal Code, 1860 does not define the word "obscene" or "porn". Section 292 IPC basically states that a book, pamphlet, paper, writing, drawing, painting, representation, figure on any other object shall be deemed to be obscene if:—

1. it is lascivious, or
2. it appeals to the prurient interest, or
3. its effects, or (where it comprises 2 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 persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

Coming specifically to the Information Technology Act, section 67 of the Information Technology Act defines an offence substantially similar to section 292 IPC, the only material difference being that section 67 of the Information Technology Act has made the offence of obscenity applicable to any material in the electronic form and in the electronic world. Thus, each and every electronic information, which is obscene, would come within the rigours of section 67 of the Information Technology Act, 2000.

Section 67 uses the same tests for determining obscenity as are defined under section 292 IPC. Thus, section 67 Information Technology Act refers to

"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..."

These are the same expressions, which are used in section 292 IPC.

Neither the Information Technology Act, 2000 nor the Indian Penal Code, 1860 give any definitions of the terms "lascivious" or "prurient". The Webster's New World Dictionary defines the term "lascivious" as characterized by or expressing lust or lewdness, wanton, tending to excite lust. Similarly, the term "prurient" has been defined as having lustful ideas or desires, full of or causing lust; lascivious; lewd. It is further important to note that the Dictionary defines the term "lust" as a desire to satisfy one's sexual needs; especially strong sexual desire, excessive desire, great zest, to feel an intense desire, especially sexual desire.

Neither are there any uniform standards for determining what is lascivious or prurient nor there can be. By its very inherent nature, lust, as a feeling, differs from person to person and from situation to situation. Recognizing the same, the Hon'ble Supreme Court of India has held that the concept of obscenity differs from country to country and the same is dependant on the standards in contemporary society. The idea as to what is to be deemed to be obscene has varied from age to age, from region to region and even from person to person, depending upon the particular social conditions and there cannot be an immutable standard of moral values.[22]

Another challenge that arises for consideration is what would be the standards that are likely to be kept in mind by the authorities in determining whether any information or material in the electronic form is lascivious or appeals to the prurient interest.

For this, it would be interesting to examine the trends of judicial pronouncements made by the Supreme Court and various High Courts on various occasions to dwell more upon the ingredients of section 292 IPC.

22. *Ranjit D. Udeshi* v. *State*, (1962) 2 Cr LJ 741: ILR 1962 Bom 538: AIR 1962 Bom 268 (271).

It may be pertinent to mention that the landmark judgment that the Supreme Court delivered on section 292 IPC, on which section 67 of the Information Technology Act is based, was in the case entitled *Ranjeet Udeshi* v. *State of Maharashtra*.[23] In that judgment, the Supreme Court held as under:—

> *"The word, as the dictionaries tell us, denotes the quality of being obscene which means offensive to modesty or decency: lewd, filthy and repulsive. It cannot be denied that it is an important interest of society to suppress obscenity. There is, of course, some difference between obscenity and pornography in that the latter denotes writings, pictures, etc., intended to arouse sexual desire while the former may include writings etc. not intended to do so but which have that tendency. Both, of course, offend against public decency and morals but pornography is obscenity in a more aggravated form.*
>
> *... Condemnation of obscenity depends as much upon the morals of the people as upon the individual. It is always a question of degree or as the lawyers are accustomed to say, of where the line is to be drawn. It is, however, clear that obscenity by itself has extremely poor value in the propagation of ideas, opinions and informations of public interest or profit. When there is propagation of ideas, opinions and informations of public interest or profit, the approach to the problem may become different because then the interest of society may tilt the scales in favour of free speech and expression. It is thus that books on medical science with intimate illustrations and photographs, though in a sense immodest, are not considered to be obscene but the same illustrations and photographs collected in book from without the medical text would certainly be considered to be obscene. Section 292, Penal Code deals with obscenity in this sense and cannot thus be said to be invalid in view of the second clause of article 19."*

In this case, Justice M. Hidayatullah held that in order to determine whether any material is obscene or not, the test laid down in *Regina* v. *Hicklin*,[24] should not be discarded. The *Hicklin* case lays emphasis on the potentiality of the mentioned object or material to deprave and corrupt by immoral influences as the critical factor to determine obscenity. In 1868, in the landmark case entitled *Regina* v. *Hicklin*, the test of obscenity was defined as follows,

> *" ...the test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those, whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall..."*

The Supreme Court further held in *Ranjeet Udeshi* v. *State of Maharashtra*, that what is obscene would always remain a question to be decided in each case. However, the Apex Court advocated that it was the duty of the court to consider the alleged obscene matter by taking an overall view of the entire work. It was further held that an overall view of the obscene matter in the setting of the whole work would, of course, be necessary, but the obscene matter must be considered by itself and separately to find out whether it is so gross and its obscenity is so decided, that it is likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the book is likely to fall.

23. AIR 1965 SC 881: (1965) 1 SCWR 778 (1965) 2 Cr LJ 8.
24. 3 LR QB 360 (1868).

Further, in the case entitled *Chandrakant Kalyandas Kakodkar* v. *State of Maharashtra*,[25] the Supreme Court held that the standards of obscenity would differ from country to country depending on the standards of morals of contemporary society. *"What is considered as a piece of literature in France may be obscene in England and what is considered in both countries as not harmful to public order and morals may be obscene in our country".*

It was further held that,

> *"what we have to see is whether a class, and not an isolated case, into whose hands, the book, article or story falls suffer in their moral outlook or become depraved by reading it or might have impure and lecherous thoughts aroused in their minds. The charge of obscenity must, therefore, be judged from this aspect."*

It is the duty of the Court to consider the obscene matter by taking an overall view of the entire work and to determine whether the obscene passages are so likely to deprave and corrupt those whose minds are open to such influences and in whose hands the book is likely to fall and in doing so, one must not overlook the influence of the book on the social morality of our contemporary society.[26]

The use of the term "obscenity" is restricted to sexual immorality. The true test is thus not to find out what depraves the morals in any way whatsoever but what leads to deprave in only one way, *viz.*, by exciting sexual desires and lascivious thoughts.[27]

The question regarding "obscenity" is one of fact and depends upon various circumstances and no hard and fast rule can be laid down. It does not depend altogether on oral evidence but must be judged by the Court.[28]

The effect produced by the publication on an ordinary member of the society has to be ascertained. Such ordinary persons are expected to be of normal temperament. The standard of the reader is neither one of exceptional sensibility nor one without any sensibility whatsoever.[29]

A vulgar writing is not necessarily obscene. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the novel whereas obscenity has the tendency to deprave and corrupt those, whose minds are open to such immoral influences.[30]

If a publication has the tendency to deprave and corrupt the minds of people reading it, it is within the mischief of the section (292 IPC) though the author or the publisher has an ulterior object, which is innocent and laudable.[31]

Whether the publication is obscene or not depends upon the material itself and not upon the motive.[32]

25. (1969) 2 SCC 687: 1970 Cr LJ 1273: AIR 1970 SC 1390.
26. AIR 1970 SC 1390 (1391, 1392, 1395).
27. *Sukanta Haider* v. *State*, AIR 1952 Cal 214 (216): 1952 Cr LJ 575.
28. *Shri Chandrakant Kalyandas Kakodkar* v. *State of Maharashtra*, (1969) 2 SCC 687: 1970 Cr LJ 1273: AIR 1970 SC 1390 (1392).
29. *Ranjit D. Udeshi* v. *State*, (1962) 2 Cr LJ 741: ILR 1962 Bom 538: AIR 1962 Bom 268 (270, 271).
30. *Samaresh Bose* v. *Amal Mitra*, AIR 1986 SC 967 (983): 1986 Cr LJ 24: (1985) 4 SCC 289.
31. *C.T. Prim* v. *State*, AIR 1961 Cal 177 (180): (1961) 1 Cr LJ 371: ILR (1960) 1 Cal 867.
32. *Kailash Chandra* v. *Emperor*, 56 Cal LJ 123: Cr LJ 771: AIR 1932 Cal 651 (652, 654).

In determining whether or not a publication is obscene regard must be had to that publication alone; other books not the subject of charges cannot be considered.[33]

A picture of a woman in the nude is not *per se* obscene. For the purpose of deciding whether such picture is obscene, one has to consider to a great extent the surrounding circumstances, the pose of the posture, the suggestive element in the picture and the person or persons in whose hands it is likely to fall.[34]

The scope of the expression "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" has to be interpreted in the light of the various principles and tests laid down by the aforesaid judicial pronouncements.

The perusal of the aforesaid authorities and judicial pronouncements make it clear that the Supreme Court and various High Courts have relied more upon the element of the impact on the public at large rather than pure nudity standards. This has been a more balanced approach, as nudity *per se* cannot be said to be obscene or lascivious or prurient. If that were so, then our entire ancient cultural heritage involving nudity like Khajuraho and Kamasutra would have been made illegal. Surely this is not the case.

The next consideration that engages one's mind is whether the principles of law laid down by the different pronouncements detailed above under section 292 IPC could fairly and materially be made applicable to the offence under section 67 Information Technology Act, 2000. I am of the opinion that this indeed would be the logical approach.

However, I would like to add a note of caution to the effect that the said judicial pronouncements under section 292 IPC cannot be fully applied to section 67, Information Technology Act, 2000. This is so as the abovenoted judgments have been delivered in the context of the actual world and the specific requirements of section 292 IPC which relate to a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, in the real world. None of the aforesaid judgments have been delivered in the context of the electronic environment and the Internet.

Section 67 of the Information Technology Act has created a bit of confusion by merely copying the material phrases from section 292 IPC and by not taking into consideration the changed standards of society and human behaviour in modern India. The Indian Penal Code was enacted in 1860, at a time when India was under the colonial rule of the British and the Indian society was highly conservative.

With the passage of each succeeding decade and with our independence, standards of perceptions and morals have changed substantially. The passage of time has led to further liberalization of ideas relating to nudity and pornography. The 1990s saw the liberalization of the Indian economy, and the influx of Western

33. *Ranjit D. Udeshi* v. *State of Maharashtra*, AIR 1965 SC 881 (888, 889, 891): (1965) 1 SCWR 778: (1965) 2 Cr LJ 8.

34. *State* v. *Thakur Prasad*, AIR 1959 All 49 (52, 53): 1958 All LJ 578: 1959 Cr LJ 9.

inputs, television channels and the coming of the Internet have all radically changed perspectives relating to morals, pornography and obscenity in India.

It would have been better if the Legislature had taken the changed societal standards in consideration while enacting section 67 of the Information Technology Act. The Information Technology Act has not really defined standards to ascertain what is obscene, lascivious or prurient in the context of the electronic medium at a time when Internet is flooded with pornography. It has been left to the subjective interpretation of the relevant law-enforcement agency to define what exactly is obscene, in the context of the peculiar facts and circumstances of each case.

No doubt, the pronouncements made under section 292 IPC would act, as guiding principles for courts but the courts would be required to act proactively and interpret section 67 of IT Act, 2000 in the context of Internet, cyberspace and the electronic form. This is all the more required, especially at a time when the world at large is struggling to cope up with the challenges of controlling the menace of online pornography.

There is no doubt that pornographic and blue films and pictures are indeed lascivious in nature and they appeal to the prurient interest as well. I am of the opinion that the *Hicklin* test would still be applicable in the context of the electronic form, though the Judiciary would now be required to suitably modify and adapt the *Hicklin* test in the context of the online environment and the Internet.

Another basic concern relating to section 67, Information Technology Act, 2000 would be as to how the same would be implemented outside the territorial boundaries of India. At the time of writing, as per one estimate, more than half of the total content available on the net is pornographic. A majority of the pornographic content of the Internet has been hosted on websites, which are in turn hosted on web servers, which are outside the territorial jurisdiction of India, though available here. How would law enforcement agencies in India check the offence of online pornography emanating outside the country? Technically speaking, the Information Technology Act, 2000 states in sections 1(2) and 75 that it shall be applicable not only to the whole of India but also to any offence or violation of the provisions of this Act done by any person of any nationality anywhere in the world. This approach is clearly not practical under the norms of existing international law. No country can assume jurisdiction over the citizens of other countries. Enacting a law like the Information Technology Act with transnational jurisdiction is likely to create a lot of challenges and problems, more so in the context of regulating online obscenity and pornography.

Another point to note is the tremendous disparity of punishment between section 292 IPC and section 67 of the Information Technology Act. Under section 292 IPC, a person convicted of the offence can be punished with imprisonment upto 2 years and fine upto two thousand rupees in the first conviction and with imprisonment upto 5 years and fine upto five thousand rupees in subsequent convictions.

The quantum of punishment in section 67 of the amended Information Technology Act is higher than section 292 of Indian Penal Code. Under section 67,

Information Technology Act, a person convicted of the offence can be punished with imprisonment which may extend to 3 years and fine which may extend to 5 lakh rupees on first conviction and with imprisonment which may extend to 5 years and fine which may extend to 10 lakh rupees on second or subsequent convictions.

The only material difference that section 67 makes to the offence defined under section 292 IPC is that it has extended the same offence to the electronic format. Thus, a peculiar situation is likely to emerge in the practical working and implementation of the Information Technology Act.

For example, a person may publish a pornographic book and he is liable to be punished with imprisonment up to two years under section 292 IPC. But at the same time, if the same person publishes the pornographic book in the electronic form, then he becomes entitled to a higher imprisonment of 3 years and fine up to 5 lakh rupees under section 67, Information Technology Act, 2000.

It is important to note that publishing a pornographic book in the real world and in the electronic world is not substantially different in any way. Only the procedures are different. While in the real world, a person would get a pornographic book published by means of the printing press over actual paper, in the electronic medium, he would publish the same book by converting it into the electronic form by means of an electronic process and which may be stored in a computer, computer system, computer network or floppy, disk, CD etc.

It is equally important to note that the pornographic content of the book in question does not change, whether it is published upon paper in the actual world or whether it is published in the electronic form in a computer file. Similarly, the intention to publish the pornographic content in the form of the pornographic book does not change at all in the two instances.

It can be argued that since all things are the same in the two different scenarios of publishing in the actual world and in the electronic form, there is no rationale in giving a higher quantum of punishment for the publication in the electronic form as compared to publication in the real world. It can be further argued that the delivery mechanism of a particular process or the procedure adopted for arriving at any product has never held any importance or relevance in criminal jurisprudence of our country and moreso, in the context of granting of penal punishment. This erroneous approach by law makers in adopting penal standards for granting the quantum of punishment for the same offence under the Information Technology Act is likely to lead to immense complications and weird results. It can also be argued that not only is this approach likely to lead to miscarriage of justice but it is also likely to violate the fundamental rights granted to the citizens under Chapter III of the Constitution of India.

However, I am of the opinion that due to the inherent nature of the electronic medium and the electronic format, any information is capable of being transmitted at a far greater speed to a much larger number of people than a similar exercise in the real world with available procedures. This is so because of the very character of the electronic media and its potential capabilities of instantaneously spreading pornographic content to innumerable people.

Thus, the impact of publishing, transmitting or causing to be published or transmitted any obscene material in the electronic form, can have a far more impact on innumerable people, and as such, the Legislature has adopted a correct approach in granting an enhanced quantum of punishment for an offender under section 67 of the Information Technology Act, 2000.

Section 292 IPC uses the words "any other object". This is a very wide term and can be argued to be including any material or object in an electronic form. However, since section 67 of the Information Technology Act, 2000 specifically deals with obscene materials in the electronic form, section 292 IPC shall not be applicable in case of obscene electronic materials. It may be stated here that the Information Technology Act, 2000 is a special legislation, which overrides the inconsistent provisions of the existing legislations. Section 81 of the Information Technology Act, 2000 specifically states as under:

> *"The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force."*

Thus, this really means that section 292 IPC shall not be applicable to any material or information in the electronic form and in the context of the electronic form, the provisions of section 292 IPC shall be overridden by section 67 of the Information Technology Act, 2000.

By virtue of the Information Technology (Amendment) Act, 2008, section 67 has been made as a bailable offence. Earlier section 67 used to be a non-bailable, where the accused was only entitled to bail on the discretion and subjective satisfaction of the court. However by virtue of coming into effect of the Information Technology (Amendment) Act, 2008, section 67 has been converted into a bailable offence as the quantum of punishment is only 3 years. The quantum of fine has been increased from the earlier 1,00,000 INR to 5,00,000 INR on the first conviction and to the earlier 2,00,000 INR to 10,00,000 INR under the second conviction. However practically speaking, this move initiated by the Information Technology (Amendment) Act, 2008 is a historical mistake as it has taken the deterrence out of the offence under section 67 of the Information Technology Act, 2000. With the coming into effect of the provisions of section 67, publishing pornography or obscene electronic information or its transmission is now no longer a big thing. People tend to get a feeling that since the said offence is a bailable offence, they will get automatic bail and thereafter, a number of people are known to have gone and deleted the relevant incriminating electronic evidence that would have been incriminating them resulting into cybercrime convictions. That is the reason why the number of convictions under section 67 of the Information Technology Act, 2000 has been very scarce.

The net effect of the Information Technology (Amendment) Act, 2008 is also that it has not only broadened the ambit and scope of section 67 of the Information Technology Act, 2000 but has further broadened its applicability. Now given the fact that the Information Technology (Amendment) Act, 2008 has made the Information Technology Act, 2000 fully applicable to all communication devices, section 67 of the Information Technology Act, 2000 is applicable to all cell phones, personal digital assistants or combination of both or any other device which is

used to communicate, send or transmit any text, video, audio or image. Thus, all kinds of mobile devices, mobile platforms, cell phones and electronic information published therein which is obscene has been brought within the ambit of section 67 of the amended Information Technology Act, 2000. This suddenly has huge ramifications from the perspective of users. Today, a large number of people not only view pornography on their mobile devices, but further send SMSs or MMSs containing pornographic content. The moment a person sends pornographic SMS or MMS to any other person, he is deemed to have published, transmitted as well as caused to be published and transmitted the said obscene content. Such an act would fall within the ambit of section 67 of the Information Technology Act, 2000. Further, all kinds of pictures captured through mobile phones which are obscene in nature, further fall within the ambit of section 67 of the Information Technology Act, 2000. It is further pertinent to note that section 67 of the Information Technology Act, 2000 does not make viewing of obscene electronic information or pornography as an offence, it is only concerned with the limited acts of publishing, transmission or causing to be published or transmitted obscene electronic information.

It is further pertinent to note that the Legislature is committed to not only making publishing or transmission as well as causing to be published or transmitted obscene electronic information a crime, but it has also taken proactive steps to ensure that such content ought not to be published or transmitted. In that regard, it is pertinent to note that the Central Government notified the Information Technology (Intermediary Guidelines) Rules, 2011. This is applicable to all intermediaries as defined under section 2(1)(w) of the Information Technology Act, 2000. Thus, any legal entity which in respect of any particular electronic record, receives, stores or transmits that record on behalf of another person or provides any service with respect to that record, are bound by the said guidelines. Rule 3 of the said Information Technology (Intermediary Guidelines) Rules, 2011 mandate that these intermediaries must have in place the rules and regulations, terms and conditions and user agreement which inform the users of their computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is obscene, pornographic, pedophilic or invasive of another's privacy.

If despite the said provisions detailed in the intermediaries terms and conditions, any person still violates the same, the intermediaries are mandated on whose computer system the information is stored or hosted to exercise due diligence while discharging their obligations under the Act. Once they obtain knowledge of the said pornographic information either by themselves or such pornographic content is brought to their actual knowledge by any affected person in writing, the said intermediaries are mandated to act within 36 hours and wherever applicable to disable such information that is in contravention of the law. If the said intermediary failed to do the said exercise, they would also be seen as a co-conspirator and co-abettor of the crimes under section 67 of the Information Technology Act, 2000. As such when one reads cumulatively sections 67 and 79 of the amended Information Technology Act, 2000 as amended alongwith Information Technology (Intermediary Guidelines) Rules, 2011, it is abundantly

clear that intermediaries must exercise due diligence in the manner as stipulated under law and if they do not do so in respect of any obscene or pornographic content available on the computer resource, they could face criminal liability under section 67 of the Information Technology Act, 2000.

It is further pertinent to point out that the proviso of section 67B is also applicable in section 67 of the IT Act. Section 67 has to be read in conjunction with the proviso to section 67B of the amended Information Technology Act, 2000. This proviso provides that the provisions of section 67 do not extend to certain exempted category. The provisions of this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form, provided two conditions are fulfilled. The first condition that is required to be fulfilled is that the publication of such book, pamphlet, paper, writing, drawing, painting, representation of figure in the electronic form is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation of figure is in the interest of science, literature, art or learning or other objects of general concern.

The second condition that is required to be fulfilled is that the said book, pamphlet, paper, writing, drawing, painting, representation of figure in the electronic form is kept or used for any *bona fide*, heritage or religious purposes.

If any of the above two conditions are fulfilled, then section 67 of the amended Information Technology Act, 2000 shall not be applicable.

When one looks at the exempted categories, it is important to note that the law uses the word "as being for the public good".

The word "public good" has not been defined in the Information Technology Act, 2000. However there is ample jurisprudence with regard to what constitutes public good.

The Superintendent, Central Prison Fatehgarh v. *Dr. Ram Manohar Lohia*, AIR 1960 SC 633: (1960) 2 SCR 821, the Supreme court of India held as follows:

The expression "public order" has a very wide connotation. Order is the basic need in any organised society. It implies the orderly state of society or community in which citizens can peacefully pursue their normal activities of life.

The words "public order" were also understood in America and England as offences against public safety or public peace. The Supreme Court of America observed in Cantewell v. Connecticut *(1) thus:*

"The offence known as breach of the peace embraces a great variety of conduct destroying or menacing public order and tranquillity. It includes not only violent acts and words likely to produce violence in others. No one would have the hardihood to suggest that the principle of freedom of speech sanctions incitement to riot. When clear and present danger of riot, disorder, interference with traffic upon the public streets, or other immediate threat to public safety, peace, or order appears, the power of the State to prevent or punish is obvious."

The foregoing discussion yields the following results: (1) "Public order" is synonymous with public safety and tranquillity: it is the absence of disorder involving breaches of local significance in contradistinction to national upheavals, such as revolution, civil strife, war, affecting the security of the State.

Municipal Council, Raipur v. *State of Madhya Pradesh*, AIR 1970 SC 1923: (1970) 1 SCR 915, the Supreme court of India held as follows:

'Public Order' is an expression of wide connotation and signifies that state of tranquillity which prevails among the members of a political society as a result of internal regulations enforced by the government which they have established."

Later he observed:

"'Public safety' ordinarily means security of the public or their freedom from danger. In that sense, anything which tends to prevent danger to public health may also be regarded as securing public safety."

The learned counsel urges that "public order" includes "public safety" and the latter comprises "public health". We see no force in this contention and Ramesh Thappar's *case does not say so. In our view "Public Order" in this context means public peace and tranquillity.*

Further, it is important to note that the requirement is not only that the publication has to be justified as being in the public good but that said justification only has to be on the ground that the said book, pamphlet, paper, writing, drawing, painting, representation of figure is in the interest of science, literature, art or learning or in the topics of general concern. Thus, *e.g.*, a picture of a nude body of a female could come within the parameters of section 67 of the Information Technology Act, 2000. However, in case if the picture is published for the purposes of showing the anatomy of the female body as in the interest of science, the publication of the said picture in the electronic form may not qualify for the applicability of section 67 of the Information Technology Act, 2000.

The suggested picture of two adults having sexual intercourse may be brought within the ambit of section 67 of the Information Technology Act, 2000. However, if the said suggested picture is used in the context of giving education as to how sexual intercourse takes place between two adults or the same is in the interest of advancement of science or learning, then the same would not qualify within the parameters of section 67 of the Information Technology Act, 2000.

Further, if any person makes in the electronic form, any of the sculptures which exist in Khajuraho that could qualify under section 67 of the Information Technology Act, 2000, but in case if the said sculptures from Khajuraho are captured in the electronic form, the said electronic publication being in the interest of art would not qualify for attracting section 67 of the Information Technology Act, 2000, thanks to the proviso to section 67B of the Information Technology Act, 2000.

If two adults are captured in the electronic form performing various poses of sexual relations as depicted in Kamasutra, that publication would attract section 67 of the Information Technology Act, 2000, but in case if the said publication is done as re-creation of the Kamasutra in the exact manner and spirit as depicted in Kamasutra, the same could be deemed to be a publication for public good and in the interest of literature, art and other subject of general concern and as such, would not attract the applicability of section 67 of the Information Technology Act, 2000.

For example, if Kamasutra is reproduced in the electronic form, the said electronic book would not attract section 67 of the Information Technology Act, 2000, thanks to the proviso to section 67B. If any electronic publication is kept or used for *bona fide* heritage or religious purposes, the said electronic publication would also not qualify for attracting section 67 of the Information Technology Act, 2000.

Further if an electronic book, paper, pamphlet, drawing, painting, representation of Lord Mahavira is made, then the said electronic publication would be kept or used for *bona fide*, heritage or religious purposes and would qualify for the exemption from the applicability of section 67 of the amended Information Technology Act, 2000, thanks to the proviso to section 67B of the Information Technology Act, 2000.

At this stage, it would be relevant to refer to some of the cases which have been reported in India in the context of obscenity in the electronic medium.

Over a period of last one decade, section 67 has been invoked in various cases in India.

One of the most celebrated case under section 67 of the Information Technology Act, 2000 has been that of *State* v. *Avinish Bajaj*. This was a case where an obscene MMS known as the DPS MMS became the subject matter of controversy. A student uploaded a message on Baazee.com, an online auction portal, which is now EBay.in, offering to make available for consideration the said MMS to people. The moment Baazee.com came to know about it, it was pulled down, but by that time history had been created. Number of people downloaded the said MMS. Consequently, a case was registered under section 67 of the Information Technology Act, 2000. Avinish Bajaj applied for bail. The matter came up for hearing before the Delhi High Court, who in the case entitled *"Avinish Bajaj* v. *State of NCT of Delhi,"*116 (2005) DLT 427, it *inter alia* held as under:

"5. Mr. Jaitely, has underscored that in section 67 of the Information Technology Act, 2000 an offence is committed by a person who publishes or transmits any material which is lascivious or appeals to the prurient interest. sections 292 and 294 of the Indian Penal Code have also been mentioned which contemplate the selling, letting on hire, distribution or public exhibition of obscene matter. He has emphasized that the provision does not bring within its sweep the causing of the transmission in contradistinction to the publication of obscene material. Prima facie *it has not been established from the evidence that has been gathered till date that any publication took place by the accused, directly or indirectly. The actual obscene recording/clip cannot be viewed on the portal of Baaze.com. This question will have to be decided. It has been argued on behalf of the accused that 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.* Prima facie *Baaze.com has endeavored to plug the loophole although it is to be expected that similarly placed persons should do so with immediate alacrity. This case will indubitably bring to the fore the dangers endemic in this business, which must be addressed forthwith.*

6. It has also been shown that only 14 days J/C General had been requested for on the submission that "investigation reveal that same MMS clipping was listed for

sale on 27th November, 2004 in the name of DPS Girl having fun". It has also been contended that initially the prosecution had conceded the grant of bail, but it was subsequently argued to the contrary.

8. The accused has actively participated in the investigations, and even before me it has not been suggested to the contrary by Counsel for the State. The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof. Even though the accused is no longer an Indian National, he is of Indian origin with family roots in our country. It cannot possibly be argued that a foreign national is disentitled to the grant of bail. Reference to Ram Govind Upadhyay *v.* Sudarshan Singh *may not be relevant at this stage since the evidence that has been collected indicates only that the obscene material may have been unwittingly offered for sale on the website; and that heinous nature of the alleged crime may be attributable to some other person.*

9. The accused is enlarged on bail subject to furnishing two sureties in the sum of Rs. 1,00,000 each to the satisfaction of the concerned Court/Metropolitan Magistrate/Duty Magistrate. The accused shall also not leave the territories of India without the leave of the Court and for this purpose shall surrender his passport to the Magistrate. It is implicit in the grant of bail that he shall participate and assist in the investigation."

That further after the grant of bail, charge-sheet was filed which was sought to be quashed before the Delhi High Court. The Delhi High Court in the case entitled "*Avinish Bajaj* v. *State*" in the year 2008, held as follows:

"20.9 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.*

(c) However, as far as the petitioner Avinish 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 85 IT Act is made out against the petitioner since the law as explained by the decisions of the Supreme Court recognizes 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."

Further, it is pertinent to point out that the Hon'ble High Court found the *prima facie* case against the accused under section 67 of Information Technology Act, 2000 and ordered to continue the case under section 67 read with section 85 of IT Act. Aggrieved by this order the accused/petitioner went to the Supreme Court, the Supreme Court in the case entitled "*Avinish Bajaj* v. *State*" being Criminal Appeal No. 1483 of 2009, held as under:

46. Presently, we shall advert to the other two appeals, i.e., Criminal Appeal Nos. 1483 of 2009 and 1484 of 2009 wherein the offence is under section 67 read with section 85 of the 2000 Act. In Criminal Appeal No. 1483 of 2009, the director of the company is the appellant and in Criminal Appeal No. 1484 of 2009, the company. Both of them have called in question the legal substantiality of the same order passed by the High Court. In the said case, the High Court followed the decision in Sheoratan Agarwal *(supra) and, while dealing with the application under section 482 of the Code of Criminal Procedure at the instance of Avnish Bajaj, the Managing Director of the company, quashed the charges under sections 292 and 294 of the Indian Penal Code and directed the offences under section 67 read with section 85 of the 2000 Act to continue. It is apt to note that the learned single Judge has observed that a* prima facie *case for the offence under sections 292(2)(a) and 292(2)(b) of the Indian Penal Code is also made out against the company.*

48. Keeping in view the anatomy of the aforesaid provision, our analysis pertaining to section 141 of the Act would squarely apply to the 2000 enactment. Thus adjudged, the director could not have been held liable for the offence under section 85 of the 2000 Act. Resultantly, the Criminal Appeal No. 1483 of 2009 is allowed and the proceeding against the appellant is quashed. As far as the company is concerned, it was not arraigned as an accused. Ergo, the proceeding as initiated in the existing incarnation is not maintainable either against the company or against the director. As a logical sequeter, the appeals are allowed and the proceedings initiated against Avinish Bajaj *as well as the company in the present form are quashed.*

Further, there have been other cases which have been reported in the public media. As per reports, the court in Mapusa, Panaji sentenced a husband to undergo imprisonment for two years and also directed to pay fine of Rs. 10,000 under section 67 of the Information Technology Act, 2000. This punishment was awarded to the husband because of his sending lewd and defamatory text messages to his estranged wife on her cell phone.[35]

It is further pertinent to note that on various occasions, the Government of India has gone ahead and blocked and banned various pornographic websites including www.incometaxpune.com and savitabhabhi.com, on the ground of them being obscene.[36]

35. http://articles.timesofindia.indiatimes.com/2012-09-05/goa/33614125_1_smss-mapusa-defamatory-text-messages.
36. http://www.chmag.in/article/sep2011/law-relating-cyber-pornography-india.

Riya Sen MMS scandal broke out when she was allegedly shot in an inappropriate state along with her then beau Ashmit Patel. Riya maintained that she was not the girl in the MMS but the striking similarity and the fact that Ashmit was also there in the video raised speculation. The bubbly and confident Preity Zinta was in shock when the infamous Preity Zinta scandal rocked the media. It was almost a 5 minute clip of a woman being captured taking bath in a hotel bathroom with the camera shooting the entire scene from a peephole. Preity Zinta had personally checked the clip and found that it was not her. The Khatta Meetha star, Trisha Krishnan had an MMS controversy stuck to her immediately after she debuted in the Telugu film industry. A girl who looked similar to Trisha was shot in the bathroom in an almost 10 minute clip. The Trisha MMS was one of the most downloaded MMS and though the actress refused to comment. This is one of the most (in)famous Bollywood MMSes that circulated in the Indian media. The passionate kissing between Kareena Kapoor and Shahid Kapoor was filmed by a journalist who wrote about it in his paper. News spread like wildfire and it became the talk of the town for a week.

In the case entitled *"State of Tamil Nadu* v. *Suhas Kutty,*[37]*"*, a Chennai court sentenced a former boyfriend for online obscenity who had morphed a picture of his girlfriend on the body of a nude model and had circulated it to close friends and family. On 24-3-2004 a Charge-sheet was filed under section 67 of IT Act, 2000, 469 and 509 IPC before The Hon'ble Addl. CMM, Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C. No. 4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked.

Honourable Sri Arulraj, Additional Chief Metropolitan Magistrate, Egmore, delivered the judgment on 5-11-04 as follows:

> *"The accused is found guilty of offences under sections 469, 509 IPC and 67 of IT Act, 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under section 469 IPC and to pay fine of Rs. 500 and for the offence under section 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs. 500 and for the offence under section 67 of IT Act, 2000 to undergo RI for 2 years and to pay fine of Rs. 4000 All sentences to run concurrently."*

Arjika Case

Prior to the coming into effect of the Information Technology Act, 2000, the *Arjika* case had emerged. As reported, in this case, the police registered a case under section 292 of the Indian Penal Code after being alerted by Interpol. The crux of the case is that there was a site called *www.sweeties.arjika.com*, which was hosting child pornography material. The concerned website showed customized videos of three hours duration, where children were depicted in sexual orgies. The videos showed pictures of naked children between the ages of 6 and 15. However, all this pornographic material was camouflaged beautifully. The site on its home page featured the famous cartoon character Pokeman. On clicking the same, there was hard-core child pornographic material available on the site.

37. http://www.naavi.org/cl_editorial_04/suhas_katti_case.htm

Interpol, who has a detection wing against online child pornography, alerted the CBI who registered the case under section 292 IPC. Thereafter, CBI arrested one Arvind K Shyam Jagdam of Arjika Impex Pvt. Ltd., a Hyderabad-based computer engineer on the ground that he owned the domain, which was hosting the pedophile site. Investigations further revealed that Jagdam allegedly set up a free website with free web space to be taken by anyone in cyberspace after due registration at the site. Consequently, someone in Peru registered on this free website and created a pedophilic site under the camouflage of cartoon character Pokeman on the home page. Another interesting element of the case was that the naked children shown on the site were missing from their respective homes. It is also important to note that in this case, Jagdam had offered a free website with free web space to anyone on the Internet so long as he registered on the site. As such, Jagdam had no physical control over the contents of the website and could not be said to be the author of the contents. The authorities basically alleged Jagdam to be guilty of negligence on the ground that when he got the free space through North Sky, he had signed an agreement promising that no pornographic site would be hosted by *www.arjika.com*.

This case also raises complicated issues relating to jurisdiction, since the domain name in question is owned by an Indian, the creator of the pedophilic site is based in Peru while the server of the website is based in America. This case raises tremendously complicated issues concerning various aspects relating to online pornography.

Air Force Bal Bharati School Case

In the first case of its kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the Information Technology Act, 2000. In this case, a 16-year old boy of Air Force Bal Bharti School, a prominent school of Delhi, created a website at the URL www.amazing-gents.8m.net. The website was hosted by the schoolboy on free web space. It was dedicated to Air Force Bal Bharti School and contained text material. On this site, lucid, explicit, sexual details were given about various "sexy" girls and teachers of the school. Girls and teachers of the school were also classified under the basis of their physical attributes and perceived sexual preferences. The website was going on as a part of an adult boy's joke amongst a students' peer group.

This continued for some time till one day, the beans were spilt when one of the boys told a girl "featured" on the site about it. The father of the girl, being an Air Force officer, registered a case under section 67 of the Information Technology Act, 2000 with the Delhi Police Cyber Crime Cell. The police picked up the concerned student and kept him at Timarpur juvenile home. It was almost after one week that the Juvenile Board granted bail to the 16-year-old student. It is pertinent to note that the website did not contain any photographic material but only had text material which was allegedly obscene in nature.

State of Tamil Nadu v. *Dr. L. Prakash*

In the last week of December, 2001, India saw the registration of yet another case under section 67 of the Information Technology Act, 2000. The case was registered against Dr. L Prakash of Chennai on the complaint of Ganesh, a young man from Pondicherry.

Ganesh filed a criminal complaint at the Vadapalani police station at Chennai, alleging that Dr. L. Prakash was blackmailing him to have sex with women for featuring in pornographic videos and pictures. Ganesh, an SSLC student, alleged that Dr L Prakash threatened him with a revolver and forced him into sex. It is also alleged that Ganesh escaped to Pondicherry once but the doctor again blackmailed Ganesh into the sex racket.

Dr. L. Prakash is alleged to have lured college girls and working women for his pornographic videos and pictures with offers of big money. Even the women working at his clinic were reportedly not spared. Dr. Prakash allegedly preyed on women to keep his porn websites *www.realindianporn.com* and *www.tamilsex.com* thriving. The doctor allegedly circulated blue films and nude pictures through e-mails from his home. It was also alleged that the doctor's brother Laxmanan, who resides in the United States, helped him to sell pornographic videos in the West from which, the earnings reportedly ran into thousands of US dollars.

Consequently, a case was registered under section 67 of the Information Technology Act, 2000, section 4 read with section 6 of the Indecent Representation of Women Act and section 27 of the Arms Act and sections 120B and 506(2), IPC.

Dr. L. Prakash was arrested on December 14, 2001, for making pornographic vidoes using young girls and boys who came his way and also sending the video CDs labelled as 'surgical procedures' to the US and France, to be published by pornographic websites.

Fast track court judge R Radha, convicted Dr. L. Prakash for life imprisonment and imposed a fine of Rs. 1.27 lakh on Prakash and Rs. 2,500 each on his associates Saravanan (a ward boy in Prakash's clinic), Vijayan (driver) and Asir Gunasinth (radiologist). Considering the gravity of offences committed by the accused, maximum punishment under the Immoral Trafficking (Prevention) Act should be given. He was also convicted under IPC (conspiracy and kidnapping), IT Act (internet pornography), Indecent Representation of Women (Prohibition) Act and Arms Act. The court acquitted him of charges of rape. Further, Dr L Prakash was barred from medical practice by the Medical Council[38].

This case assumes tremendous importance in the light of the fact that online pornographic sites and brokers have been directly targeted for the first time in our country.

It is surprising that it took roughly 14 months after the coming into operation of the new Indian Cyberlaw, before the first real case aimed at online pornography was registered.

It is pertinent to note that the first case under section 67 of the Information Technology Act namely, *Bal Bharti Air Force School* case had a different colour to it in the sense that only a text based website was made by the concerned school boy. In the *Chennai* case, the case involved pornographic films and pictures taken by Dr. L. Prakash at his seaside resort, which were then supplied on the website *www.realindianporn.com* and *www.tamilsex.com*. The arrest of Dr. Prakash is also

38. http://www.dnaindia.com/india/report_chennai-porn-doc-gets-life_1149735.

important because Dr. Prakash becomes the first adult Indian to be arrested in an online pornography case under section 67 of the Information Technology Act.

The biggest question that arises is how would the present provision of section 67, IT Act, 2000 be implemented? The Information Technology Act, 2000 does not specify the *lex fori*, or the forum for trying the offence under section 67. In which area would a case of online pornography be registered? Which court would assume territorial jurisdiction on the same? These issues have not yet been sorted out.

Another fear that is looming large is whether section 67 of the Information Technology Act, 2000 would be effective or would it just remain a paper tiger. Clearly there are numerous lacunae in section 67 of Information Technology Act and its practical implementation is likely to lead to numerous problems, complications and challenges. The biggest challenge is that section 67 of the Information Technology Act only makes publishing or causing to be published or transmitted any lascivious or prurient material in the electronic form, a penal offence. Accessing or viewing any pornographic or obscene electronic information has not been made a penal offence. This issue is a matter of immense debate in the international Cyberlaw circles.

With the passage of time, it is hoped that the various issues raised by section 67 of the Information Technology Act, 2000 would be properly resolved.

Section 67A – Punishment for Publishing or Transmitting of Material Containing Sexually Explicit act, etc., in Electronic Form

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

Section 67A of the Information Technology Act, 2000 has been inserted by virtue of the Information Technology (Amendment) Act, 2008. Such a provision did not specifically exist earlier. Section 67A virtually copies the exact parameters of section 67 of the Information Technology Act, 2000 with slight modification. Section 67 of the Information Technology Act, 2000 as amended only deals with material in the electronic form which is lascivious or which 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 the relevant circumstances, to read, see or hear the matter contained or embodied in it. Section 67 deals broadly with the broad ambit and parameters of electronic or digital obscenity or pornography. However the Legislature has sought to add a specific section which specifically only deals with electronic material which contains sexually explicit acts or conduct. This has been sought to be brought within the ambit of section 67A of the amended Information Technology Act, 2000. Thus, the focus of section 67A is on any material in the electronic form which contains sexually explicit act or conduct.

Section 67A does not have any explanation as to what is the definition of "sexually explicit act or conduct".

Since Information Technology Act, 2000 is silent on the same, the Dictionary meaning of the said words would be applicable.

According to the freedictionary.com, **Explicit means a.** Fully and clearly expressed; leaving nothing implied. **b.** Fully and clearly defined or formulated: *"generalizations that are powerful, precise, and explicit" (Frederick Turner).* **2.** Forthright and unreserved in expression **3. a.** Readily observable, **b.** Describing or portraying nudity or sexual activity in graphic detail.[39]

According to Oxford dictionary, **Explicit means** (*adjective)* stated clearly and in detail, leaving no room for confusion or doubt, (of a person) stating something in an explicit manner, describing or representing sexual activity in a graphic fashion, (*noun)* the closing words of a manuscript, early printed book, or chanted liturgical text.[40]

According to en.wiktionary.org, **Explicit means** (adjective) Very specific, clear, or detailed.[41]

Further according to lectlaw, Sexually Explicit Conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.[42]

The cumulative reading of the aforesaid clearly shows that any content in the electronic form which contains explicit sexual act or conduct, would be covered within the provision of the offence under section 67A of the amended Information Technology Act, 2000. Thus, any electronic content which shows explicit sexual intercourse and other sexually explicit acts including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or public area of any person in this regard would be covered. In layman's language, hard-core pornography is sought to be covered under section 67A of the amended Information Technology Act, 2000 whereas pornography in general including soft pornography is sought to be covered under section 67 of the Information Technology Act, 2000. Thus if any person does any of the following acts pertaining to electronic material which contains sexually excited act or conduct, he would be liable under section 67A of the Information Technology Act, 2000:

(a) publishing of such content.
(b) transmission of such content.
(c) causing to be published such content.
(d) causing to be transmitted such content.

39. http://www.thefreedictionary.com/explicit
40. http://oxforddictionaries.com/definition/english/explicit
41. http://en.wiktionary.org/wiki/explicit
42. http://www.lectlaw.com/def2/s040.htm

However the limited applicability of section 67A is only in respect of material which is in the electronic form. Thus all kinds of blue films, hard-core pornographic clips, whether on computers or communication devices or mobile phones, their publication and transmission would be fully covered within the ambit of section 67A of the amended Information Technology Act, 2000.

As regards to what would be the exact meanings of the terms "publishing", "transmission" or "causing to be published or transmitted", kindly refer to the commentary under section 67 of the Information Technology Act, 2000.

The Legislature has sought to make a distinction between general pornographic material and sexually explicit act or conduct related electronic content. While digital obscenity under section 67 has been made a bailable offence, the law has sought to make the offence of publishing, transmission or causing to be published or transmitted, material in the electronic form which contains the sexually explicit acts or conduct as a much more serious offence. Under section 67A, the person on first conviction can be punished with imprisonment of either description for a term which may extend to 5 years and with fine which may extend to 10 lac. In the event of second or subsequent conviction, the person concerned can be punished with imprisonment of either description for a term which may extend to 7 years and also with fine which may extend to 10,000,00 INR. Thus section 67A is a non-bailable offence where the accused of the said offence is not entitled to bail as a matter of right but is entitled to bail subject to the subjective satisfaction and discretion of the court of law.

The net result of section 67A is that computers and mobile users in India will have to become extremely careful whenever they are either taking photographs or MMSs or videos from their or others mobile phones of sexually explicit acts or conduct. Such an act would qualify as an offence under section 67A. Further people need to be careful when they actually transmit MMSs or SMSs containing sexually explicit acts or conduct as the said SMSs and MMSs would also qualify to be covered under section 67A of the amended Act. Hence, given the tremendous adoption of mobile phones, users would be best advised to exercise caution when they deal with electronic material which contains sexually explicit acts or conduct.

It is further pertinent to point out that the proviso of section 67B is also applicable in section 67A of the IT Act. Section 67A has to be read in conjunction with the proviso to section 67B of the amended Information Technology Act, 2000. This proviso provides that the provisions of section 67A do not extend to a certain exempted category. The provisions of this section do not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form, provided two conditions are fulfilled. The first condition that is required to be fulfilled is that the publication of such a book, pamphlet, paper, writing, drawing, painting, representation of figure in the electronic form is proved to be justified as being for the public good on the ground that a such book, pamphlet, paper, writing, drawing, painting, representation of figure is in the interest of science, literature, art or learning or other objects of general concern.

The second condition that is required to be fulfilled is that the said book, pamphlet, paper, writing, drawing, painting, representation of figure in the electronic form is kept or used for any *bona fide*, heritage or religious purposes.

If any of the above two conditions are fulfilled, then section 67A of the amended Information Technology Act, 2000 shall not be applicable.

When one looks at the exempted categories, it is important to note that the law uses the word "as being for the public good".

The word "public good" has not been defined the Information Technology Act, 2000. However there is ample jurisprudence with regard to what constitutes public good.

In *Superintendent Central Prison, Fatehgarh* v. *Dr. Ram Manohar Lohia*,[43] the Supreme court defines the term public order as *"Public order " is synonymous with public safety and tranquillity: it is the absence of disorder involving breaches of local significance in contradistinction to national upheavals, such as revolution, civil strife, war, affecting the security of the State.*

Further the Supreme Court in *Municipal Council Raipur*[44] case defines public order as *"Public Order" in this context means public peace and tranquility.*

Further it is important to note that the requirement is not only that the publication has to be justified as being in the public good but that said justification only has to be on the ground that the said book, pamphlet, paper, writing, drawing, painting, representation of figure is in the interest of science, literature, art or learning or in the topics of general concern. Thus, *e.g.*, a picture of a nude body of a female could come within the parameters of section 67A of the Information Technology Act, 2000. However, in case if the picture is published for the purposes of showing the anatomy of the female body as in the interest of science, the publication of the said picture in the electronic form may not qualify for the applicability of section 67A of the Information Technology Act, 2000.

Further if any person makes in the electronic form, any of the sculptures which exist in Khajuraho that could qualify under section 67A of the Information Technology Act, 2000, but in case if the said sculptures from Khajuraho are captured in the electronic form, the said electronic publication being in the interest of art would not qualify for attracting section 67A of the Information Technology Act, 2000, thanks to the proviso to section 67B of the Information Technology Act, 2000.

Further, if two adults are captured in the electronic form performing various poses of sexual relations as depicted in Kamasutra, that publication would attract section 67A of the Information Technology Act, 2000, but in case if the said publication is done as re-creation of the Kamasutra in the exact manner and spirit as depicted in Kamasutra, the same could be deemed to be a publication for public good and in the interest of literature, art and other subject of general concern and as such, would not attract the applicability of section 67A of the Information Technology Act, 2000.

If Kamasutra is reproduced in the electronic form, the said electronic book would not attract section 67A of the Information Technology Act, 2000, thanks to the proviso to section 67B. Further if any electronic publication is kept

43. AIR 1960 SC 623: (1960) 2 SCR 821: 1960 Cr LJ 1002.

44. *Municipal Council Raipur* v. *State of Madhya Pradesh*, AIR 1970 SC 1923: 1970 Cr LJ 1656: (1970) 1 SCR 915.

or used for *bona fide* heritage or religious purposes, the said electronic publication would also not qualify for attracting section 67A of the Information Technology Act, 2000.

It is further pertinent to note that the Legislature is committed to not only making publishing or transmission as well as causing to be published or transmitted obscene electronic information a crime, but it has also taken proactive steps to ensure that such content ought not to be published or transmitted. In that regard, it is pertinent to note that the Central Government notified the Information Technology (Intermediary Guidelines) Rules, 2011. This is applicable to all intermediaries as defined under section 2(1)(w) of the Information Technology Act, 2000. Thus, any legal entity which in respect of any particular electronic record, receives, stores or transmits that record on behalf of another person or provides any service with respect to that record, are bound by the said guidelines. Rule 3 of the said Information Technology (Intermediary Guidelines) Rules, 2011 mandates that these intermediaries must have in place the rules and regulations, terms and conditions and user agreements which inform the users of their computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is obscene, pornographic, pedophilic or invasive of another's privacy.

If despite the said provisions detailed in the intermediaries terms and conditions, any person still violates the same, the intermediaries are mandated, on whose computer system the information is stored or hosted, to exercise due diligence while discharging their obligations under the Act. Once they obtain knowledge of the said pornographic information either by themselves or such pornographic content is brought to their actual knowledge by any affected person in writing, the said intermediaries are mandated to act within 36 hours and wherever applicable to disable such information that is in contravention of the law. If the said intermediary has failed to do the said exercise, they would also be seen as a co-conspirator and co-abettor of the crimes under section 67A of the Information Technology Act, 2000. As such, when one reads cumulatively sections 67A and 79 of the amended Information Technology Act, 2000 as amended alongwith Information Technology (Intermediary Guidelines) Rules, 2011, it is abundantly clear that intermediaries must exercise due diligence in the manner as stipulated under law and if they do not do so in respect of any obscene or pornographic content available on the computer resource, they could face criminal liability under section 67A of the Information Technology Act, 2000.

Section 67B – Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc., in Electronic Form

"Whoever,—

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with 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 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.*

Explanation.—For the purposes of this section "children" means a person who has not completed the age of 18 years."

Section 67B has been inserted in the Information Technology Act, 2000 by the Information Technology (Amendment) Act, 2008.

One of the main criticisms of section 67 of the amended Information Technology Act, 2000 was that the said provision was a general provision on obscenity and pornography and that it did not specifically deal with the delicate issue pertaining to child pornography. World over, it has been seen that countries have understood the significance of focusing on specific components of pornography. For example, the United States of America has focused extensively on child pornography. However, India did not have any specific legislation or legal provisions dealing with child pornography. The Information Technology (Amendment) Act, 2008 removed that criticism by inserting section 67B in the Information Technology Act, 2000. When one examines the said provisions of section 67B, it is clear that section 67B includes within its ambit numerous kinds of acts and circumstances all impacting children. When one looks at the structure and scope of section 67B, one realizes that the Legislature has provided sufficient safeguards to protect children online in the context of India. Various kinds of activities impacting child pornography have been specifically brought within the ambit of section 67B of the amended Information Technology Act, 2000. These activities are as follows:

(a) publishing material in the electronic form, which depicts children engaged in sexually explicit act or conduct;

(b) transmitting material in the electronic form, which depicts children engaged in sexually explicit act or conduct;

(c) causing to be published, material in the electronic form, which depicts children engaged in sexually explicit act or conduct;

(d) causing to be transmitted, material in the electronic form, which depicts children engaged in sexually explicit act or conduct.

According to the freedictionary.com, "**Explicit**" means a. Fully and clearly expressed; leaving nothing implied. b. Fully and clearly defined or formulated. 2. Forthright and unreserved in expression 3. a. Readily observable, b. Describing or portraying nudity or sexual activity in graphic detail.[45]

According to Oxford dictionary, "**Explicit**" means (*adjective)* stated clearly and in detail, leaving no room for confusion or doubt, (of a person) stating something in an explicit manner, describing or representing sexual activity in a graphic fashion, (*noun)* the closing words of a manuscript, early printed book, or chanted liturgical text.[46]

According to en.wiktionary.org, "**Explicit**" means (adjective) Very specific, clear, or detailed.[47]

Further according to lectlaw, Sexually Explicit Conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.[48]

The aforesaid acts are made an offence under section 67B(a). Further various activities concerning material in the electronic form which depicts children in obscene or indecent or sexually explicit manner, have also been covered under the ambit of section 67B. These activities include the activity of creating text or digital images, collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing such kind of child pornographic content. It is pertinent to note that the Legislature has for the first time in the history of Indian Cyberlaw, brought in the concept of penalizing a person for browsing electronic material depicting children in obscene or indecent or sexually explicit manner. The net effect of this is that whenever a person even browses child pornographic websites or websites which contain child pornographic material which show children in obscene or indecent or sexually explicit manner, the said activities have been brought within the ambit of penalty under section 67B of the amended Information Technology Act, 2000. Further even downloading child pornography and distributing the same has been brought within the ambit of the offence under section 67B of the amended Information Technology Act, 2000.

There are large numbers of pedophiles existing on the Internet. The number of pedophilic activities in India is constantly on the rise. There have been various cases in the public domain where children have been made targets by pedophiles. As such, to target the activities of pedophiles, under section 67B(c), anyone who

45. http://www.thefreedictionary.com/explicit
46. http://oxforddictionaries.com/definition/english/explicit
47. http://en.wiktionary.org/wiki/explicit
48. http://www.lectlaw.com/def2/s040.htm

cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act commits an offence. Further such action of cultivating, enticing or inducing children in a manner which can offend a reasonable adult on a computer resource have also been brought within the ambit of section 67B(c).

Thus all kinds of activities of pedophilic nature targeted at Indian children, have been sought to be brought within the ambit of section 67B of the amended Information Technology Act, 2000.

Further, facilitating child abuse online is an offence under section 67B(d) of the amended Information Technology Act, 2000. This facilitation of abuse of children can be in any manner or manifestation whatsoever.

Further, if any person records in the electronic form his own abuse or that of others pertaining to sexually explicit act with children, that has also been brought within the ambit of penalty under section 67B(e) of the amended Information Technology Act, 2000. Thus if a person shoots in the electronic form, the factum of his having intercourse or sexually explicit acts with children, that child pornographic movie and the entire act concerning the same would also qualify as an offence under section 67B of the amended Information Technology Act, 2000.

The *Explanation* to section 67B states that for purposes of this section, children mean a person who has not completed the age of 18 years. Thus any person who has not completed the age of 18 years and activities connected or concerned with him which fall within the ambit of section 67B of the amended Information Technology Act, 2000, are punishable thereunder.

Section 67B has taken a far more stringent stand on child pornography. That is the reason why the offence under section 67B is made punishable on a higher scale than the quantum of punishment given under section 67 of the Information Technology Act, 2000. Under section 67B, the offence is punishable on the first conviction with imprisonment for either description for a term which may extend to 5 years and fine which may extend to 10,000,00 INR. In the event of any second or subsequent conviction, the accused could be punished with imprisonment of either description for a term which may extend to 7 years and also with fine which may extend to 10,000,00 INR.

Proviso to section 67B of the amended Information Technology Act, 2000 provides that the provisions of section 67B do not extend to certain exempted categories. The provisions of this section do not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form, provided two conditions are fulfilled. The first condition that is required to be fulfilled is that the publication of such book, pamphlet, paper, writing, drawing, painting, representation of figure in the electronic form is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation of figure is in the interest of science, literature, art or learning or other objects of general concern.

The second condition that is required to be fulfilled is that the said book, pamphlet, paper, writing, drawing, painting, representation of figure in the electronic form is kept or used for any *bona fide*, heritage or religious purposes.

If any of the above two conditions are fulfilled, then section 67B of the amended Information Technology Act, 2000 shall not be applicable.

When one looks at the exempted categories, it is important to note that the law uses the word "as being for the public good".

The word "public good" has not been defined in the Information Technology Act, 2000. However there is ample jurisprudence with regard to what constitutes public good.

In *Superintendent Central Prison, Fatehgarh* v. *Dr. Ram Manohar Lohia,*[49] the Supreme court defines the term public order as *"Public order " is synonymous with public safety and tranquillity: it is the absence of disorder involving breaches of local significance in contradistinction to national upheavals, such as revolution, civil strife, war, affecting the security of the State.*

Further the Supreme Court in *Municipal Council, Raipur*[50] case defines public order as *"Public Order" in this context means public peace and tranquility.*

Further it is important to note that the requirement is not only that the publication has to be justified as being in the public good but that said justification only has to be on the ground that the said book, pamphlet, paper, writing, drawing, painting, representation of figure is in the interest of science, literature, art or learning or in the topics of general concern.

Section 67B aims to protect children from sexual predators and pedophiles.

It is further pertinent to note that the legislature is committed to not only making publishing or transmission as well as causing to be published or transmitted obscene electronic information a crime, but it has also taking proactive steps to ensure that such content ought not to be published or transmitted. In that regard, it is pertinent to note that the Central Government notified the Information Technology (Intermediary Guidelines) Rules 2011. This is applicable to all intermediaries as defined under section 2(1)(w) of the Information Technology Act, 2000. Thus, any legal entity which in respect of any particular electronic record, receives, stores or transmits that record on behalf of another person or provides any service with respect to that record, are bound by the said guidelines. Rule 3 of the said Information Technology (Intermediary Guidelines) Rules, 2011 mandates that these intermediaries must have in place the rules and regulations, terms and conditions and user agreement which inform the users of the users of their computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is obscene, pornographic, pedophilic or invasive of another's privacy or/and harms minors in any way.

If despite the said provisions detailed in the intermediaries terms and conditions, any person still violates the same, the intermediaries are mandated on whose computer system the information is stored or hosted to exercise due diligence while discharging their obligations under the Act. Once they obtain knowledge of the said pornographic information either by themselves or such pornographic content is brought to their actual knowledge by any affected person

49. AIR 1960 SC 633: (1960) 2 SCR 821: 1960 Cr LJ 1002.
50. *Municipal Council Raipur* v. *State of Madhya Pradesh,* AIR 1970 SC 1923: 1970 Cr LJ 1656: (1970) 1 SCR 915.

in writing, the said intermediaries are mandated to act within 36 hours and wherever applicable to disable such information that is in contravention of the law. If the said intermediary has failed to do the said exercise, they would also be seen as a co-conspirator and co-abettor of the crimes under section 67B of the Information Technology Act, 2000. As such, when one reads cumulatively section 67B and 79 of the amended Information Technology Act, 2000 as amended alongwith Information Technology (Intermediary Guidelines) Rules, 2011, it is abundantly clear that intermediaries must exercise due diligence in the manner as stipulated under the law and if they do not do so in respect of any obscene or pornographic content available on the computer resources, they could face criminal liability under section 67B of the Information Technology Act, 2000.

Since the entire scope of information described under section 67B of the amended Information Technology Act, 2000, harms minors in one way or the other, all kinds of electronic content and activities detailed in section 67B which impact or are connected with children or child pornography would be fully covered within the ambit of this content which harms minors in any way.

Since all such kinds of activities are abetting child pornography, then using mobile phones and communication devices also would qualify within the ambit of section 67B of the amended Information Technology Act, 2000

Thus seen from overall perspective, sections 67, 67A and 67B of the amended Information Technology Act, 2000 constitute a distinct code in their ownselves pertaining to India's legislative response against pornography, obscenity and child pornography *per se*. These, when read with section 292 of the Indian Penal Code, seek to prevent the publishing or transmission of pornography and obscene materials both in the physical and electronic ecosystem as also in the physical world. At the time of writing, not many cases have been reported under section 67A and 67B of the amended Information Technology Act, 2000 nor have there been any convictions in this regard. It will be interesting to see how the jurisprudence around the entire issues pertaining to online obscenity and child pornography emerges in India, as time passes by.

Section 67C – Preservation and Retention of Information by Intermediaries

"(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may 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 also be liable to fine."

Section 67C has been inserted in the Information Technology Act, 2000 by virtue of Information Technology (Amendment) Act, 2008. Section 67C is focused on preservation and retention of the relevant electronic information and logs by all intermediaries. Section 67C(1) provides that all intermediaries are mandated to preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may so prescribe. It is important to note that an intermediary is the repository of all relevant information

pertaining to all relevant electronic transactions. This is so, given the intrinsic nature and role of intermediaries.

Intermediary with respect to any particular electronic records, includes any person who on behalf of another person, receives, stores or transmits that particular electronic record or provides service with respect to that record.

Given the intrinsic nature of the activities of an intermediary, an intermediary stores huge volumes of information. This information would not only include information pertaining to illegal or criminal acts done by legal entities, but would also include automatically computer-generated data and computer logs which have a connection and association with various electronic activities done by various legal entities. This information including computer logs and meta data is extremely relevant information for the purposes of not just cyber forensics but also for the purposes of identification of relevant stake-holders and information which throws substantial light on the nature and kind of illegal and other activities committed by the relevant entities. As such, intermediaries are mandated to preserve such information. Section 67C(1) says this information may be specified by the Central Government, who may also specify the manner and format of retention and preservation of such information and its duration. It is pertinent to note that the Central Government notified the Information Technology (Intermediary Guidelines) Rules, 2011. Rule 3(4) of the Information Technology (Intermediary Guidelines) Rules, 2011 clearly state that intermediaries shall preserve information which is stored, hosted or published on the intermediaries' computer system which is in violation of Rule 3(2) of the Information Technology (Intermediary Guidelines) Rules, 2011 and associated records for at least 90 days for investigation purposes. Further it is pertinent to note that under section 79(3)(b), the intermediary is mandated to not vitiate the evidence in any manner whatsoever of any event. Currently, at the time of writing, the manner and format of preservation and retention of such electronic information as is indicated by section 67C have not been so specified by the Government. However it is only a question of time before the Government specifies the manner and format of preservation and retention of such information as is mandated under section 67C of the amended Information Technology Act, 2000.

Of further relevance are the provisions of section 67C(2). Section 67C(2) carves out a new offence. As per the said provision, if any intermediary intentionally or knowingly contravenes the provisions of section 67C(1) which deals with mandatory preservation and retention of information for the duration and in the manner and format specified by the Central Government, that act has been made as an offence. The said offence is punishable with imprisonment for a term which may extend to 3 years and shall also be liable for fine. Thus, section 67C (2) creates a new offence under the Information Technology Act, 2000. The said offence is a bailable offence where the concerned legal entity is entitled to bail. In case, the intermediary is a company, then section 85 of the Information Technology Act, 2000 would be applicable. By virtue of the same, every person who, at the time, the said contravention was committed, was in charge of, and was responsible to the said intermediary company for the conduct of business of the said intermediary company as well as the intermediary company shall be guilty of the said offence.

The net effect of section 67C is that intermediaries will now be made more accountable in respect of their electronic records. The last one decade has shown that intermediaries and service providers have generally been very lax and careless about retaining and preserving relevant electronic records. Given the fact that storage of electronic records was expensive earlier, a large number of service providers would invariably not even store electronic information for a couple of months. However as time is passing by, electronic storage is becoming increasingly less expensive. As such now intermediaries are mandated to preserve and retain all information that the Government may so specify along with its manner and format and for the duration to specify.

If any intermediary fails to do so, he would be playing with fire as its activities would attract the offence under section 67C(2) of the amended Information Technology Act, 2000. Section 67C of the Information Technology Act, 2000 is going to play an important role not only in ensuring intermediaries discipline themselves in terms of retention and preservation of electronic records and computer logs but also for the purposes of facilitating availability of such electronic records and computer logs for the purposes of cyber forensics, cyber investigation and also for legal proceedings in a court of law. At the time of writing, no case under section 67C has been registered as per information available in the public domain. It is imperative that section 67C(2) needs to be stringently implemented to ensure that intermediaries do not take their mandatory obligations of retention and preservation of concerned electronic records and logs lightly and further understand the significance and scope of their business activities. Over a period of time effective implementation of section 67C is likely to build up an enabling framework in the country whereby intermediaries fulfil their mandatory obligations of preservation and retention of relevant electronic records and evidence including computer logs for the purposes of efficient and seamless administration of law and justice in the times to come.

Section 68 - Power of 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 to a fine not exceeding one lakh rupees or to both."

The language of section 68(2) has been substituted by way of the Information Technology (Amendment) Act, 2008. By virtue of amendment the term *"intentionally or knowingly"* has been inserted in the Act.

Section 68 (1) of the Information Technology Act gives additional powers to the Controller to give various directions to ensure compliance with the provisions of the Information Technology Act, 2000, rules and regulations made thereunder. The Controller has discretion to direct a Certifying Authority or any employee of such authority to take such steps or measures if they are necessary to ensure

compliance with the provisions of the Information Technology Act, Rules and regulations made thereunder. The Controller may give these directions by a written order. The words used under section 68 (1) of the Information Technology Act are "by order" which can be verbal or written. However, it shall be imperative upon the Controller to issue a written order.

Similarly, the Controller has been given the discretion to direct a Certifying Authority or any of its employees to cease carrying on such activities as specified in the order if they are necessary to ensure compliance with the Information Technology Act, 2000, rules and regulations made thereunder. These functions and powers that the Controller has to perform are given under section 18 of the Information Technology Act, 2000.

Further, section 68(2) of the Information Technology Act provides that intentional or knowing failure to comply with any order passed under section 68(1) of the Information Technology Act shall be an offence. This offence is punishable with imprisonment for a term not exceeding two years or a fine not exceeding 1,00,000 INR or both. The offence can be committed either by the Certifying Authority and or any third party who so directed by means of the said order under section 68(1) of the Information Technology Act by the Controller of Certifying Authorities. However the offence under section 68(2) of the Information Technology Act is a bailable offence where the accused is entitled to bail as a matter of right.

The purpose of inserting section 68 of the Information Technology Act is to ensure complete compliance with the provisions of the Information Technology Act, 2000, Rules and regulations made thereunder.

Section 69 – Power to Issue Directions for Interception or Monitoring or Decryption of any Information through any Computer Resource

"(1) Where the Central Government or a State Government or any of its officer specially 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 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.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency 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."

Section 69 has been amended by the Information Technology (Amendment) Act, 2008. Section 69, after amendment, today becomes one of the most important tools in the hands of sovereign India to protect its sovereign rights from various illegal, criminal and terrorist activities that have been targeted against India. The earlier section 69 had a different flavour altogether. Section 69 of the un-amended Information Technology Act, 2000 read as follow:

"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."

However as time passed by, it was very clear that the need of the Government to intercept any information became more and more acute. This is so because of the immense challenges that were being faced by the Indian nation in the context of attempts made to prejudicially impact its sovereignty, integrity and security. In that context, section 69 assumes paramount significance. Section 69 provided for the power to issue directions for interception of any information through any computer resource.

The Mumbai attacks happened on 26-11-2008. The said event demonstrated in no unclear terms as to how technology could be used so as to prejudicially impact the Indian sovereignty, security and integrity. In the wake of the 26/11 Mumbai attacks, section 69 was amended by the Information Technology (Amendment) Act, 2008. The amended section 69 is on a broader pedestal than the earlier section 69. This is so because the earlier section only dealt with the power of interception. However, the amended section 69 now talks about three distinct processes being interception, monitoring and decryption.

The significance of section 69 is brought forward by the fact that it talks about "computer resources". The term "computer resource" is defined under section 2(1)(k) to mean computer, computer systems, computer network, data, computer database or software. However, when one examines the definition of the term

"computer network" defined under section 2(1)(j) of the Information Technology Act, 2000 it clearly means the inter-connection of one or more computers, computer systems or communication devices through the use of satellite, microwave, terrestrial line, wire, wireless or other communication media as also through terminals or a complex consisting of two or more inter-connected computers or communication devices, whether or not the inter-connection is continuously maintained. Thus, all kinds of computer resource networks as also communication devices as also computers, computer systems and computer networks come within the ambit of the term "computer resource", as referred to under section 69 of the Information Technology Act, 2000. The coverage of section 69 is thus comprehensive for all kinds of computers, computer systems, computer networks, computer resources, communication and electronic devices.

Section 69 provides the discretion to direct interception, monitoring or decryption of information through any computer resource.

The earlier section 69 of the Information Technology Act, 2000 had vested in the hands of the Controller of Certifying Authorities, the discretion so as to direct interception of any information transmitted to any computer resource.

However, as time passed by, potentially it was realized that the said exercise was not a convenient nor expedient exercise since the earlier law had only provided for the Controller of Certifying Authorities to be satisfied for interception and then the Controller could direct any agency of the Government to intercept any information transmitted through any computer resource. The Legislature realized that given the speed in which criminal activities are being done and the manner, in which India's computer resources and computer networks are being targeted, it is only necessary and expedient that the time delay in getting the appropriate directions for interception of electronic evidence, be minimized to the barest extent possible. As such, the Legislature decided that instead of the Controller of Certifying Authorities, it shall now be the appropriate Government who will have the power to direct interception, monitoring or decryption of information through any computer resource. The said appropriate Government could either be the Central Government or it could be a State Government or it could be any of its officers who are specially authorized by the Central Government or the State Government in this behalf.

There are various important elements which constitutes the salient features of section 69 of the amended Information Technology Act, 2000.

The first significant thing to note about section 69 is that it actually grants powers to both Governments, Central and State in India, in the context of interception, monitoring and decryption of information through any computer resource.

The power under section 69 can only be exercised by the following:

(a) the Central Government; or

(b) a State Government; or

(c) Any of its officers specifically authorized by the Central Government; or

(d) Any of its officers specifically authorized by the State Government.

It is pertinent to point out that section 69 has not defined the terms "interception" "monitoring" or "decryption". Even section 2 of the Information Technology Act, 2000 is silent in giving any definitions to these terms. However, the government notified the Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009 in the year of 2009. The definition clause of the Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009 has defined the terms "Interception", "Monitoring" and "Decryption".

Rule 2(f) of the Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009 defines the term "decryption" to mean the process of conversion of information in non-intelligible form to an intelligible form *via* a mathematical formula, code, password or algorithm or a combination thereof.

Further rule 2(l) of the Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009 defines the term "intercept" as with its grammatical variations and cognates expressions, to mean 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 an information available to a person other than a sender or recipient or intended recipient of that communication, and includes—

(a) Monitoring of any such information by means of a monitoring device;

(b) Viewing, examination or inspection of the contents of any direct and indirect information; and

(c) Diversion of any direct and indirect information from its intended destination to any other destination;

Further, rule 2(m) of the Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009 defines the term "interception device" to mean any electronic, mechanical, electro- mechanical, electro-magnetic, optical and 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 any reference to an "interception device" includes, where applicable, a reference to a "monitoring device".

Rule 2(o) of the Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009 defines the term "Monitor" as with its grammatical variations and cognates expressions, to include to view or to inspect or listen to or record information by means of monitoring device.

Rule 2(p) of the Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009 defines the term "Monitoring Device" to mean any electronic, mechanical, electro- mechanical, electro- magnetic, optical and 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 view or to inspect or to listen to or record any information.

The power of section 69 is indeed very vast and can be invoked on the discretion of any of the aforesaid legal entities. However, before exercising such powers, the aforesaid legal entities must be satisfied that it is necessary to issue directions for interception or monitoring or decryption of information through any computer source in any of the following circumstances:

(a) In the interest of the sovereignty or integrity of India;

(b) In the interest of defence of India;

(c) In the interest of security of the State;

(d) In the interest of friendly relations with foreign States;

(e) In the interest of public order;

(f) In the interest of preventing incitement to the commission of any cognizable offence relating to the above; or

(g) For investigation of any offence.

Clearly, the aforesaid are broad parameters which have not been specifically defined.

After being satisfied about the necessity of the aforesaid, appropriate Government or its officers has to record reasons in writing about its satisfaction and about the necessity and expediency of the proposed action of interception or monitoring or decryption and only then, can appropriate Government or its officers, by order, direct interception or monitoring or decryption of the relevant information. The language of section 69(1) has been drafted in mandatory terms and all the conditions have to be fulfilled before interception of the information can be ordered.

Interception or monitoring or decryption of information is a very precarious and dangerous phenomenon as it has immense impact and connotations on the fundamental rights, the privacy and fundamental freedoms of citizens. Interception or monitoring or decryption of information can be seen as a reasonable restriction, which can be imposed upon the enjoyment of fundamental rights. These interceptions or monitorings or decryptions have to be reasonable and have to stand the test of reasonableness, as has been laid down by the Supreme Court in various judgments. Since such kind of power of interception or monitoring or decryption is capable of being misused, therefore, all the conditions stipulated under section 69(1) have to be strictly followed. Otherwise, the court, in its writ jurisdiction, is empowered to strike down any action of interception.

Article 19(1)(a) of the Constitution of India, grants the fundamental right to freedom of speech and expression. Article 19(1)(a) states that "all citizens shall have the right to freedom of speech and expression".

People write or speak what they feel like, in exercise of their fundamental right under article 19(1)(a) of the Constitution of India. Similarly, people freely express their thoughts in the electronic environment. The relevant issue, therefore, before us is whether interception or monitoring or decryption of electronic information transmitted through any computer resource would amount to a violation of article 19(1)(a) of the Constitution of India.

It is important to note that unlike the right to freedom of speech and expression guaranteed by the American Constitution, the right to freedom of speech and expression under article 19(1)(a) of the Constitution of India includes the right to acquire information and disseminate it. The Supreme Court has held in *Secretary, Ministry of Information and Broadcasting, Government of India* v. *Cricket Association of Bangalore*,[51] as follows:—

> *"The freedom of speech and expression includes right to acquire information and to disseminate it. Freedom of speech and expression is necessary, for self-expression, which is an important means of free conscience and self-fulfilment. It enables people to contribute to debates on social and moral issues. It is the best way to find a truest model of anything, since it is only through it that the widest possible range of ideas can circulate. It is the only vehicle of political discourse so essential to democracy. Equally important is the role it plays in facilitating artistic and scholarly endeavours of all sorts. The right to communicate, therefore, includes right to communicate through any media that is available whether print or electronic or audio-visual such as advertisement, movie, article, speech etc. That is why freedom of speech and expression includes freedom of the Press. The freedom of the Press in terms includes right to circulate and also to determine the volume of such circulation. This freedom includes the freedom to communicate or circulate one's opinion without interference to as large a population in the country, as well as abroad, as is possible to reach. This fundamental right can be limited only by reasonable restrictions under a law made for the purposes mentioned in article 19(2)… The burden is on the authority to justify the restrictions."*

Under article 19(1)(a), every citizen has a right to impart and receive information as part of his fundamental right to speech and expression. The right to communicate effectively has been read as an integral part of article 19(1)(a) of the Constitution. There are no geographical barriers on communication. Hence every citizen has a right to use the best means available for the purpose. At present, electronic media, *viz.*, Internet, TV and radio, is the most effective means of communication.

Under the Constitution, the State is not only under an obligation to respect this fundamental right of the citizens, but equally under an obligation to ensure conditions under which this right can meaningfully and effectively be enjoyed by one and all. Freedom of speech and expression is basic to and indivisible from a democratic polity.

As noted, the right to freedom of speech and expression is not an absolute right and the same is restricted by certain reasonable restrictions as are given in article 19(2) of the Constitution. Article 19(2) of the Constitution states, "Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, insofar as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in 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".

51. AIR 1995 SC 1236: 1995 AIR SCW 1856.

Article 19(2) refers to reasonable restrictions as are essential for the proper working of the nation and the Government. As the Supreme Court has held in *Supdt. Central Prison* v. *Ram Manohar Lohia*[52]:

> *"…. It is self-evident and commonplace that freedom of speech is one of the bulwarks of a democratic form of Government. It is equally obvious that freedom of speech can only thrive in an orderly society. Clause (2) of article 19, therefore, does not affect the operation of any existing law or prevent the State from making any law in so far as such law imposes reasonable restrictions on the exercise of the right of freedom of speech in the interest of public order, among others."*

Article 19(2) says that the reasonable restrictions must be in 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. Under section 69 of the Information Technology Act, similar grounds of reasonable restrictions have been cited to direct interception of any information transmitted through any computer resource.

Section 69 of the Information Technology Act, 2000 does not use the words "reasonable restrictions". However, it does elaborate the grounds of reasonable restrictions to be the grounds on which the officials of the appropriate government can order interception and decryption of any information transmitted through any computer resource.

The first four grounds given in section 69(1) of the Information Technology Act, 2000 relating to sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order relate to different issues concerning national interests of the country at large.

The words "sovereignty or integrity of India" and "the security of the State" are vast in import and impact the very existence of the Indian nation. The Supreme Court has held that incitement to crimes of violence like murder would undermine the security of the State.[53]

The Supreme Court in *Supdt. Central Prison* v. *Ram Manohar Lohia*,[52] has elaborately dealt with the concept of public order as appeared in article 19(2) of the Constitution of India. In the said judgment, the Supreme Court has held as under:—

> *"…The words "public order" were also understood in America and England as offences against public safety or public peace.*
>
> *The offence known as breach of the peace embraces a great variety of conduct destroying or menacing public order and tranquility. It includes not only violent acts and words likely to produce violence in others. No one would have the hardihood to suggest that the principle of freedom of speech sanctions incitement to riot…. When clear and present danger of riot, disorder, interference with traffic upon the public streets, or other immediate threat to public safety, peace or order appears, the power of the State to prevent or punish is obvious.*

52. AIR 1960 SC 633: (1960) 2 SCR 821: 1960 Cr LJ 1002.
53. *State of Bihar* v. *Shailabala Devi*, AIR 1952 SC 329: 1952 SCR 654: 1952 Cr LJ 1373.

The American decisions sanctioned a variety of restrictions on the freedom of speech in the interests of public order. They cover the entire gamut of restrictions that can be imposed under different heads in article 19(2) of our Constitution.

But in India under article 19(2) this wide concept of "public order" is split up under different heads. It enables the imposition of reasonable restrictions on the exercise of the right to freedom of speech and expression in the interests of 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. All the grounds mentioned therein can be brought under the general head "public order" in its most comprehensive sense. But the juxtaposition of the different grounds indicates that, though sometimes they tend to overlap, they must be ordinarily intended to exclude each other. "Public order" is therefore something, which is demarcated from the others. In that limited sense, particularly in view of the history of the amendment, it can be postulated that "public order" is synonymous with public peace, safety and tranquility. Hence "public order" is synonymous with public safety and tranquility, the absence of disorder involving breaches of local significance in contradistinction to national upheavals, such as resolution, revolution, civil strife, war affecting the security of the State.

The limitation imposed in the interests of public order to be a reasonable restriction, should be one, which has a proximate connection or nexus with public order, but not one far-fetched, hypothetical or problematical or too remote."

This interpretation of "public order" would be applicable in the context of section 69(1) of the Information Technology Act, 2000.

The Supreme Court in *Secretary, Ministry of Information & Broadcasting, Government of India* v. *Cricket Association of Bengal*,[54] has held its following ratio with regard to article 19(2) of the Constitution of India which also has a direct bearing on section 69 of the Information Technology Act:—

"...The first set of grounds, viz., the sovereignty and integrity of India, the security of the State, friendly relations with foreign States and public order are grounds referable to national interest whereas the second set of grounds, viz., decency, morality, contempt of court, defamation and incitement to offence are conceived in the interest of society. The inter-connection and the inter-dependence of freedom of speech and the stability of society is undeniable. They indeed contribute to and promote each other. Freedom of speech and expression in a democracy ensures that the change desired by the people, whether in political, economic or social sphere, is brought about peacefully and through law. That change desired by the people can be brought about in an orderly, legal and peaceful manner is by itself an assurance of stability and an insurance against violent upheavals which are the hallmark of societies ruled by dictatorships, which do not permit this freedom. The converse is equally true. The more stable the society is, the more scope it provides for exercise of right of free speech and expression. A society, which feels secure, can and does permit a greater latitude than a society whose stability is in constant peril...

54. AIR 1995 SC 1236: 1995 AIR SCW 1856.

... The right to freedom of speech and expression cannot rise above the national interest and the interest of society, which is, but another name for the interest of general public."

It is also essential that the order of the Government officials directing interception must be reasonable and must pass the test of reasonableness. In *Suptd. Central Prison, Fatehgarh* v. *Ram Manohar Lohia*,[55] the Supreme Court held as follows:

"... The word "reasonable" has been defined by this court in more than one decision. It has been held that in order to be reasonable, "restrictions must have reasonable relation to the object which the legislation seeks to achieve and must not go in excess of that object." The restriction made "in the interests of the public order" must also have reasonable relation to the object to be achieved, i.e., the public order. If the restriction has no proximate relationship to the achievement of public order, it cannot be said that the restriction is a reasonable restriction within the meaning of the said clause."

In the case entitled *P.P. Enterprises* v. *Union of India*,[56] the Supreme Court has held as under:—

".... The expression 'reasonable restrictions' signifies that the limitation imposed on a person in enjoyment of that right should not be arbitrary or of an excessive nature beyond what is required in the interest of the public. No cut and dry test can be applied to each individual statute impugned, nor an abstract standard or general pattern of reasonableness can be laid down as applicable in all cases."

The issue of whether section 69 is violative of article 19(1)(a) of the Constitution of India will have to be tested in the hot waters of judicial scrutiny. However, it is important to note the test of reasonableness, which the Supreme Court has laid down, upon which every statutory provision has to be tested for its compliance. In *MRF Ltd.* v. *Inspector, Kerala Government*,[57] the Supreme Court has held as under:—

"... In examining the reasonableness of a statutory provision, whether it is violative of the Fundamental Right guaranteed under article 19, one has to keep in mind:

(1) The Directive Principles of State Policy.

(2) Restrictions must not be arbitrary or of an excessive nature so as to go beyond the requirement of the interest of the general public.

(3) In order to judge the reasonableness of the restrictions, no abstract or general pattern or a fixed principle can be laid down so as to be of universal application and the same will vary from case to case as also with regard to changing conditions, values of human life, social philosophy of the Constitution, prevailing conditions and the surrounding circumstances.

55. AIR 1960 SC 633: (1960) 2 SCR 821: 1960 Cr LJ 1002.
56. AIR 1992 SC 1016.
57. AIR 1999 SC 188: 1998 AIR SCW 3550: (1998) 8 SCC 227.

(4) *A just balance has to be struck between the restrictions imposed and the social control envisaged by article 19(6).*

(5) *Prevailing social values as also social needs which are intended to be satisfied by the restrictions.*

(6) *There must be a direct and proximate nexus or a reasonable connection between the restrictions imposed and the object sought to be achieved. If there is a direct nexus between the restrictions, and the object of the Act, then a strong presumption in favour of the constitutionality of the Act will naturally arise."*

If the appropriate Government or any of its authorized officers are satisfied about any of the aforesaid parameters, the appropriate Government or its authorized representative or officers, may, direct interception, monitoring or decryption of information. Further, if the aforesaid parameters are satisfied, the appropriate Government or its officers may direct any agency of the appropriate government to do any of the following:

(a) To intercept any information generated, transmitted, received or stored in any computer resource.

(b) To monitor any information generated, transmitted, received or stored in any computer resource.

(c) To decrypt any information generated, transmitted, received or stored in any computer resource.

(d) Cause to be intercepted any information generated, transmitted, received or stored in any computer resource.

(e) Cause to be monitored any information generated, transmitted, received or stored in any computer resource.

(f) Cause to be decrypted any information generated, transmitted, received or stored in any computer source.

However, the said discretion can only be exercised subject to reasons to be recorded in writing. Further, the exercise of such powers is subject to the provisions of sections 69(2) of the Information Technology Act, 2000.

Thus, the scope of the powers that have been granted, are indeed huge wide and comprehensive. The only caveat is that the said powers have to be exercised subject to the provisions of section 69(2) of the amended Information Technology Act. Section 69(2) stipulates that the procedural safeguards subject to which such interception, monitoring or decryption may be carried out shall be such as may be specified. However, all procedures, safeguards, checks and balances as may be prescribed by the appropriate Government from time-to-time with regard to interception, monitoring or decryption, shall need to be carried out.

It is pertinent to note that earlier section 69 only talked about interception of information transmitted through any computer resource in India. However, the ambit, scope and applicability of the amended section 69 has been tremendously widened and made far more comprehensive. Section 69 now deals not just with interception but also with monitoring and decryption of information which is generated, transmitted, received or stored in a computer resource. Thus, the current

section 69 is far wider in its applicability and is of tremendous relevance from the perspective of protecting and preserving the sovereign interests of India.

The said agency of the appropriate Government which has been directed to intercept, monitor or decrypt or cause to be intercepted, monitored or decrypt any information generated, transmitted, received or stored in any computer resource, has been given the mandatory responsibility to call upon any subscriber or intermediary or person in-charge of the computer resource to co-operate in such an exercise. It is also been made mandatory responsibility of the said subscriber or intermediary or any person in-charge of the computer resource, to extend all facilities and technical assistance to the said specified agency, for the purposes of interception, monitoring or decryption. Further, whenever such an agency calls for any assistance, facilities or technical assistance, the subscriber, intermediary or any other person in-charge of the computer resource has the mandatory duty to extend all technical facilities and technical assistance with respect to the following:

- Providing access to or securing access to the computer resource generating, transmitting, receiving or storing such information:
- To intercept, monitor or decrypt the information as the case may be.
- To provide information stored in the computer resource.

Thus, each subscriber or intermediary or person in charge of a computer resource, has to be mentally prepared that whenever he or she is called upon by any specified agency, which has been authorized to intercept monitor or decrypt information, he/she would be required to extend mandatorily all possible facilities and technical assistance for the aforesaid activities. This would include technically extending facilities and technical assistance to provide access or to secure access to the relevant computer resource which is generating, transmitting and receiving or storing such information. Thus, not only the physical access to the said computer resource would have to be provided but even access to all data and information resident therein or transmitted therefrom, shall also be required to be provided.

Further, the said subscriber, intermediary or other person has to be prepared to extend all facilities and technical assistance to intercept, monitor or decrypt information, as the case may be. It is clear that there are a lot of potential problems regarding the actual implementation of this section as we go along. This is so because it is possible that the subscriber, intermediary or person in-charge of the computer resource, may or may not have all facilities and technical assistance to intercept monitor or decrypt information. Further, the said subscriber intermediary or person in-charge of computer resources is further mandated to extend all facilities and technical assistance to provide information in the computer resource.

The Legislature has been very comprehensive in elaborating all detailed obligations that it requires the subscribers, intermediaries or persons in-charge of computer resources to perform, when they are called upon to do so, by an agency which is directed to intercept, monitor or decrypt information under section 69 of the amended Information Technology Act, 2000. However, while legislating such a provision, the Legislature seems to have forgotten that it may not be possible at all times for the said subscriber, intermediary or other person in-charge of

computer resource to provide or extend all facilities and technical assistance to intercept, monitor or decrypt information, as the case may be. While, in theory it is good to straddle the said subscriber, intermediary or person in-charge of its computer resource, with all obligations to extend facilities and technical assistance for the said operations, the practical situation may be completely different. This assumes all the more significance, given the specific provisions that are provided under section 69(4) of the Information Technology Act, 2000.

Section 69(4) categorically says that if the subscriber, intermediary or any person in-charge of a computer resource fails to assist the agency in the manner as referred to under section 69(3), he commits an offence. The said offence shall be punishable with imprisonment for a term which may extend to 7 years and shall also be liable to fine. Thus, section 69(4) creates a very serious and complex offence. The danger of section 69(4), is that large number of subscribers, intermediaries and persons in-charge of computer resources may come within the ambit of the mischief under section 69(4), inadvertently or unintentionally. The way section 69(4) is worded, there is no need to show the existence of any intention or knowledge. A mere failure to assist the agency has been made a crime punishable with imprisonment for a term which may extend to 7 years, apart from fine. It is very much possible that lot of unsuspecting and *bona fide* subscribers, intermediaries and persons in-charge of computer resources may be sucked in the whirlpool of the offence created under section 69(4) of the amended Information Technology Act, 2000. The Legislature has overlooked the practical realities that at the relevant time, the subscriber, intermediary or persons in-charge of computer resources may not have all facilities and technical assistance for the purposes of interception, monitoring or decrypting information of any computer resource. This is so because, the facilities of interception, monitoring or decryption of information would involve not just specialized software and tools but also various new kinds of hardware. Non-purchasing of the said hardware as also the software for interception, monitoring or decryption of information, could come within the ambit of failure to assist the agency. Hence, it is very much possible that the law enforcement agencies may book large number of subscribers, intermediaries or persons in-charge of computer resources on the ground that they have failed to assist the designated agency for interception, monitoring or decryption. Section 69(4) is a provision which is likely to be potentially misused, as time passes by. This becomes all the more relevant, in the context of computer resources servers and computer resources computing. A large number of subscribers, intermediaries and persons in-charge of computer resources do not retain with them the facilities and technical assistance to intercept, monitor or decrypt information, passing through the said computer resources hardware, or any other computer devices or computer networks. In the event of the said subscribers, intermediaries or persons in-charge of computer resources being called upon by the designated agency to extend all facilities and technical assistance to intercept, monitor or decrypt information, there are chances that such group of subscribers, intermediaries or persons in-charge of computer resources may not be in a position to extend the said facilities and technical assistance. Penalizing the said failure to do so is a very harsh step and is likely to become a contentious bed of issues, as time passes by.

Given the fact that the exercise of the powers of interception, monitoring or decryption of information through any computer resource are directly related to national interest, failing to assist the agency to extend all facilities and technical assistance given under section 69(3) itself becomes an offence. If the subscriber or intermediary or any other person mentioned under section 69(3) fails to extend all facilities and technical assistance to the agency under section 69(3), he shall be punishable with a very serious offence. The said offence is defined under section 69(4) of the Information Technology Act, 2000 and is punishable with imprisonment for a term which may extend to 7 years and shall also be liable to fine. Thus, the offence under section 69(4) is a non-bailable cognizable offence, triable by the Magistrate of the First Class.

It is pertinent to note that the Government of India has already notified the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. These Rules were also notified on 27th October, 2009 and stipulate certain safeguards while giving directions to intercept, monitor or decrypt any information.

Rule 3 of the said Rules stipulates that no person shall carry out the interception, monitoring or decryption of any information generated, transmitted, received or stored in any computer resource except by an order issued by the competent authority. The Rules further provide that in unavoidable circumstances, such order may be issued by an officer not below the rank of Joint Secretary to the Government of India who has been authorized by the competent authority. The Rules further provide that in the event of an emergency, interception, monitoring or decryption of any information may be carried out with the prior approval of the head or the second senior-most officer of the security and law enforcement agency at the Central level and the offices authorized in this behalf not below the rank of Inspector-General of Police or an officer of equivalent rank in the State or Union Territory level.

The competent authority has been defined under the said Rules to mean the Secretary in the Ministry of Home Affairs in the case of Central Government or the Secretary in-charge of the Home Department, in the case of a State Government or Union Territory as the case may be.

Rule 11 of the said Rules mandates that the directions for interception or monitoring or decryption shall remain in force earlier for a period not exceeding 60 days from the date of its issue. The said direction may be renewed from time-to-time not exceeding the total period of 180 days. Further, the intermediaries have been mandated to provide all facilities, cooperation and assistance for interception, monitoring or decryption of information mentioned in the directions. Further, the intermediaries or any person in-charge of their computer resources are mandated to provide technical assistance and the equipment including hardware, software, firmware, storage, interface and access to the equipment, wherever requested by the agency who is authorized for performing interception or monitoring or decryption, including for the purposes of installation of equipment for such purposes, the maintenance testing and use of such equipment, the removal of such recruitment or the performance of any action required for accessing of stored information connected with the subject at-hand. Further, the Rules stipulate that there must be

destruction of records of interception, monitoring or decryption by the concerned security agencies in every six months except in such cases where such information is required or likely to be required for functional requirement purposes.

The Rules categorically stipulate in rule 24 that there is prohibition of interception, monitoring or decryption of information without authorization from the concerned competent authority. Further, rule 25 mandates that the contents of intercepted or monitored or stored or decrypt information shall not be used or disclosed by the intermediary or any of its employees or person in-charge of its computer systems or computer resources to any person other than the intended recipient of such information.

Some people see section 69 as an embodiment of Internet censorship in India.

It is also often argued that section 69 is amenable to tremendous abuse and there are no adequate checks and balances for the purposes of ensuring that the huge ambit of powers granted under section 69 are misused and abused.

Seen from another angle, section 69 of the Information Technology Act, 2000 has done away with the earlier requirements of the section to go through an independent statutory authority being the Controller of Certifying Authorities before interception could be ordered. Right now, the appropriate government can direct interception, monitoring or decryption of any information without the need for going to an independent authority in this regard.

It has also been pointed out that section 69 brings along with it, civil liberties concerns. Seen from one perspective, section 69 of the Information Technology Act, 2000 is far more intrusive than the Indian Telegraph Act, 1885. Thus, section 69 talks about any information generated, transmitted, received or stored in any computer resource. It refers to all data, message, text, images, sound, voice, codes in the electronic form, computer programmes, software and databases or micro film or computer generated microfiche. The net effect of the same is that the Government or a police officer would listen to any of your phone call communications, read your SMSes, e-mails and monitor your browsing behaviour, without the need for having permission from the Magistrate of the court of competent jurisdiction.

The scope of the amended section 69 of the Information Technology Act, 2000 is bigger and broader than the scope of the un-amended section 69. The earlier section 69 only talked about interception of information transmitted through any computer source. However, the amended section 69 talks about the powers of interception, monitoring, blocking and decryption of any information through any computer resource. Thus, all kinds of information and data in the electronic form either resident on or transmitted or sent from or received at any computer source in India becomes amenable to section 69 of the Information Technology Act, 2000. Further, section 69 of the amended Information Technology Act, 2000 broadens the scope of surveillance to include the investigation of any offence, whether cognizable or not. There are no adequate safeguards in place under section 69 of the Information Technology Act, 2000 and the potential of it being abused exists.

It can further be argued that section 69 of the Information Technology Act, 2000 infracts the fundamental right of privacy of a citizen and as such, it is violative of article 21 of the Constitution of India. To examine this aspect, it is

important to note the inherent character of interception or monitoring or decryption. Interception of electronic messages can be seen as constituting a form of telephone tapping. Also, it is important to note that the words "intercept any information" in section 69(1) of the IT Act, 2000 are somewhat similar to the process of telephone tapping. In both the processes, there is interception of information that is happening through different mediums. Thus, it would be prudent to examine whether telephone tapping would constitute a violation of right to privacy under article 21 of the Constitution of India.

The issue relating to telephone tapping by the Government under section 5(2) of the Telegraph Act came up in challenge before the Supreme Court in the famous case of *People's Union for Civil Liberties (PUCL)* v. *Union of India*.[58] In this case, the Supreme Court, after examining the International Covenant of Civil and Political Rights, the Universal Declaration of Human Rights and the provisions of various laws came to the conclusion that the right to privacy is an integral part of the right to life as enshrined under article 21 of the Constitution of India. In this case, Supreme Court has held:

> *"....Right to privacy is a part of the right to "life and personal liberty" enshrined under article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, article 21 is attracted. The said right cannot be curtailed 'except according to procedure established by law....The right to privacy – by itself – has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy". Conversations on the telephone are often of an intimate and confidential character. Telephone conversation is a part of modern man's life. It is considered so important that more and more people are carrying mobile telephone instruments in their pockets. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract article 21 of the Constitution of India unless it is permitted under the procedure established by law."*

Thus, it would follow that like telephone-tapping, interception of electronic information would infract article 21 of the Constitution of India unless it is permitted under the procedure established by law. Since section 69 of the Information Technology Act, 2000 provides for the procedure for interception of electronic information as established by law, section 69 would not infract Article 21 of the Constitution of India.

It is pertinent to note that section 5(2) of the Telegraph Act has the same five grounds for interception as are enumerated under section 69 of the Information Technology Act, 2000. In the same case being *PUCL* v. *Union of India*, it was further held as under:—

> *"....The first step under section 5(2) of the Act, therefore, on the occurrence of any public emergency or the existence of a public safety interest. Thereafter the*

58. (1997) 1 SCC 301: AIR 1997 SC 568: 1997 AIR SCW 113.

competent authority under section 5(2) of the Act is empowered to pass an order of interception after recording its satisfaction that it is necessary or expedient so to do in the interest of (i) sovereignty and integrity of India, (ii) the security of the State, (iii) friendly relations with foreign States, (iv) public order, or (v) for preventing incitement to the commission of an offence. When any of the five situations mentioned above to the satisfaction of the competent authority require, then the said authority may pass the order for interception of messages by recording reasons in writing for doing so.

Section 5(2) of the Act shows that so far the power to intercept messages/conversations is concerned, the section clearly lays down the situations/conditions under which it can be exercised. But the substantive law as laid down in section 5(2) of the Act must have procedural backing so that the exercise of power is fair and reasonable. The procedure itself must be just, fair and reasonable. "Procedure" must rule out anything arbitrary, freakish or bizarre. A valuable constitutional right can be canalized only by civilized processes."

Consequently, the Supreme Court issued various directions, which are even more relevant in the context of section 69 of the Information Technology Act, 2000. It is important to quote the guidelines issued by the Supreme Court in the matter:

"...In order to rule out arbitrariness in the exercise of power under section 5(2) of the Act and till the time the Central Government lays down just, fair and reasonable procedure under section 7(2)(b) of the Act, it is necessary to lay down procedural safeguards for the exercise of power under section 5(2) so that the right to privacy of a person is protected...

1. *An order for telephone-tapping in terms of section 5(2) of the Act shall not be issued except by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. In an urgent case the power may be delegated to an officer of the Home Department of the Government of India and the State Governments not below the rank of Joint Secretary. Copy of the order shall be sent to the Review Committee concerned within one week of the passing of the order.*
2. *The order shall require the person to whom it is addressed to intercept in the course of their transmission by means of a public telecommunication system, such communications as are described in the order. The order may also require the person to whom it is addressed to disclose the intercepted material to such persons and in such manner as are described in the order.*
3. *The matters to be taken into account in considering whether an order is necessary under section 5(2) of the Act shall include whether the information which is considered necessary to acquire could reasonably be acquired by other means.*
4. *The interception required under section 5(2) of the Act shall be the interception of such communications as are sent to or from one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications to or from, from one particular person specified or described in the order or one particular set of premises specified or described in the order.*
5. *The order under section 5(2) of the Act shall, unless renewed, cease to have effect at the end of the period of two months from the date of issue. The authority which issued the order may, at any time before the end of two-month period renew the order if it considers that it is necessary to continue the order in terms of section 5(2) of the Act. The total period for the operation of the order shall not exceed six months.*
6. *The authority which issued the order shall maintain the following records:*
   - *(a) the intercepted communications,*
   - *(b) the extent to which the material is disclosed.*
   - *(c) the number of persons and their identity to whom any of the material is disclosed.*
   - *(d) the extent to which the material is copied, and*
   - *(e) the number of copies made of any of the material.*
7. *The use of the intercepted material shall be limited to the minimum that is necessary in terms of section 5(2) of the Act.*
8. *Each copy made of any of the intercepted material shall be destroyed as soon as its retention is no longer necessary in terms of section 5(2) of the Act.*
9. *There shall be a Review Committee consisting of Cabinet Secretary, the Law Secretary and the Secretary, Telecommunication at the level of the Central Government. The Review Committee at the State level shall consist of Chief Secretary, Law Secretary and another member, other than the Home Secretary, appointed by the State Government.*
   - *(a) The committee shall on its own, within two months of the passing of the order by the authority concerned, investigate whether there is or has been a relevant order under section 5(2) of the Act. Where there is or has been an order, whether there has been any contravention of the provisions of section 5(2) of the Act.*
   - *(b) If on an investigation the Committee concludes that there has been a contravention of the provisions of section 5(2) of the Act, it shall set aside the order under scrutiny of the Committee. It shall further direct the destruction of the copies of the intercepted material.*
   - *(c) If on investigation, the Committee comes to the conclusion that there has been no contravention of the provisions of section 5(2) of the Act, it shall record the finding to that effect..."*

It is relevant to note that the aforesaid judgment has been delivered in the context of section 5(2) of the Indian Telegraph Act, 1885. Section 5(2) of the Indian Telegraph Act, 1885 provides that in the event of happening of any of the five conditions, also stipulated under section 69 of the Information Technology Act, 2000, the Central or State Governments have the power to direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order.

In the light of this scenario, and also the fact that computer penetration in the country is still at a low level, the blanket provision made under section 69 may

not be in sync with the reality. Is it fair to punish someone for failing to assist the intercepting agency on the ground of not extending all facilities and technical assistance for decrypting information, when the said subscriber or person does not have access to such facilities and technical assistance for decryption? Also, in the process, there is a danger of innocent persons being accused for an offence of not giving assistance to the interception agency, due to their economic inability or for reasons beyond their control. You cannot punish a man for not providing you with a facility that he does not have or cannot afford. It is incumbent upon the intercepting agency to take recourse to all technical assistance and facilities on its own for the purpose of decryption.

There would also be a problem under section 69(3) for the subscriber inasmuch as such offence violates the protection against self-incrimination, which has been guaranteed as a Fundamental Right under article 20(3) of the Constitution of India and section 161(2), Cr. P.C. Article 20(3) of the Constitution of India provides that no person accused of any offence shall be compelled to be a witness against himself. It is pertinent to note that article 20(3) of the Constitution uses the word "accused". However, it is not necessary that the actual trial should have commenced against a person or charges framed against him in order to claim protection against self-incrimination.

The Hon'ble Supreme Court in *Nandini Satpati* v. *P.L. Dani*,[59] held that the term "accused" used in article 20(3) of the Constitution of India and section 161(2) of the Cr. P.C. includes a suspect as well. The Court further held that the rule against self-incrimination is not restricted to the offence for which the accused is being interrogated, it extends to other offences also *qua* which the accused apprehends incrimination. Thus, section 69 creates an offence, which is *ultra vires* the protection against self-incrimination under article 20(3) from the Constitution of India and section 161(2) of the Cr. P.C.

It can also be argued that the kind of powers given for interception can violate the cause of an individual's freedom and privacy and that the same should not be allowed. There is a huge debate going on the same in the US, as there have been various heated arguments on the surveillance systems and Carnivore. It is yet to be ascertained as to how this particular section would be implemented in the times to come.

Further, such a provision under the law is likely to be potentially far more misused than any other specific provisions detailed under section 69 of the amended Information Technology Act, 2000.

It will be very important that the procedures and safeguards, subject to which such interception, monitoring or decryption may be carried out as referred to under section 69(2), apart from the ones detailed in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 be made, as far as possible, most comprehensive and detailed so as to potentially rule out any potential misuses of section 69 of the Information Technology Act, 2000. Further, the said procedures and safeguards need to be detailed, keeping in mind not just the requirements of national security

59. AIR 1978 SC 1025: 1978 Cr LJ 968: (1978) 2 SCC 424.

and sovereignty of India but also of the capacity and capability of the subscribers, intermediaries or persons in-charge of computer resources to extend all facilities and technical assistance to intercept, monitor or decrypt information, as the case may be.

The problem arises because of the usage of the words "all facilities and technical assistance" as detailed under section 69(3). The words "all facilities and technical assistance" is an absolute and all encompassing phrase, which does not admit of any exceptions.

Had the law talked about all available or reasonable facilities or technical assistance, then the situation may have been different. However, with the current law stipulating the need for the subscriber, intermediary or person in charge of computer resources to extend all facilities and technical assistance to intercept, monitor or decrypt information, there are going to be a lot of challenges, as one examines the practical implementation of section 69 in the times to come.

When one examines the public domain, one finds that there is hardly any reference to invocation of powers under section 69 of the Information Technology Act, 2000.

Seen from an overall perspective, section 69 represents a paradox of its kind. While there is an inherent right of Sovereign Government to have recourse to the powers of interception, blocking or monitoring so as to protect its sovereign interests, yet at the same time there is a need for ensuring that there is a balance between exercise of such powers and the protection and preservation of civil liberties and fundamental rights of citizens on the other hand. At no point of time, should these powers be made a basis for trammelling upon the civil liberties of citizens in circumstances. However as time passes by, there is increasing clarity that should there be a conflict between the inherent sovereign needs of the Sovereign Government to exercise its sovereign rights with the national interest with the enjoyment of civil liberties, national interests are invariably likely to take a higher level of priority.

A perusal of the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 also shows that there is scope for more improvement thereunder. There is need for ensuring that there are more adequate checks and balances to ensure that the power under section 69 of the Information Technology Act, 2000 is not abused or misused in any manner whatsoever.

The power under section 69 of the Information Technology Act, 2000 is also to be seen in the context of the powers given in the context of blocking for public access of information through any computer resource.

Section 69A – Power to Issue Directions for Blocking for Public Access of any Information through any Computer Resource

"(1) *Where the Central Government or any of its officer specially 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 also be liable to fine."

Section 69A has been added in the Information Technology Act, 2000 by the Information Technology (Amendment) Act, 2008. Section 69A is dedicated to this subject of issuing directions for blocking for public access of any information through any computer resource.

Earlier, the Information Technology Act, 2000 did not have specific power to direct blocking of information through any computer resource and the same was delegated to be exercised by Indian Computer Emergency Response Team (Indian Computer Emergency Response Team).

This is for the first time that blocking as a phenomenon has been addressed under the Information Technology Act, 2000. It may be pertinent to point out that in the Information Technology Act, 2000, blocking was not specifically mentioned. Consequently the Ministry of Information Technology, Department of Information Technology issued the Gazette Notification (Extraordinary) number G. S. R. 181 (E) dated 27th February, 2003. By means of the said notification, Computer Emergency Response Team of India (CERT-IN) had been designated as the single authority for issuance of instructions in the context of blocking of websites.

Thereafter, the Ministry of Communication and Information Technology, Department of Information Technology, Government of India also published another Gazette Notification bearing number G.S.R. 529 (E), dated 7th July, 2003 with the subject "Procedure for Blocking of Websites". By means of the said gazette notification, the detailed procedure for blocking of website was laid down.

The said procedure of blocking of websites was resorted to from 2003 onwards for a variety of purposes and circumstances. However, the Legislature felt that there was a need for providing for specific legislative provisions on blocking. Consequently, section 69A was inserted in the Information Technology Act, 2000.

By virtue of section 69A, the power to issue directions for blocking for public access of any information through any computer resource, has now been specifically stipulated in the hands of the Central Government or any of its officers specially authorized by it in this behalf. Thus, by virtue of section 69A, the provisions of this section have precedence over the notifications dated 27th February, 2003 and 7th July, 2003.

However as time has passed by, it is being felt by the Governments that there is an increasing need to give inherent powers to the Government to direct blocking for public access of any information through any computer resource. In this

context, section 69A has been inserted into the Information Technology Act, 2000.

A perusal of the said section clearly shows that the term "blocking" or "block for access" has not been defined either under section 69A of the Information Technology Act, 2000 or under section 2 of the Information Technology Act, 2000.

As per the online dictionary, **"Blocking"** means 1. The action or process of obstructing movement, progress, or activity, in particular. 2. Obstructing or impeding the actions of an opponent in a game, esp. (in ball sports) one who does not have control of the ball.

According to the Oxford dictionaries, blocking means the action of blocking or obstructing someone or something, in particular; and the grouping or treatment of things (*e.g.*, shades of colour) in blocks.

When one examines section 69A, one realizes that while the powers under section 69A have been conferred both on the Central and State Governments, the power to issue directions for blocking for public access of any information through any computer resource can only be exercised by the Central Government or by any of its officers specially authorized by it in this regard. The power under section 69A can only be exercised if the Central Government or any of its officers are satisfied that it is necessary or expedient to give directions for blocking for public access of any information through any computer resource on certain stipulated grounds as detailed below:

(a) In the interest of sovereignty of India;
(b) In the interest of integrity of India;
(c) In the interest of defence of the State;
(d) In the interest of security of the State;
(e) In the interest of friendly relations with foreign States;
(f) In the interest of public order; or
(g) For preventing incitement to the commission of any cognizable offence relating to the above.

The Central Government, if satisfied that any of the above conditions exist, has been given the discretion to direct any agency of the government or intermediary to block for access by the public any specific information, which is generated, transmitted, received, stored or hosted in any computer resource. The power also includes the power to direct the causing to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer source. Section 69A categorically provides that the power can only be exercised after the reasons are recorded in writing for the exercise of such powers. Further exercise of such powers are subject to provisions of section 69A(2).

Section 69A(2) provides that blocking for access by the public may be carried out subject to certain procedures or safeguards which shall be such as may be prescribed.

It is pertinent to note that the Government has notified the Information Technology (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

These Rules have specifically stipulated that the Central Government shall designate, by notification in the Official Gazette, an officer of the Central Government not below the rank of a Joint Secretary as the designated officer for the purposes of issuing directions for blocking for access by the public any information generated, transmitted, received, stored or hosted in any computer resource, as detailed under section 69A of the Information Technology Act, 2000.

The Rules stipulate that every organization, for the purposes of these Rules, have to mandatorily designate one of its officers as the Nodal Officer. The designated officer of the Government, either on receipt of the request form Nodal Officer of an organization or competent court, will, by order direct any agency of the Government or intermediary to block for access by the public any information or part thereof which is generated, transmitted, received, stored or hosted in any of the computer resource, as per section 69A(1).

The Rules further provide for the process to be followed in the event of blocking of information in cases of emergency. In a case of emergency nature, the Secretary, Department of Information Technology has been given the discretion that he may as an interim measure, issue directions to any identified or identifiable person or intermediaries in control of relevant computer resources, hosting such information or a part thereof, without giving them an opportunity of being heard. Further, all intermediaries are mandated that they shall designate at least one person to receive or handle the directions for blocking of access by the public, any information generated, transmitted, received, stored or hosted in any computer resource under these Rules. The designated officer is further mandated to maintain complete records of the request received and action taken care thereof in its electronic databases and also in register of the cases of blocking for public access of information generated, transmitted, received, stored or hosted in a computer resource.

The Government has felt that the directions for blocking for public access of any information through any computer source is a serious matter. As such, any intermediary who fails to comply with the directions issued under section 69A(1), commits a serious offence under section 69A (3) of the Information Technology Act, 2000. The said offence is punishable for a term which may extend to 7 years and shall also be liable to fine. Thus, the intermediaries have been exposed to criminal penalty for the purposes of ensuring that they strictly follow all directions for blocking for public access of any information, through any computer resource in India.

In my opinion, while blocking is an important ammunition in the arsenal of any Sovereign Government, in today's context of *ubiquitous* computing and the social media adoption, blocking today has become an irrelevant phenomenon. This is so because given the intrinsic nature and architecture of the Internet, it is possible to access any blocked website, using proxy servers and variety of highly sophisticated free tools available on the Internet. As such, blocking doesn't *per se* help in any material purposes. On the other hand, blocking of any website tends to give far more Internet traffic and exposure to the blocked website.

History has been witnessed to the fact that whenever Indian Government has apparently blocked any website, the said websites have generated far more Internet

traffic. The examples of the Kyn Hun Yahoo group banned by the Government of India and also the banning of the savitabhabhi.com website are classical examples in this regard. Further, given the inherent nature, architecture and character of the Internet, it is always possible to go and access the said information or website that is blocked from indirect means. Further, it needs to be appreciated that blocking of any website at best is only a phenomenon that is effective within the territorial boundaries of India. The same does not apply to any Internet Service Providers or Intermediaries which are located outside the physical boundaries of India.

Further, the Government stepped up its efforts to stop an online campaign of mis-information and rumour-mongering in the wake of lower Assam riots and ordered blocking of 16 Twitter accounts, including two belonging to journalists,

The Department of Telecommunications (DoT) ordered blocking of the accounts on August, 20. The blocked accounts included those maintained by a columnist and a journalist working for a TV channel. According to the leaked list, Indian Government also blocked 30 Twitter URLs, 3 Wikipedia URLs, 11 Blogger URLs and 8 Wordpress URLs. Some URLs belong to Pakistani websites. The list also contained URLs belonging to several mainstream media websites, including The Telegraph and Al Jazeera.[60]

India has seen various websites being blocked on orders passed by different courts. In May, 2012, a number of websites including Vimeo, Privacybay, Torrent and other Torrents websites were blocked on orders received from the Department of Telecommunications. In April, 2012, the Madras High Court had passed John Doe orders concerning certain websites. In June, 2012, the Madras High Court had clarified that the entire websites could not be blocked under the garb of John Doe order and only the offending pages of the website need to be blocked.

It has been held in the landmark case of *Secretary, Ministry of Information & Broadcasting* v. *Cricket Association of Bengal*, that the right to freedom of speech and expression under article 19 of the Constitution includes the right to receive and impart information irrespective of the medium and it has been argued that Internet is a medium for disseminating information and that when websites are blocked, users of the Internet would be prejudicially impacted in terms of their ability to access such information and that such blocking would directly infringe the citizens' freedom of speech and expression.

Section 69A(3) creates a new offence. The intermediary, who fails to comply with the directions of blocking as given under section 69A of the Information Technology Act, 2000, commits an offence. The said offence is punishable with imprisonment for a term which may extend to 7 years and shall also be liable to fine. Thus, a very serious, heinous crime has been created by section 69A(3). It will be the mandatory responsibility of the intermediary, once directed to block for access by the public or cause to be blocked for access by the public, any information, to ensure that the said information be blocked forthwith. Failure to comply with the direction of blocking will invite imprisonment for a term which would extend to 7 years as also to fine. Needless to say, if the intermediary is a

60. http://articles.timesofindia.indiatimes.com/2012-08-24/internet/33365347_1_twitter-accounts-twitter-users-assam

company, the provisions of section 85 of the Information Technology Act, 2000 shall come into force. If the offences under section 69A(3) is committed by a company, every person, who at the time the contravention was committed, was in-charge of and was responsible to the intermediary company for the conduct of the business of the company as well as the intermediary company, shall be guilty of the said contravention and shall be liable to be proceeded against and punished accordingly.

Section 69A provides an important tool in the arsenal of the Government to deal with undesirable information which is generated, transmitted, received, stored and hosted in any computer resource in India. The said power shall be an important power for assisting the Government of India in meeting various challenges, as time passes.

Seen from another angle, portions of Information Technology (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009 are violative of article 14 of the Constitution as they do not, give any reasonable opportunity of being heard to the website, that is about to be blocked. Further, the Rules are silent as to what remedies need to be invoked by the owners or administrators or operators of the blocked websites to ensure that their blocked websites could become unblocked. The Information Technology (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009 need to be re-visited so as to make them far more equitable and fair. Also given the fact that the blocking at the maximum can only be done upto 180 days, there have been instances reported in the public domain, where number of websites have been blocked for a longer period of time. There is a need for re-visiting the section, provisions and the rules made thereunder so as to ensure that principles of natural justice, good conscience and equity are not subjugated under the garb of exercising of the right and power to give directions for blocking for public access of any information through any computer resource.

One of the inherent problems under section 69A is that it does not seek to provide any remedy to the concerned owners or administrators or operators of websites whose websites are blocked under section 69A. The only option that is available to the aggrieved persons is to approach the High Court in its writ jurisdiction challenging the order of the concerned competent authority. However, the same could take a lot of time and as such, the process of unblocking of websites does not have an adequate efficacious remedy in this regard. This becomes all the more relevant, since an order under section 69A is not capable of being challenged in the Cyber Appellate Tribunal.

History has also witnessed the fact that inadvertently sometimes, sites are incorrectly blocked and unblocking of an incorrectly blocked website could also take a couple of months which could cause huge amount of damage and irreparable loss and injury to the owners and operators of the said websites and also to the entire public, given their intrinsic right to access the Internet.

Privacy advocates have further argued that there is no provision in place to deal with a scenario when there is a clear nexus between an intermediary and information or resource sought to be monitored or intercepted. Another criticism

of the Rules under section 69 is that Rules have provided for the concept of sharing of information with concerned agencies.

As such, the efficacy of blocking any specific information needs to be re-assessed and re-examined. However, nonetheless it can still be stated that the power to block and the consequent blocking of information generated, transmitted, received, stored or hosted in any computer resource, still is an important significant, power in the weaponry of any sovereign nation in its fight against the challenges raised by undesirable information generated, transmitted, received, stored or hosted in any computer resource.

Section 69B – Power to Authorize to Monitor and Collect Traffic Data or Information through any Computer Resource for Cyber Security

"(1) *The Central Government may, to enhance cyber security and for identification, analysis and prevention of 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 punished with an imprisonment for a term which mayextend 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, data, size, duration or type of underlying service and any other information."*

Section 69B has been added in the Information Technology Act, 2000 by the Information Technology (Amendment) Act, 2008. Section 69B has been added for the purposes of enhancing cyber security of India and for the purposes of identification, analysis and prevention of intrusion or spread of computer contaminants in the country.

Section 69B refers to the concept of "traffic data" and its monitoring and collection. It is pertinent to point out that the concept of cyber security has been defined for the first time in the Information Technology Act, 2000 by virtue of section 2(1)(nb), which have been inserted by the 2008 amendments. Section 2(1)(nb) defines cyber security to mean protecting information, equipment, devices,

computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

For the purposes of enhancing cyber security and for the purposes of identification, analysis and prevention of intrusion or spread of computer contaminants or virii in the country, section 69B has given a discretionary power to the Government. This power includes the power to authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. This power can only be exercised by notification in the Official Gazette.

It is pertinent to point out that the term "traffic data" has been defined by *Explanation (ii)* to section 69B of the Information Technology Act, 2000 in very vast terms. *Explanation (ii)* to section 69B clearly gives a definition of the term "traffic data". As per the said explanation, "traffic data" basically means any data which:

(a) Is identifying any person, computer system or computer network or location to or from which the communication is or may be transmitted;

(b) Any data which is purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted.

Traffic data is a vast ocean which includes any data which either identifies or being purports to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted. The followings kinds of data parameters have been classified to be included within the ambit of the definition of the term "traffic data":

(a) Communications origin;

(b) Destination;

(c) Route;

(d) Time;

(e) Data;

(f) Size;

(g) Duration;

(h) Type of underlying service; or

(i) Any other information.

Thus, all information pertaining to Internet Protocol Addresses, computer logs and information which can throw light on the way the data or information in the electronic form is generated, transmitted, sent, received or stored or forwarded, would thus qualify as "traffic data".

Further, the term "Traffic data" has been defined by Online Dictionary as any computer data or other data relating to a communication by means of a computer program, computer, computer system, or network, generated by a computer program, computer, computer system, or network that form a part in the chain of communication, indicating the communication's origin, destination, route, format,

intent, time, date, size, duration, or type of underlying service. Traffic data includes packet headers, pen register and trap and trace data.[61]

The UK's Privacy and Electronic Communications Regulations defines the term "Traffic data" to mean any data which is processed:

- to convey a communication on an electronic communications network; or
- for the billing in respect of that communication ('billing data' under the Telecommunications (Data Protection and Privacy) Regulations, 1999).

It includes data relating to the routing, duration or time of a communication.[62]

Council of Europe's Convention on Cybercrime has underlined its treaty position relating to traffic data in the following term:

"Article 1(d) – Traffic data

28. For the purposes of this Convention traffic data as defined in article 1, under sub-paragraph d., is a category of computer data that is subject to a specific legal regime. This data is generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself.

29. In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive.

30. The definition lists exhaustively the categories of traffic data that are treated by a specific regime in this Convention: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service. Not all of these categories will always be technically available, capable of being produced by a service provider, or necessary for a particular criminal investigation. The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. The "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used within the network, e.g., file transfer, electronic mail, or instant messaging.

31. The definition leaves to national legislatures the ability to introduce differentiation in the legal protection of traffic data in accordance with its sensitivity. In this context, article 15 obliges the Parties to provide for conditions and safeguards that are adequate for protection of human rights and liberties. This implies, inter alia,

61. http://itlaw.wikia.com/wiki/Traffic_data.

62. http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/traffic_data.aspx

that the substantive criteria and the procedure to apply an investigative power may vary according to the sensitivity of the data."

The aforesaid treaty position, as detailed in Council of Europe's Convention on Cybercrimes, elaborates the concept of "traffic data" and how the same may be dealt with, by national Legislations, of nations who are signatories of the said Convention on Cybercrimes.

Thus, the concept of "traffic data" is all encompassing and includes all kinds of data which is used either for identifying or to identify any specific person, computer system or computer network. Such traffic data is further used to identify any location to or from which, the communication is or may be transmitted. The significance of traffic data for protecting the sovereignty and integrity of any nation, can hardly be overestimated. Traffic data gives the vital signals and information to the law enforcement agencies, who are investigating various contraventions and challenges to national security and cybersecurity of any nation. In the context of India, traffic data assumes tremendous significance, given the challenges to national security and cyber security that India is currently facing. Over the last few years, India has seen various amounts of criminal activities and attacks which are targeted at not just undermining the sovereignty and integrity of India as also the security of the State and friendly relations with other nations. Further, such attacks on Indian national security and cyber security are aimed to destabilize the nation and further negatively impact public order.

Thus, in order to meet the challenges raised by cyber criminals and cyber terrorists, law enforcement agencies require traffic data for the purposes of not just proactively taking steps to protect the national security and cyber security of India but also to specifically rely upon them in instances where cyber crimes and crimes against nations, are being investigated against cyber criminals and cyber terrorists.

In that particular scenario, traffic data assumes tremendous significance since that is the crucial and relevant link through which, the concerned cyber criminal/ cyber terrorist is linked to the crime.

It is pertinent to note that the earlier Information Technology Act, 2000 did not talk anything about traffic data. However, the concept of traffic data has been taken by India from the Council of Europe's Convention on Cyber Crime where such concept has been more elaborately detailed.

Section 69B of the amended Information Technology Act, 2000 gives the discretion to Central Government to notify in the Official Gazette and authorize any agency of the Government, to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. The said discretion can be exercised to enhance cyber security of India as also for identification, analysis and prevention of intrusion or spread of computer contaminants in the country.

Thus, the focus of the power under section 69B(1) is to authorize any agency of the Government to monitor or collect traffic data or information. The said traffic data becomes extremely relevant for the purposes of identifying origins of any electronic data or information messages, computer contaminant or other malicious programs or spyware or executable files and such traffic data when monitored, can

effectively help the Indian Government to ensure that it can take steps to protect and preserve its cyber security.

Given the fact that traffic data is often in the possession of either intermediary or any other person in-charge of its computer resource, sections 69B(2) provides mandatory duties to be fulfilled by the intermediary or any other person in-charge of the computer resource in this regard. Whenever the agency authorized under section 69B(1) calls upon the intermediary or any other person in-charge of the computer resource to do so, the intermediary or the said person in-charge are mandated to provide technical assistance and extend all facilities to such agency. The said technical assistance and extension of facilities must be to enable the activities of the said stipulated agency to have online access or to secure and provide online access to the computer resource which is generating, transmitting, receiving or storing such traffic data or information. The monitoring and collecting of traffic data has to be subject to certain procedures and safeguards, which shall be such as may be prescribed.

The said agency of the Government, which is so authorized by the Central Government, has been given the powers to call upon any legal entity in India to provide technical assistance pertaining to monitoring and collection of traffic data or information generated, transmitted, received or stored in a computer resource. Further, the said agency has been given the powers to call upon any person in-charge of a computer resource or any intermediary to extend all facilities to such agency for the following purposes:

(a) To enable online access, or
(b) To secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

It is pertinent to note that the Central Government has notified the Information Technology (Procedures and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009. The said Rules have defined the competent authority to mean the Secretary to the Government of India in the Department of Information Technology under the Ministry of Communications and Information Technology. The said Secretary has been authorized to give directions for monitoring and collection of traffic data under section 69B of the Information Technology Act, 2000. The Secretary, Department of Information Technology, Ministry of Communications & Information Technology has been further empowered to issue directions for monitoring of traffic data or information for all or any of the following purposes relating to cyber security detailed in the paragraph below:

Rule 3(2) of the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009 has given the parameters when the competent authority issues direction for monitoring. Rule 3(2) reads thus:—

"Rule 3(2) The competent authority may issue direction for monitoring for any or all of the following purposes related to cyber security, namely:

(a) forecasting of imminent cyber incident

(b) monitoring network application with traffic data or information on computer resource;

(c) *identification and determination of viruses or computer contaminant;*

(d) *tracking cyber security breaches or cyber security incidents;*

(e) *tracking computer resource breaching cyber security or spreading virus or computer contaminants;*

(f) *identifying and Tracking of any person who has breached, or is suspected of having breached or being likely to breach cyber security;*

(g) *undertaking forensic of the concerned computer resource as a part of investigation or internal audit of the information security practices in the computer resource;*

(h) *accessing stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force;*

(i) *any other matter relating to cyber security."*

The intermediaries or person in-charge of computer resources are mandated by means of the said Rules to put in place adequate and effective internal checks to ensure that unauthorised monitoring or collection of traffic data or information does not take place. Further, such intermediaries or person in-charge of the computer resources have to ensure that they have internal mechanisms to maintain secrecy, utmost care and precaution in the matter of monitoring and collection of traffic data and information as it affects privacy of citizens.

Rule 9 of the Information Technology (Procedures and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009, specifically prohibit monitoring or collection of traffic data or information, without authorization from the concerned competent authority. Further, the agency authorized to collect or monitor traffic data or information is mandated not to use or disclose the details of monitored or collected traffic data for any purpose, except for forecasting imminent cyber threats or general trend of port wise traffic on Internet or general analysis of cyber incidents or for investigation or in judicial proceedings before the competent court in India.

Given the intrinsic nature of collecting and monitoring traffic data, the Rules stipulate that strict confidentiality shall be maintained in respect of directions for monitoring or collection of traffic data or information issued by the competent authority.

Further, the said Rules mandate that the records including electronic records pertaining to directions for monitoring or collection of traffic data shall be destroyed after the period of 9 months from the date of receipt of direction or creation of record, whichever is later. However, such record will be kept for a longer period than 9 months, where traffic data or information is or is likely to be required for functional requirements.

The law has sought to ensure that directions for monitoring and collecting traffic data or information are studiously complied with by all intermediaries. Any intermediary who intentionally or knowingly fails to provide technical assistance and extend all facilities to the authorized 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, commits a serious offence. The said offence is punishable under section 69B(4) of the

Information Technology Act, 2000 and is punishable with imprisonment for a term which may extend to 3 years and shall also be liable to fine.

The *Explanation (i)* to section 69B provides that the term "computer contaminant" shall have the same meaning as is assigned to it by section 43 of the Information Technology Act, 2000. *Explanation (i)* to section 43 of the Information Technology Act, 2000 provides that computer contaminant means:

(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."*

Thus, seen holistically, section 69, 69A and 69B together represent a bundle of the processes that have been specifically now enshrined in the Indian IT law for the purposes of effectively strengthening the hands of the Government not only to help protect and preserve the security, sovereignty and integrity of India but also for the purposes of protection and preservation of cyber security in India. Contraventions of section 69, 69A and 69B are of a serious nature and imprisonment ranging from three years to 7 years has been stipulated in case if any intermediary or person in-charge of any computer, computer system, computer network or computer resource commits any of the offence as detailed under section 69(4), 69A(3) and 69B(4) of the Information Technology Act, 2000.

The said powers are hoped to further help and strengthen the hands of the Indian Government in its fight against cyber terrorism and further giving the direction of ensuring that its computers, computer systems, computer networks and computer resources are not misused to prejudicially impact Indian nation, its citizens and its sovereign interests, both in the physical world as also in cyberspace.

It is pertinent to note that Group of Experts on privacy constituted by Planning Commission, Government of India under the Chairmanship of Justice Ajit Prakash Shah, Former Chief Justice, Delhi High Court specifically recommends as follows:—

"At the moment, interception/access in India is addressed in two legislations, the Telegraph Act and the Information Technology Act. Each Act prescribes varying standards and procedures for interception through Rules, thus, creating similarities and differences in the Indian interception regimes.

Broad similarities between the regimes include: authorization for interception must be based on executive orders, orders for interception must be reviewed by an overseeing committee, all interception orders must contain similar specified information, and every agency intercepting communications must establish similar procedures for oversight and security of the interception. Differences range from the permitted grounds for surveillance, the type of interception that is permitted to be undertaken (monitoring, tracking, intercepting etc.), the type and granularity of information that can be intercepted, the degree of assistance that authorized agencies

can demand from service providers, and the destruction and retention requirements of intercepted material. These differences have created an unclear regulatory regime that is non-transparent, prone to misuse, and that does not provide remedy for aggrieved individuals. By requiring that each legislation be in compliance with the National Privacy Principles, the Principles should be used to harmonize the interception regime in India."

The said Committee have further stressed that intermediaries must be mandated to provide an internal check to ensure the security, confidentiality and privacy of intercepted material and intermediaries should be held legally responsible for any unauthorised access or disclosure of intercepted materials.

Section 70 – Protected System

"(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation.—*For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.*

(2) The appropriate Government may, by order in writing, 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."

The language of section 70 has been substituted by virtue of the Information Technology (Amendment) Act, 2008.

Section 70 deals with the concept of protected system. Section 70 provides that any computer, computer system or computer network may be declared to be a protected system by the appropriate Government, by necessary notification. The notification may be published in the Official Gazette as well as in the electronic gazette within the meaning of section 8 of the Information Technology Act, 2000.

The word "protected system" is not defined in the Information Technology Act 2000. Even section 2 pertaining to Definitions does not define the protected system. However as is evident from the words, protected system would refer to a system that stands protected by law.

As per section 70(1), discretion has been granted to appropriate governments, whether it be the Central Government or the State Governments, to declare any computer resource as a protected system. The said discretion can be exercised as the appropriate Government so deems it necessary so to do. Of course, the said discretion has to be exercised by appropriate notification in the Official Gazette.

The appropriate governments have been given the power to declare the following kinds of computer resources to be a protected system:

(a) Any computer resource which directly affects the facility of Critical Information Infrastructure; or

(b) Any computer resource which indirectly affects the facility of Critical Information Infrastructure.

Hence, the crucial ingredient in section 70(1) is that the relevant computer resource must directly or indirectly affect the facility of Critical Information Infrastructure before it can be quantified and declared as a protected system.

The *Explanation* to section 70(1) gives the meaning of the term "Critical Information Infrastructure". The said *Explanation* defines the term "Critical Information Infrastructure" being the computer resource whose incapacitation or destruction shall have a mandatory debilitating impact upon any of the following:

(a) National security;

(b) Economy;

(c) Public health; or

(d) Safety

The term "computer resource" is defined under section 2(1)(k) of the amended Information Technology Act, 2000, to mean computer, computer system, computer network, data, computer database or software.

It is pertinent to note that *Explanation* does not give any definitions of the terms "national security", "economy", "public health" or "safety". Even the Information Technology Act, 2000 in its Definition clause does not give any definitions for these parameters detailed under section 70(1).

Since the said words are not being defined, it is imperative to see how the words are defined in the public domain.

Definition of National Security

Wikipedia gives a good *Explanation* of "National Security".

The 1996 definition propagated by the National Defence College of India accretes the elements of national power:

"National security is an appropriate and aggressive blend of political resilience and maturity, human resources, economic structure and capacity, technological competence, industrial base and availability of natural resources and finally the military might."

Harold Brown, U.S. Secretary of Defence from 1977 to 1981 in the Carter administration, enlarged the definition of national security by including elements such as economic and environmental security:

"National security then is the ability to preserve the nation's physical integrity and territory; to maintain its economic relations with the rest of the world on reasonable terms; to preserve its nature, institution, and governance from disruption from outside; and to control its borders."

In Harvard history Professor Charles Maier's definition of 1990, national security is defined through the lens of national power:

> *"National security... is best described as a capacity to control those domestic and foreign conditions that the public opinion of a given community believes necessary to enjoy its own self-determination or autonomy, prosperity and wellbeing."*

Macmillan Dictionary (online version), defines the term as *"the protection or the safety of a country's secrets and its citizens"* emphasising the overall security of a nation and a nation State.

Walter Lippmann, in 1943, defined it in terms of war saying that *"a nation has security when it does not have to sacrifice its legitimate interests to avoid war, and is able, if challenged, to maintain them by war".*[63]

Definition of Economy

As per Wikipedia the English words "economy" and "economics" can be traced back to the Greek words. The first recorded sense of the word "economy" is in the phrase "the management of economic affairs", but later is recorded in more general senses, including "thrift" and "administration". The most frequently used current sense, denoting "the economic system of a country or an area", seems not to have developed until the 19th or 20th century.

An economy consists of the economic systems of a country or other area; the labour, capital, and land resources; and the manufacturing, production, trade, distribution, and consumption of goods and services of that area.[64]

Economy refers to the large set of inter-related economic production and consumption activities which aid in determining how scarce resources are allocated.[65]

Definition of Public Health or Safety

In *Romesh Thappar* v. *The State of Madras,* AIR 1950 SC 124: 1950 SCR 594, the Supreme Court of India held as follows:

> *"Public safety" ordinarily means security of the public or their freedom from danger. In that sense, anything which tends to prevent dangers to public health may also be regarded as securing public safety. The meaning of the expression must, however, vary according to the context. In the classification of offences in the Indian Penal Code, for instance, Chapter XIV enumerates the "offences affecting the public health, safety, convenience, decency, and morals" and it includes rash driving or riding on a public way (section 279) and rash navigation of a vessel (section 280), among others, as offences against public safety, while Chapter VI lists waging war against the Queen (section 121), sedition (section 124A) etc. as "offences against the State", because they are calculated to undermine or affect the security of the State, and Chapter VIII defines "offences against the public tranquillity" which include unlawful assembly (section 141) rioting (section 146), promoting enmity between classes (section 153A), affray (section 159) etc. Although in the context of a statute*

63. http://en.wikipedia.org/wiki/National_security
64. http://en.wikipedia.org/wiki/Economy
65. http://www.investopedia.com/terms/e/economy.asp#axzz2FAgobhO0

> *relating to law and order "securing public safety" may not include the securing of public health, it may well mean securing the public against rash driving on a public way and the like, and not necessarily the security of the State. It was said that an enactment which provided for drastic remedies like preventive detention and ban on newspapers must be taken to relate to matters affecting the security of the State rather than trivial offences like rash driving, or an affray. But whatever ends the impugned Act may have been intended to subserve, and whatever aims its framers may have had in view, its application and scope cannot, in the absence of limiting words in the statute itself, be restricted to those aggravated forms of prejudicial activity which are calculated to endanger the security of the State. Nor is there any guarantee that those authorized to exercise the powers under the Act will in using them discriminate between those who act prejudicially to the security of the State and those who do not."*

Thus, seen from a holistic perspective, the Governments have been given the power to declare any computer resource as a protected system whose destruction or incapacitation directly or indirectly or prejudicially impacts, in a debilitating manner, India's national security, economy, public health or safety.

The concept of protected system assumes all the more significance given the attacks on Estonia in the year 2007.

Cyberattacks on Estonia refers to a series of cyber attacks that began 27 April, 2007 and swamped websites of Estonian organizations, including Estonian Parliament, banks, Ministries, newspapers and broadcasters, amid the country's row with Russia about the relocation of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn. Most of the attacks that had influence on the general public were distributed denial of service type attacks ranging from single individuals using various methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred.[66]

In the year 2007, the Critical Information Infrastructure of Estonia was hacked and economy was virtually paralyzed. As such it becomes imperative for every sovereign nation to designate certain Critical Information Infrastructure as its protected systems.

Further under section 70(2), the appropriate Governments, whether it be the Central Government or State Governments, have been given the discretion to further authorize the persons who are authorized to access the protected systems declared under section 70(1). This authorization has to be by means of a written order. Thus, the net effect of section 70(1) and (2) is that only people who are authorized to access the projected system, are entitled to access the protected system. Any other person who attempts to access or secures access to the protected system commits an offence.

Section 70(3) defines a new offence. This offence is committed when any person secures access or attempts to secure access to a protected system in

66. http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

contravention of section 70 of the Information Technology Act, 2000. Given the fact that the protected systems are critical for national security and economy, this has been made serious heinous crime. The offence under section 70(3) is punishable with imprisonment of either description for a term which may extend to 10 years and shall also be liable to fine.

Further as per section 70(4), the Central Government has been mandated to prescribe the following for such notified protected systems:—

(a) information security practices concerning such protected systems; and

(b) information security procedures concerning such protected systems.

The concept of protected system has come for some legal analysis.

The Government of Kerala issued a notification under section 70 of the Information Technology Act, 2000 (IT Act) declaring the FRIENDS application software as a protected system. In connection with that, litigation arose known as *Firos* v. *State of Kerala*, AIR 2006 Ker 279: 2006 (3) KLT 210. In the said litigation which was decided by the Kerala High Court, it was held as under:

> *"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 for 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/ Organisations.*
>
> *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. P10 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. P10 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."*

The matter is currently subjudice as the judgment of the Kerala High Court has been challenged in the Supreme Court of India.

Thus seen from a holistic perspective, section 70 provides for the protection and preservation of Critical Information Infrastructure of India by empowering the Governments to notify critical computer resource as protected systems. Further, so much significance is attached to the concept of protected system by the law that the law not only penalizes the act of securing access to the computer system without authorization as an offence under section 70 of the Information Technology Act, 2000; but it further penalizes any attempt to secure access to a protected system in contravention of section 70 of the Information Technology Act, 2000. Further given the fact that imprisonment upto 10 years is accorded for an offence under section 70(3), the present provision hopes to further strengthen the hands of the Governments in protecting and making secure Critical Information Infrastructure and further hopes to protect security of governmental networks and computer resources and information which have a direct effect on the sovereignty, integrity of India, security of State, friendly relations with other nations, public order, decency, morality.

Also in today's context, where information and data have a strong influence on societies, nations and economies, maintaining the sanctity of protected systems, having invaluable data, has become a critical priority for any nation. Indian Legislature has recognized the imminent danger to these protected systems and has thus enacted the section 70 of the Information Technology Act, 2000.

It is also interesting to note that this offence does not necessitate the existence of an intention or *mens rea*. Any person securing access or attempting to secure access, even unintentionally or accidentally, would be liable for conviction under section 70 of the Information Technology Act, 2000. Thus, an intentional or an accidental access, or attempt to secure access, to a protected system gets punished under the same terms.

What is of importance is how do we define the words "attempts to secure access to a protected system"? The quantum of proof that would be required to prove attempt is not clear. Also what would constitute "attempt to secure access" is not clear and would depend upon the facts and circumstances of each case. Would it be a mere step taken that would constitute an attempt or does it have to be a series of steps, which would constitute attempt? The law on the subject is yet to develop.

At the time of writing, not many instances have come forward where Governments in India have proactively declared any of its Critical Information Infrastructure as protected systems. However as time passes by, it will become increasingly imperative for the Governments to declare their Critical Information Infrastructure as protected. Even otherwise, from a strategic and legal perspective, it makes perfect legal strategy for the appropriate government to declare their Critical Information Infrastructure as protected systems.

Section 70A – National Nodal Agency

"(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.

(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."

Since, computer resources infrastructure including computers, computer systems, computer networks and communication devices are important critical aspects for not just the security and stability of India but also for the purposes of Indian economy and all sectors and communication, the Central Government has decided to come up with the concept of a National Nodal Agency. By means of the amendments to the Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008, the Central Government has created the concept of a National Nodal Agency. The said Nodal Agency shall be with respect to critical information infrastructure protection. Under section 70A, the Central Government has reserved upon itself, the discretion to notify, by publishing in the Official Gazette, any organization of the Government to be the National Nodal Agency in respect of critical information infrastructure protection.

The said agency shall be responsible for all aspects for the protection, preservation and security of the national critical information infrastructure. This will be such critical information infrastructure, which is critical for the country as a whole and also for its various sovereign functions. The said National Nodal Agency shall be responsible for all steps, measures and acts that need to be done or taken relating to protection of critical information infrastructure of India. The said Nodal Agency has also been burdened with the responsibility of ensuring research and development in respect of critical information infrastructure. The Central Government has further reserved upon itself, the power to prescribe the manner of performing, functions and duties of the said National Nodal Agency.

Considering the fact that today computer networks are extremely relevant for the purposes of communication and also form the lifeline of Indian economy, protecting computer networks and related infrastructure pertaining to the same would be a bigger priority for any Government and India is no exception. As such, the concept of National Nodal Agency in the perspective of computer networks as critical information infrastructure of India, becomes all the more relevant.

Section 70B – Indian Computer Emergency Response Team to Serve as National Agency for Incident Response

"(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 white papers relating to information security practices, procedures, prevention, 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.

(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 authorized in this behalf by the agency referred to in sub-section (1)."

Section 70B has been added in the Information Technology Act, 2000 by virtue of the Information Technology (Amendment) Act, 2008. Section 70B is dedicated to the Indian Computer Emergency Response Team (Indian Computer Emergency Response Team) as also its functions, duties and connected issues and offences.

As the title of section 70B states, the Indian Computer Emergency Response Team shall serve as the national agency for incident response.

As per section 70B(1), the Central Government has been mandated that it shall appoint an agency of the Government to be called as the Indian Computer Emergency Response Team. The said appointment shall only be by means of notification in the Official Gazette.

Section 70B(2) mandates that the Central Government shall mandatorily provide Indian Computer Emergency Response Team, the Director-General and such other officers and employees as may be prescribed. Further, section 70B(3) stipulates that the salary and allowances and terms and conditions of the Director-General and other Indian Computer Emergency Response Team officers and employees may be prescribed by the Government.

Section 70B(4) is possibly one of the most significant provisions under section 70B. Section 70B(4) mandates that the Indian Computer Emergency Response Team (Indian Computer Emergency Response Team) shall serve as India's National Agency in the area of cyber security. Further, Indian Computer Emergency Response Team has been designated as the National Agency for performing various functions as stipulated under section 70B(4)(a) to (f). Thus, it shall be the responsibility of Indian Computer Emergency Response Team concerning the collection, analysis and dissemination of information on cyber incidents. Such function is in sync with the normal function expected out of Computer Emergency Response Teams. Further, Indian Computer Emergency Response Team shall also be performing the function of providing forecast and alerts of cyber security incidents. It shall also be empowered for handling cyber security incidents. It has also been made responsible for coordination of cyber incident response activities. Further, Indian Computer Emergency Response Team has been mandated to issue guidelines, advisories, vulnerability notes and whitepapers. This should relate to information security practices, information security procedures, information security prevention, response of cyber incidents and reporting of cyber incidents. Section 70B(4)(f) is a very vast clause which says such other functions relating to cyber security as may be prescribed have also been made the function of the Indian Computer Emergency Response Team as India's national agency in the area of cyber security.

Under section 70B(5), the manner and performing functions and duties of Indian Computer Emergency Response Team may be prescribed by the Government.

The net effect of the reading section 70B as a whole is that the Indian Computer Emergency Response Team is regarded as a national agency of cyber security. This

is an unprecedented step as Computer Emergency Response Teams across the world are only teams constituted for the purposes of identifying computer emergencies and the response required to deal with such emergencies. However, making Indian Computer Emergency Response Team as the national agency in the area of cyber security, the Indian Information Technology Act, 2000 has gone far beyond other cyber legislations of the world.

Seen from one angle, the Indian Computer Emergency Response Team is primarily concerned with collection, analysis and dissemination of information of cyber incidents, the computer threats and providing appropriate response mechanisms for the same. The way the wordings of section 70B(4) is inserted in law, it is clear that the Information Technology Act, 2000 has sought to make the Indian Computer Emergency Response Team as the Indian National Agency in the field of cyber security.

Seen from another angle, such an approach is not legally prudent. An agency that is primarily aimed at collecting information pertaining to computer agencies and identifying their responses, are only doing portion of the activities under the broad umbrella of cyber security. However, making Indian Computer Emergency Response Team as the national agency for cyber security in respect of stipulated activities, tends to give different connotations to not just readers but also to different stakeholders in the information security ecosystem.

Further perusal of the provisions of section 70B(6) shows that huge powers have been given to Indian Computer Emergency Response Team. Indian Computer Emergency Response Team has been given the discretion to call for information for the purposes of carrying out the provisions of section 70B(4). In that context, Indian Computer Emergency Response Team has been given the power to give directions to call for information to any of the following:

(a) Service providers;

(b) Intermediaries;

(c) Data centres;

(d) Body corporates; and

(e) Any other person.

It is pertinent to note that the term "intermediary" is obviously defined in very broad terms under section 2(1)(w) with respect to any particular electronic records to mean any person, who on behalf of another person, receives, stores or transmits that record or provides any service with respect to that record. Further, the term "intermediary" includes within its ambit telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online auction sites and cyber cafes. The term "body corporate" is defined under *Explanation (i)* to section 43A to mean any company and including a firm, sole proprietorship or other association of individuals engaged in commercial or business activities. Thus by a single stroke, section 70B(6) gives discretion to call for any kind of information from just about any legal entity.

Huge powers have been given to the Indian Computer Emergency Response Team. There are no adequate checks and balances mentioned under section 70B of the Information Technology Act, 2000 to ensure that the said powers are not abused and misused.

One of the most significant changes made to jurisprudence is sought to be done by section 70B(7). Section 70B(7) introduces a new offence in the Information Technology Act, 2000. If any service provider, intermediaries, data centres, body corporates or person who is called by means of a direction under section 70B(6) to give information, fails to provide the said information or fails to comply with the directions under section 70B(6), that act is now declared as a penal offence. The said offence is punishable under section 70B(7) with imprisonment for a term which may extend to 1 year or with fine which may extend to 1,000,00 INR or with both. Thus, merely failing to provide information called for by Indian Computer Emergency Response Team becomes an offence. Further, merely failing to comply with the directions issued by the Indian Computer Emergency Response Team under section 70B(6) also becomes an offence. Both the offences, though minor offences, are punishable only with imprisonment for a term which may extend to 1 year and fine which may extend to 1,000,00 INR or with both.

Another issue is that there is no reckless cognizance of offences under section 70B(8). Section 70B(8) stipulates that no court of law shall take cognizance of any offence under section 70B, except in a manner as stipulated in the said provision. A complaint needs to be made by an officer authorized in this behalf by Indian Computer Emergency Response Team, before any court of law can take cognizance of any offence under section 70B(8).

Seen from an overall perspective, section 70B becomes a code in its own self as far as Indian Computer Emergency Response Team is concerned. It not only provides for its accreditation but is also stipulated as the National Agency in the area of cyber security in performing their functions as stipulated under section 70B(4). Further, huge powers have been granted to Indian Computer Emergency Response Team to call for information from any legal entity in India. Entities are mandated to comply with the said directions of Indian Computer Emergency Response Team and if they fail to comply with the same or if they fail to provide data or information so required by the said entity, they are exposed to criminal liability of having committed an offence punishable with imprisonment and fine.

A holistic meaning of section 70B gives rise to the impression that a lot of powers have been sought to be concentrated under the Indian Computer Emergency Response Team without adequate checks and balances in this regard to ensure that such huge powers granted under section 70B of the Information Technology Act, 2000 are not arbitrarily misused or misutilized.

It is pertinent to note that the Indian Computer Emergency Response Team has since been working as India's National Agency in the area of cyber security and has been performing its functions stipulated by section 70B of the Information Technology Act, 2000.

Section 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 Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

Section 71 creates law on a new offence to ensure the sanctity of information that is provided, to become a part of the Electronic Signature regime envisaged under the Information Technology Act, 2000. The Legislature has appreciated that the Electronic Signature regime in the country would only be successful if correct particulars and material facts are furnished to the relevant statutory authorities under the Information Technology Act, 2000 so as to prevent misuse.

If any Certifying Authority makes a misrepresentation to the Controller or suppresses any material or relevant fact from the Controller for the purpose of obtaining any licence for becoming a Certifying Authority, this has been declared as a penal offence punishable with imprisonment up to two years or with fine up to one lakh rupees or with both.

Similarly, if any person makes any misrepresentation to a Certifying Authority or suppresses any material or relevant fact from the Certifying Authority for obtaining any Digital Signature Certificate, that also has been made a penal offence punishable with imprisonment up to two years or fine up to one lakh rupees or with both.

If any Certifying Authority is found guilty of making any misrepresentation or suppressing any material facts, the Certifying Authority would be guilty of committing an offence under section 71. If the Certifying Authority is an individual, the individual shall be duly punished as stipulated above. If the Certifying Authority is a partnership firm, the partners of the partnership firm will be duly sentenced to imprisonment or fine. If the Certifying Authority is a company, the punishment and sentence shall be served by every person who at the time of misrepresentation or suppression of material facts, was in-charge of and was responsible to the Certifying Authority for the conduct of the business of Certifying Authority company. In addition, the concerned Directors of the Certifying Authority company would also be liable to punishment. This situation becomes clear from a perusal of section 85 of the Information Technology Act, 2000.

It may also be noted that if misrepresentation or suppression takes place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or any other officer of the company, such director, manager, secretary or other officer would also be deemed to be guilty of misrepresentation and suppression under section 71.

Any person making any misrepresentation or suppression of any material facts from the Certifying Authority for obtaining a Electronic Signature Certificate, apart from being liable for the offence under section 71, also faces the consequences of revocation of his Electronic Signature Certificate in terms of section 38(2)(a). Similarly, if a Certifying Authority is guilty of an offence under section 71 of the Information Technology Act, 2000, then apart from facing punishment under section 71, the licence of the Certifying Authority may also be revoked by the Controller under section 25(1)(a) of the Information Technology Act, 2000.

A provision like section 71 is a positive step to ensure that people give correct and true particulars, to the concerned authorities, while dealing with Electronic signatures and do not manipulate, misrepresent or suppress material and relevant facts for ulterior motives or with criminal designs. Section 71 acts as a good protection or shock absorber mechanism for the entire Electronic Signature regime in India.

Section 72 – Penalty for Breach of Confidentiality and Privacy

> *"Save as otherwise provided in this Act or any other law for the time being in force, any person who, in 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."*

Section 72 enacts a new offence to preserve and protect the privacy and confidentiality of data and information. It stipulates that if any person, in pursuance of any of the power under the Information Technology Act, 2000, rules and regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material, then he is duty bound not to disclose the same to any other person. If he does so, without the consent of the concerned person, then that act has been declared as an offence punishable with imprisonment up to two years or fine up to one lakh rupees or with both.

Under the Information Technology Act, 2000, the people on whom the powers are conferred include the Controller of Certifying Authorities, Deputy Controller, Assistant Controller or any other officer authorized by them, Certifying Authorities and Adjudicating Officers. If any of the aforesaid persons, who in pursuance of the powers conferred upon them under the Information Technology Act, 2000, rules and regulations made thereunder, secure access to an electronic book, register, correspondence, information, document or other material and disclose it to any other person, without the consent of the person concerned, they are liable to be punished under the present section.

The present section is aimed at ensuring the confidentiality of data or information belonging to different persons. However, the scope of the section is limited to breach of confidentiality of information or data, by relevant statutory authorities, which have secured access to the same in pursuance of their statutory powers. The section does not target the commonly prevalent breaches of confidentiality committed by lay netizens and users.

It is pertinent to mention that the entire IT Act, 2000 is silent on the contentious issue of privacy, barring this present section and section 66E. Also, the word "privacy' does not find mention in the body of section 72 but is only mentioned in its heading.

At this juncture, let us examine the status of privacy in India in the context of cyberspace.

Man is a social animal but despite all his social leanings, there is a small area coming within the exclusive limits, which any man treasures and cherishes. This is the domain of individual privacy. We are all familiar with the concept of privacy in the actual world. Many countries today have special legislations relating to protection of individual privacy.

When Internet as a medium first came into existence, it started a big debate. Could there be privacy for netizens online? After much discussion, it was universally recognized that there exists privacy of the individual online and that he is entitled to protect the same.

The next question that arose was, how individual's online privacy going to be protected. Various governments have differed on this complicated Cyberlaw issue.

Privacy is one of the most contentious legal issues arising in Cyberspace. Just as in the actual world, privacy is of extreme importance to not only to individual netizens but also corporations and governments. In the present times, privacy of the individual netizens has acquired critical relevance.

Coming to the Indian scenario, currently there is no comprehensive legislation on privacy in our country. We do not even have a specific law on privacy like some other countries. It has been left to the Judiciary to interpret privacy within the existing legislations. The right to privacy has been held by the Supreme Court of India as an integral part of the fundamental right to life under article 21 of the Constitution of India. In *People's Union for Civil Liberties (PUCL)* v. *Union of India*,[67] the Supreme Court has held:

> *"…Right to privacy is a part of the right to "life and personal liberty" enshrined under article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, article 21 is attracted."*

But while legislating India's first Cyberlaw, namely, the Information Technology Act, 2000, the Parliament has omitted to deal with the crucial issue of privacy. The Information Technology Act, 2000 does not define privacy. It does not even touch or address the critical issue of protecting privacy online. It only talks of privacy in the heading of section 72.

A perusal of section 72 of the Information Technology Act, 2000 shows that it has been drafted in a restrictive manner to only refer to punish those persons who, after having 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.

It does not have any bearing on the violation of an individual's privacy in cyberspace. Spamming, or the practice of sending unsolicited e-mails to different persons, has not been mentioned at all in the Information Technology Act, 2000. The fact of the matter is that whenever a netizen receives an unsolicited e-mail, that itself constitutes a violation of individual's privacy. That is the reason why many States in the USA like Nevada have cyber legislations banning spamming.

---

67. (1997) 1 SCC 301: AIR 1997 SC 568: 1997 AIR SCW 113.

In addition, in today's scenario, a lot of websites collect information of net surfers, which is often not protected but is sold for commercial considerations to other companies. In other cases, the servers of websites containing valuable information of consumers are hacked into and the information is stolen for the purpose of valuable consideration. The stolen information is then invariably sold to different companies who then send unsolicited e-mails to the e-mail addresses of different persons. All these varied endeavours are a grave violation of individual privacy.

Unfortunately, in India, awareness about privacy is at a very low level in the actual world, leave aside in cyberspace.

It is important that the Government should separately legislate on privacy in cyberspace. Websites must be made to follow strict guidelines on various issues concerning individual privacy. Websites must give notice to the netizens that information about them is being collected, what is the kind of information being collected and for what purpose, as also how the collected information about the netizens would be utilized. Netizens should also be given a choice to state as to whether the information being collected about them should be used for any other purpose except for fulfilling the transaction for which the information is being collected.

For example, when I am buying music online, the website would ask different kinds of information about my tastes and me. In such a scenario, I should be given the choice to decide whether the information I give about myself to the website before buying music, should be used for any other purpose by the said website except for the purpose of completing the transaction of selling music online to me.

Cyberlaw should also give the facilities of reasonable access to the netizens. Once a person gives information about himself to the websites, he must have the right to access this information and in addition, he should also have a reasonable opportunity to make any corrections to the information or of any errors as also the choice of deleting any or the entire data or information collected on him by the website.

It is also essential for all websites, portals and companies to ensure that the collected information relating to netizens should be properly handled to rule out unauthorized access to it or its theft.

The Internet Industry has debated for self-regulation for a long duration. However, self-regulation has failed to check the abuse and violation of individual privacy. The Government of India has notified the Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data or Information) Rules, 2011, which has stipulated various compliance requirements for legal entities, possessing, dealing or handling sensitive personal data or information in their computers, computer systems and computer networks.

Cyber legislation on privacy seems to be the only answer to protect online privacy. However, Legislature needs to take care that cyber privacy legislation should be as clear as possible without leaving any scope for doubt and without leaving any possibilities for abuse by either the State or the regulators.

Another need of the hour is to educate the netizens in India at large that their online privacy is extremely valuable and that it needs to be protected at any cost. At the end of the day, evolving Cyberlaw, coupled with public awareness about protecting it, will win the battle for the cause of online privacy.

Section 72A – Punishment for Disclosure of Information in Breach of Lawful Contract

> *"Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both."*

Section 72A has been added in the Information Technology Act, 2000 by means of the Information Technology (Amendment) Act, 2008. Section 72A provides law to deal with a specific new offence dealing with the disclosure of information in breach of lawful contract.

Since the last one decade, India has seen tremendous growth in the area of outsourcing. Though outsourcing in India began in the form transcription in call centers, it soon transformed itself to higher levels of Business Process Outsourcing, Legal Process Outsourcing and Medical Process Outsourcing. The said outsourcing industry has given a boost for the Indian economy. However, the said outsourcing sectors have also seen various outages of third party data belonging to foreign clients. Hence, there has been a tremendous need to protect third party data and also misuse of information in breach of a lawful contract. As such, the Indian Legislature has been alive to the said issue and has therefore included section 72A under the Information Technology Act, 2000.

The said provision penalizes the act of disclosing information in breach of a lawful contract. Today, a large number of service providers and intermediaries have access to material containing personal information about other persons, clients and customers. Access to material is achieved during the course of providing services, under the terms of the lawful contract. We have also seen various instances where service providers and intermediaries have gone ahead and misused the said personal information about other persons. This is often done in breach of a lawful contract that would exist between the said intermediary and its customers. In order to prevent such action happening, the law has now stipulated a crime as detailed under section 72A. If any person, including an intermediary, is providing services under the terms of a lawful contract, he is obligated to abide with the terms of the lawful contract. Further, if during the factum of providing services under the said lawful contract, any person, including the intermediary, has secured access to any material which contains personal information about other person and the said access has been done with the intention to cause or knowing that is likely to cause wrongful loss or gain and further thereto, the said person, including the intermediary, discloses such

material to any other person, without the consent of the person concerned or in breach of a lawful contract, then the said act has been made as an offence punishable under the law. The said offence is punishable with imprisonment for a term, which may extend to 3 years or with fine which may extend to 5 lakh rupees or with both. The purpose of section 72A is to provide deterrence for all persons including intermediaries who have, while providing services under the terms of a lawful contract, secured access to material containing personal information about third parties. The said persons, including intermediaries, are duty bound to protect and preserve the authenticity and veracity of the said personal information about third parties. If the said persons do not choose to protect and preserve the said information but with an intention to cause or knowing that they are likely to cause wrongful loss or gain, further disclose such personal information to any other person, without the consent of the person concerned or in breach of the lawful contract, then the said act comes within the ambit of criminal penalty.

For section 72A to be applicable, it is important that the following ingredients must be fulfilled:

(a) any person needs to be providing services;
(b) the said person would also include any intermediary as defined under section 2(1)(w) of the amended Information Technology Act, 2000;
(c) the said services must be performed by the said person or intermediary under the terms of a lawful contract;
(d) that while providing such services, such person or intermediary has secured access to any material containing personal information about another person;
(e) that the said act must be done with an intention to cause wrongful loss or wrongful gain, or the said act must be caused with knowing that the said person is likely to cause wrongful loss or wrongful gain;
(f) thereafter, the concerned person or intermediary must disclose such material to any other person;
(g) that the said disclosure of such material to any other person has to be without the consent of the person concerned or;
(h) the said disclosure of such material to any other person has to be in breach of a lawful contract.

If all the above conditions are fulfilled, the said act becomes an offence under section 72A. The said offence is punishable with imprisonment for a term which may extend to 3 years or with fine which may extend to 5,000,00 INR or with both.

The section has not given any definitions of the words used therein. The term "lawful contract" is neither defined here nor under any other law. However, the term "contract" is defined under the Indian Contract Act, 1872. Section 2 (h) of the Indian Contract Act, 1872 reads as follows:—

"2(h). An agreement enforceable by law is a contract."

It is pertinent to point out that section 10 of the Indian Contract Act, 1872 specified the conditions for a valid/lawful contract. Section 10 of the Contract Act reads as follows:

"10. What agreements are contracts.—All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void.

Nothing herein contained shall affect any law in force in India and not hereby expressly repealed by which any contract is required to be made in writing or in the presence of witnesses, or any law relating to the registration of documents.

However, for the purpose of lawful contract, there must be an agreement between the parties, and the contracting parties are competent to contract. There must be a free consent of the parties. There must be a lawful consideration and object and the said contract is not expressly declared to be void.

Further, the term "personal information" has not been defined under section 72A of the Information Technology Act. It is pertinent to note that the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 have defined the term "personal information" under rule 2(1)(i) in the following terms:

"(i) "Personal information" 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."

The word "wrongful loss" and "wrongful gain" would have the same meaning as it detailed under section 23 Indian Penal Code, 1860 which states as follows:—

""Wrongful gain" is gain by unlawful means of property which the person gaining is not legally entitled.

"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.

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".

In *"Kishan Kumar v. Union of India"*[68], the Supreme Court held that, the expression*"wrongful gain includes wrongful retention and wrongful loss includes being kept out the property as well as being wrongfully deprived of property".*

Thus, a perusal of section 72A clearly shows that the law has been created for the purposes of ensuring the confidentiality and security of material containing personal information about other persons. The net effect of section 72A is that the law does not want any person to unauthorizedly access personal information about another person with intention to cause wrongful loss to that person or wrongful gain to himself and further disclosing the same to any other person, without the consent of the said person. Further, the law is even very particular that it does not want any disclosure of personal information of another person which is in breach of a lawful contract. This section assumes more significance, given the

68. AIR 1959 SC 1390: (1960) 1 SCR 452: 1959 Cr LJ 1508.

huge outsourcing industry in our country when clients are outsourcing their confidential work to entities in India.

The said provision shall be extremely relevant for the purposes of the Indian outsourcing industry. It will also be relevant for checking the misuse of personal data being done by service providers who invariably, while collecting personal data for the purposes of providing services for the customers, land up sharing the said personal data with other business partners. Today invariably, we typically are bombarded with various e-mails spam on our computer, computer systems, computer network, computer resources and communication devices asking us to buy certain insurance policies or take certain loans. The said acts are primarily done as our data, including personal information, is shared by our service provider with other third party business partners with or without consideration.

However, by the mere sharing of the said third party information and by further making such calls, there is an intention to cause and knowing that the said service provider is likely to cause wrongful loss to customers. Further, the service providers do share the said data with their business partners and that they do so for the purposes of causing wrongful gain. Section 72A promises to be a huge potent weapon in the hands of the lay consumers, who can use it against erring service providers and other legal entities who disclose information about them without their permission, to other third parties with an intention to cause or knowing that the same is likely to cause wrongful loss or wrongful gain.

I distinctly believe that if section 72A is interpreted properly and is effectively implemented, the misuse of personal information by any persons including intermediaries and its disclosure to unauthorised third parties is likely to be substantially reduced. It is interesting to see how the actual working of section 72A of the amended Information Technology Act, 2000 will pan out in the coming times.

Section 73 – Penalty for Publishing Electronic Signature Certificate False in Certain Particulars

"(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that—

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

Section 73 makes publishing of a Electronic Signature Certificate, which is false in certain particulars, a penal offence. This section is basically enacted to prevent false Electronic Signature Certificates from being published for pecuniary gain or criminal purposes.

The important ingredient of section 73 is knowledge about falsity of particulars in Electronic Signature Certificates. Section 73 visualizes three distinct kinds of offences.

(a) *Firstly*, if anyone publishes an Electronic Signature Certificate or otherwise makes it available to any other person with the knowledge that the Certifying Authority listed in the Certificate has not issued it, that becomes an offence under section 73.

(b) *Secondly*, in case, any person publishes an Electronic Signature Certificate or makes it available to any person with the knowledge that the subscriber listed for the certificate has not accepted it, then that also becomes an offence under section 73.

(c) *Thirdly*, if any person publishes an Electronic Signature Certificate or otherwise makes it available to any other person knowing fully well that the said certificate has been revoked or suspended, that also is an offence under section 73.

The proviso explains that no offence under this section shall be committed if it is proved that such publication of the Electronic Signature Certificate is for the purpose of verifying a Electronic Signature created prior to such suspension or revocation. If this proviso is not proved, then the act of publishing an Electronic Signature Certificate, which is false in certain particulars, becomes a penal offence. The offence under section 73 is punishable with imprisonment up to two years or fine up to one lakh rupees or with both.

The main objective of section 73 is that no false Electronic Signature Certificates should be in circulation in the Electronic Signature regime and if anybody is found publishing the same or making it available, it is a serious matter and the person concerned has to be punished. An analogy similar to the present situation is, when somebody starts circulating counterfeit currency affecting the economy of our country, it is a serious offence. The offence under section 73 is non-cognizable, bailable and triable by a Magistrate.

Section 74 – Publication for Fraudulent Purpose

"Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

Section 74 points out a distinct kind of crime, which deals with publication of Digital Signatures for fraudulent purposes. While section 73 of the Information Technology Act, 2000 has referred to publication of the Electronic Signature Certificates, which are false in certain particulars, section 74 talks of creation, publication and availability of an Electronic Signature Certificate for any fraudulent or unlawful purpose. Under this section, if anyone knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose, he has committed an offence punishable with imprisonment up to 2 years or with fine up to one lakh rupees or with both. The essential ingredients of section 74 are knowingly, creating, publishing or making available an Electronic Signature Certificate for fraudulent or unlawful purpose.

The offence under section 74 is non-cognizable, bailable and triable by a Magistrate.

Section 75 – Act to Apply for Offence or Contravention Committed Outside India

"(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

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

Section 75 makes the provisions of the Information Technology Act, 2000 applicable to any offence committed outside India by any person, irrespective of his nationality. This enables the law to assume jurisdiction over cyber criminals outside the territorial boundaries of India.

However, the caveat to section 75(1) is explained in section 75(2) inasmuch as section 75(1) is subject to provisions of section 75(2). The caveat provided by section 75(2) is that the Information Technology Act, 2000 shall apply to any offence or contravention committed outside India by any person if and only if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Therefore, the physical location of computer, computer system or computer network within the territorial boundaries of India is a condition precedent to the applicability of this Act to any offence or contravention committed outside India by any person irrespective of his nationality. Section 75 takes a mere practical view of the issue of extra territorial jurisdiction than section 1(2) of the Information Technology Act, 2000.

Section 1(2) of the Information Technology Act states that the Information Technology Act shall extend to the whole of India and save as otherwise provided in this Act, it applies to any offence or contravention thereunder committed outside India by any person. It has been argued that the necessity of having the present provision is because of the emergence and growth of cyberspace, which does not have any boundaries. As Internet is making geography history, it is imperative that nations enact laws that have to have all pervasive applicability and impact. Further, such an approach facilitates nations to catch cyber criminals who have indulged in cyber crimes, but who are located physically outside the territorial boundaries of nations. On the other hand, the provision is liable to be criticized inasmuch as no country can assume jurisdiction over the citizens of another nation, merely on the ground that that citizen has violated the national laws of that nation. The move has been criticized as being contrary to the established principles of international law. (For more details, kindly *see* the commentary on section 1)

Section 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, rules, 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."

Section 76 talks of the power of confiscation that is granted under the new Cyberlaw. The subject matters of confiscation include:—

1. any computer,
2. computer system,
3. floppies,
4. compact disks,
5. tape drives, or
6. any other accessories relating thereto,

However, the aforesaid objects can be confiscated only if in respect of such objects, there has been a contravention of any provision of the Information Technology Act, 2000, rules, orders or regulations made thereunder. The confiscation shall be done by a police officer not below the rank of an Inspector. Since confiscation is a part of the process of investigation of an offence, section 78 would apply in order to enable an Inspector to confiscate.

However, the proviso enables the court adjudicating the confiscation to pass an appropriate order, in case it is established to the satisfaction of the court that the person in whose power, possession or control 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 the IT Act, 2000, rules or regulations made thereunder.

The power has been given to the court that in such an instance, the court may, instead of ordering confiscation of above noted objects and accessories, make such other order authorized by the Information Technology Act, 2000 against the person contravening the provisions of the Information Technology Act, 2000 rules, orders and regulations made thereunder.

This kind of a proviso gives a wide power to the court to pass appropriate orders against the relevant person who is violating or contravening the provisions of this Act. However, the caveat is that such orders must be authorized by the IT Act, 2000. Any order which is not authorized by the IT Act, 2000, would not stand scrutiny in a court of law and is liable to be struck down.

Section 77 – Compensation, Penalties or Confiscation not to Interfere with other Punishment

"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."

The language of section 77 of the Information Technology Act, 2000 has been substituted by Information Technology (Amendment) Act, 2008.

Earlier section 77 of the Information Technology Act, 2000 stated as follows:—

Section 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."

Section 77 stipulates that the civil remedies of compensation, penalties or confiscation run on a completely different plane from the criminal liability of the concerned person. Section 77 specifically explains that if any compensation has been awarded or penalty imposed or confiscation made under the Information Technology Act, 2000, the same shall not prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force. Hence, the spirit behind section 77 is that the compensations awarded, penalties imposed and confiscation made under the Information Technology Act, 2000 are in addition to the awarding of compensation, imposing a penalty of punishment under any other law for the time being in force.

If a person has committed an offence which is punishable with a stipulated statutory punishment under any other laws including the Indian Penal Code, that person is likely to be punished in accordance with other laws along with violation of provisions of the Information Technology Act, 2000.

For example, if a person commits hacking of a computer system and steals the credit card number of the relevant subscriber and then misuses the credit card number to buy expensive jewellery and to cheat the subscriber of huge sums of money, then, in such a case, the accused person can be imposed with a liability for a sum of upto 5 crore rupees under section 43 of the Information Technology Act, 2000 and in addition, he can also be charged and punished under section 420 IPC, 1860.

Section 77A – Compounding of Offences

"A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or 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."

Section 77A has been added in the Information Technology Act, 2000 by means of the Information Technology (Amendment) Act, 2008. Section 77A deals with compounding of offences as contradistinguished from compounding of contravention under section 63 of the Information Technology Act, 2000.

This section has provided for exit from potential legal consequences for the concerned stakeholders. It also provides an important remedy for closure of legal cases where the main dispute between the parties has long been compromised.

Section 77A has provided for the concept of compounding of offences. Section 77A of the Information Technology Act, 2000 clearly provides that all offences under the Information Technology Act, 2000 can be compounded barring the following offences:

(a) offences punishable with life imprisonment; or

(b) offences punishable with imprisonment for a term exceeding three years.

It has been seen as a practical experience amongst criminal courts that criminal cases, after registration goes on for trial for years and years and a lot of inconvenience and harassment is caused to the persons who are involved in the same, even if the said persons are involved in the same, either erroneously or wrongfully.

As such, section 77A has now provided for the concept of compounding of offences. The power for compounding offences has been given to the court of competent jurisdiction. Of course, the limitation is that only such offences can be compounded which are punishable only with imprisonment for a term upto three years. This effectively means that all offences which are punishable with imprisonment for a term exceeding three years have been specifically exempted and brought outside the ambit of compounding of offences.

Thus, seen from a holistic perspective, section 77A does provide a very effective remedy for closure of criminal cases, being registered under the Information Technology Act, 2000 to the extent that the same are only punishable with imprisonment for a term which does not exceed three years. It is pertinent to note that a majority of cyber crimes including those that have been inserted into the Information Technology Act, 2000 by the Information Technology (Amendment) Act, 2008 have been made punishable with three years imprisonment. These crimes include the following:

(a) Tampering of computer source documents under section 65B of the Information Technology Act, 2000.

(b) Computer related offences under section 66 of the Information Technology Act, 2000.

(c) The offences of sending offensive messages through computer source under section 66A of the Information Technology Act, 2000.

(d) The offence of dishonestly receiving stolen computer resource under section 66B of the Information Technology Act, 2000.

(e) The offence of identity theft under section 66C of the Information Technology Act, 2000.

(f) The offence of cheating by personation by using computer resource under section 66D of the Information Technology Act, 2000.

(g) The offence for violation of privacy under section 66E of the Information Technology Act, 2000.

(h) The first conviction for the offence of publishing or transmitting of obscene electronic information under section 67 of the Information Technology Act, 2000.

(i) The offence of the failure of the intermediary to preserve and retain such information under section 67C (1) of the Information Technology Act, 2000.

(j) The offence of intermediary knowingly or intentionally not providing technical assistance to the concerned agency for cyber security under section 69B of the Information Technology Act, 2000.

(k) The offence under section 70B (7) for the failure of the service provider and intermediary to provide the information as required by Indian Computer Emergency Response Team.

(l) The offence of making misrepresentation to the Controller of Certifying Authorities under section 71 of the Information Technology Act, 2000.

(m) The offence of breach of confidentiality of privacy under section 72 of the Information Technology Act, 2000.

(n) The offence for disclosure of information and breach of lawful contract under section 72A of the Information Technology Act, 2000.

(o) The offence of publishing electronic signature certificate false in certain particulars under section 73 of the Information Technology Act, 2000.

(p) The publication of electronic signature certificates for fraudulent purposes under section 74 of the Information Technology Act, 2000.

Thus, almost a majority of cyber crimes covered under the amended Information Technology Act, 2000, have been brought within the ambit and applicability of compounding of offences. The only major offences, which cannot be compounded, relate to direct offences as defined under the amended Information Technology Act, 2000, including the following:

(a) The second conviction for publishing or transmission of obscene electronic information under section 67 of the Information Technology Act, 2000.

(b) The offence of publishing or transmitting of material containing sexually explicit act or conduct in electronic form, under section 67E of the Information Technology Act, 2000.

(c) The offence of publishing or transmission of material depicting children in sexually explicit act or conduct in the electronic form, under section 67B of the Information Technology Act, 2000.

(d) The offence of the subscriber or the intermediary failing to assist the agency in interception monitoring or decryption of information under section 69(4) of the Information Technology Act, 2000.

(e) The offence of intermediary failing to comply with the directions for blocking of public access under section 69A of the Information Technology Act, 2000.

(f) The offence of breach of protected system under section 72(3) of the Information Technology Act, 2000.

(g) The offence of Cyber terrorism under section 66 F of the Information Technology Act, 2000.

The net effect of this is that section 66F of the Information Technology Act, 2000 deals with offence of cyber terrorism which is punishable with life imprisonment and the same cannot be compounded. Further, offences for which the imprisonment is for a term exceeding three years are offences under section 67A, 67B, dealing with the offences pertaining to publishing of material containing sexually explicit act and child pornography.

Thus, barring the aforesaid offences, all other offences under the Information Technology Act, 2000 are capable of being compounded. However the compounding of the offences under the Information Technology Act, 2000 can only be done by a court of competent jurisdiction.

However the first proviso to section 77A mandates that the court of competent jurisdiction shall not compound any offence where the following circumstances are applicable:

(a) the accused is by reason of a previous conviction liable to enhanced punishment; or

(b) the accused is by reason of his previous conviction liable to punishment of the different kind.

In both the said two conditions, the said offence shall not be compounded by the court of competent jurisdiction. Further the second proviso to section 77A provides that the court shall not compound offences which belong to the following category:

(a) where such offence affects the socio-economic conditions of the country;

(b) where the offence has been committed against a child below the age of 18 years; or

(c) where the offence has been committed against a woman.

The net intention behind the second proviso to section 77A is that the law wants to protect the legal interests of not just India and its socio-economic conditions but also to protect and preserve the children below the age of 18 years as also women.

The concept of compounding has been defined under section 320 of the Cr. P.C. Section 320 Cr. P.C. stipulates as follows:

Section 320 of Cr.P.C. provides for a list of offences that can be compounded. However such offences have been classified into ones which can be compounded:—

(a) With the permission of Court,

(b) Without the permission of the Court.

Section 320 Cr.P.C stipulates as under:—

"320. Compounding of offences.—(1) The offences punishable under the sections of the Indian Penal Code specified in the first two columns of the Table next following may be compounded by the persons mentioned in the third column of that Table:—

(2) The offences punishable under the sections of the Indian Penal (45 of 1860) Code specified in the first two columns of the Table next following may, with the permission of the Court before which any prosecution for such offence is pending, be compounded by the persons mentioned in the third column of that Table."

In *Sudheer Kumar @ Sudheer* v. *Manakkandi M.K. Kunhiraman*, on 13 November, 2007 CRL. M.C. No. 1540 of 2007 (B), the Kerala High Court held as follows:

"6. Compounding is defined in Black's Law Dictionary, Seventh Edition, as

"Compounding a crime:- The offence of either agreeing not to prosecute a crime that one knows has been committed or agreeing to hamper the prosecution."

In the Law Lexicon, (3rd reprint - Second Edition) of Sri P. Ramanatha Aiyer, compounding is defined as follows:

"Compounding felony or offence: Compounding an offence is defined to be "the offence of taking a reward for forbearing to prosecute a felony; as where the party robbed takes his goods again, or other amends upon an agreement not to prosecute." (Burrill.) "See Criminal Procedure Code as to compoundable and non-compoundable offences." Offences which are not mentioned in Table of sub-sections (1) or (2) of section 320 cannot be compounded and such compounding cannot be accepted by the court, though a compromise between the victim and accused may persuade the court to take a lenient view in the matter of sentence [See Bankat v. State of Maharashtra, *(2005) 1 SCC 343*]."

Section 77A(2) provides that the compounding of an offence does not happen automatically. For the same, the person who is accused of an offence under the Information Technology Act, 2000 has been given the discretion to file an application for compounding. The said application has to be filed in the court in which the cybercrime or offence under the Information Technology Act, 2000 is pending for trial. In such a case, the provisions of section 265B and 265C Cr. P.C. shall be fully applicable. Section 265B Cr. P.C. provides as follows:—

"265B. Application for plea bargaining.

(1) A person accused of an offence may file 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)."

Further section 265C Cr. P.C. provides as follows:

"265C. Guidelines for mutually satisfactory disposition.

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, if he so desires, may 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 engage in the case."

Thus, the provisions of section 265B and 265C Cr. P.C. have been made mandatorily applicable in the context of any proceedings for compounding of offences under the Information Technology Act, 2000.

It is pertinent to note that by virtue of operation of section 81 of the Information Technology Act, 2000, the provisions of the Information Technology Act, 2000 shall have overriding effect, notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Further, when one examines in totality the provisions of section 77A of the Information Technology Act, 2000 as contradistinguished from section 63 of the Information Technology Act, 2000 one finds that the law has made a distinction between compounding of criminal offences which are penal in nature made

punishable with imprisonment and fine as contradistinguished from compounding of mere contraventions of the Information Technology Act, 2000. There could be acts which could be contraventions of the various provisions of the Information Technology Act, 2000. The mere violation of the various provisions the Information Technology Act, 2000 could also expose the person concerned to various other civil legal exposures including the liability to pay damages by way of compensation. As such, the Information Technology Act, 2000 under section 63 thereof has provided for compounding of contraventions of a civil nature which relates to the adjudication proceedings instituted for seeking damages by way of compensation under section 43 of the Information Technology Act, 2000. The said contraventions are of a civil nature and the same have also been made compoundable under section 63 of the Information Technology Act, 2000. However section 77A of the Information Technology Act, 2000 is far more specific as it only deals with compounding of penal offences, which have been made punishable with imprisonment for various terms and fines.

Thus, from the aforesaid lists, it is very clear that a majority of the cyber crimes under the amended Information Technology Act, 2000, have been brought within the ambit of compounding of offences. The author distinctly believes that with the passage of time, such kinds of provisions will help far more people to come out of the rigours of such cyber crimes.

Section 77B – Offences with three Years Imprisonment to be Bailable

"(l) Notwithstanding anything contained in the Code of Criminal Procedure, 1973,(2 of 1974) 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."

Section 77B has been added in the Information Technology Act, 2000 by means of the Information Technology (Amendment) Act, 2008. Section 77B clearly provides that all offences under the Indian Information Technology Act, 2000 which are punishable with imprisonment of three years, shall be bailable. Further, it has also been provided that the offences punishable with imprisonment of three years and above shall be cognizable. Section 77B further provides that its provisions shall have effect notwithstanding anything contained in the Code of Criminal Procedure, 1973.

It is relevant here to point out that the Information Technology Act, 2000 has not defined the term cognizable. Section 2(c) of the Code of Criminal Procedure, 1973 has defined the term "Cognizable offence", which reads as follows:

"2(c) "Cognizable offence" means an offence for which, and "cognizable case" means a case in which, a police officer may, in accordance with the First Schedule or under and other law for the time being in force, arrest without warrant."

Further, it has been provided that only the offence which is punishable with imprisonment of three years and above, shall become cognizable. This effectively means that for all offences punishable with three years imprisonment, the accused shall be entitled to bail as a matter of right. Such a scenario is not necessarily conducive for the effective deterrence of cyber crimes and mobile crimes. This is invariably so because the moment the accused is let out on bail in a bailable

offence, the propensity of the accused to go ahead and destroy the concerned incriminating electronic evidence which is not yet been recovered, is extremely high and such an exercise invariably tends to impede the effective investigation of any cyber crimes. This further ultimately impacts the conviction rate of the prosecution in terms of prosecuting the said cyber crimes. There are demerits in the approach adopted by section 77B of the amended Information Technology Act, 2000. This becomes all the more highlighted, when one considers that at the time of writing, there are only single digit cyber crime convictions under the Information Technology Act, 2000 in India, even after the decade of the operation of the Indian Cyberlaw.

The net effect of section 77B is that the offences under the Information Technology Act, 2000 punishable with imprisonment of three years are deemed as bailable. These include offences including the offences under the following sections:—

Section 65 - Tampering with Computer Source Documents.
Section 66 - Computer-Related Offences.
Section 66A - Sending offensive messages through communication service, etc.
Section 66B - Dishonestly receiving stolen computer resource or communication device.
Section 66C - Identity theft.
Section 66D - Cheating by personation by using computer resource.
Section 66E - Violation of privacy.
Section 67 - Publishing or transmitting obscene material in electronic form.
Section 67C - Contravene the provisions of section 68(1).
Section 68 - Failure to comply with the directions given by Controller.
Section 69B - Failure to comply with the directions given by Controller of section 69(2).
Section 70B - Fails to provide the information called for or comply with the direction under section 70B(6).
Section 71 - Misrepresentation.
Section 72 - Breach of confidentiality and privacy.
Section 72A - Disclosure of information in breach of lawful contract
Section 73 - Publishing electronic Signature Certificate false in certain particulars.
Section 74 - Publication for fraudulent purpose.

Thus, a perusal of the provisions of section 77B of the Information Technology Act, 2000 clearly shows that barring few offences under sections 66F, 67A and 67B, etc., majority of all cyber crimes under the Information Technology Act, 2000 have been made bailable. This has been the fundamental change that has been affected by means of the Information Technology (Amendment) Act, 2008. The net effect of this is that with a majority of cyber crimes in India being made as bailable offences, it becomes increasingly more and more difficult for the prosecution to get convictions. Practical experience has shown that the moment a person is released

on bail in a cyber crime matter, he invariably would tend to prejudicially impact the existence of the relevant incriminating electronic evidence which could have a direct impact upon the prosecution and convictions of cyber crimes in India.

I personally believe that with the introduction of section 77B, the nature and colour of the Information Technology Act 2000 as a cyber crime legislation has been damaged irreparably. The majority of cyber crimes being made bailable, is likely to give a picture to the entire world that India is a cyber crime friendly country and its legislations are cybercrime friendly and as such, the deterrence has apparently gone out of the provisions of the Information Technology Act, 2000. If India wants to strengthen its legislative provisions pertaining to digital and mobile ecosystems, it is absolutely imperative that the provisions of section 77B of the Information Technology Act, 2000 will have to be reviewed and revisited.

Section 78 – Power to Investigate Offences

"Notwithstanding anything contained in the Code of Criminal Procedure, 1973, (2 of 1974) a police officer not below the rank of an Inspector shall investigate any offence under this Act."

Section 78 has been amended by the Information Technology (Amendment) Act, 2008. Earlier, the power to investigate all offences under the Information Technology Act, 2000 were granted to a police officer, not below the rank of Deputy Superintendent of Police. However, with the elapse of time, it was found that the police officers of the rank of Deputy Superintendent of Police did not invariably have the time or the bandwidth to investigate various offences as detailed under the Information Technology Act, 2000. Consequently, by virtue of the 2008 amendments, section 78 has been amended to provide that the police officer not below the rank of an Inspector shall investigate any offence under the Information Technology Act, 2000. This has been done, notwithstanding anything contained in the Code of Criminal Procedure, 1973. The net effect of this is that all kinds of cybercrimes which are stipulated and specifically covered under the amended Information Technology Act, 2000 can only be investigated by an Inspector and no one else. The efficacy of such a step is doubtful, considering the fact that majority of inspectors are not very well conversant with the nuances and technical details pertaining to the working of computers, computer systems, computer networks, computer resources and communication devices as also data and information in the electronic form. Further, the said inspectors also do not have the wherewithal, knowledge, awareness and tools so as to effectively detect, investigate and prosecute cyber crimes including seizing appropriate electronic evidence resident on computers, computer systems, computer networks, computer resources and communication devices. Clearly, the said step is not likely to contribute to the efficient detection, investigation and prosecution of cyber crimes under the amended Information Technology Act, 2000.

CHAPTER XII
INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

tion 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 sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

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

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

(b) The intermediary 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.

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

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

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner."

Explanation.—For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary."

Technologies have made it now possible for people to be on the go, while they communicate, exchange thought processes, send and receive e-mails and do a host of other functions that were earlier perceived to be only done with stationary devices like computers and computer systems. Consequently, the increased usage

of electronic devices has now changed the way people perceive, think, govern, as well as do commerce. Today, electronic ecosystem and digital devices are increasingly being used not only for accessing Internet, sending and receiving e-mail but also for information, education and entertainment purposes, whether it be for watching a movie, listening to music, making short films and taking photographs with cameras on mobiles and for a host of new applications that are hitting the market with each passing week.

While electronic devices have increased the convenience of the users, they have also underlined the importance and significance of Intermediaries. Intermediaries are increasingly becoming important repositories of data. These Intermediaries have data pertaining to almost all activities done, using electronic ecosystems as also electronic platforms. It seems that almost suddenly, while the electronic revolution has been penetrating different parts of the world, the Intermediaries have become important players in terms of third-party data that is either resident in or processed or transmitted using the said service providers' computers, computer systems, computer networks, computer resources and communication devices.

It is in this context that Intermediaries are becoming increasingly relevant not only in the context of dispute resolution but also in the context of tracking and investigating various kinds of cyber crimes and other unwarranted criminal activities.

Given the way things are going, the importance of intermediary in terms of them being data repositories will continue to increase with the passage of time. Therefore, these intermediaries are recognised as important stakeholders in the electronic ecosystem. Further, the law seeks to stipulate the specific limits of the duties, obligations and responsibilities of these intermediaries.

In India, the law pertaining to Intermediaries is well defined. The Indian Information Technology Act, 2000 as amended has not only given a legal definition to the term "Intermediary" but has also stipulated the rights, duties and obligations of intermediaries.

Section 2(1)(w) of the amended Information Technology Act, 2000 defines the term "intermediary" in the widest possible terms in the following manner:—

> *"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes."*

The term "intermediary" has been defined in very wide terms by section 2(1)(w) of the Indian Information Technology Act, 2000 which includes any legal entity who on behalf of another person, receives, stores or transmits any particular electronic record or provides any service with respect to that record. It is pertinent to note that all network service providers, websites and online marketplaces have been brought within the ambit of the term "intermediary" under section 2(1)(w) of the amended Information Technology Act, 2000.

The law relating to Intermediaries is elaborated in section 79 of the Information Technology Act, 2000.

Section 79 of the Information Technology Act, 2000 is possibly one of the most important and significant provisions under the Indian Cyberlaw. This section's importance can further be noticed when one examines that this is the only solitary section which comes in Chapter XII entitled *"Intermediaries Not To Be Liable In Certain Cases"*. Section 79 of the Information Technology Act, 2000 as amended reads as under:-

Section 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 sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.*

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

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

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

- *(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act.*
- *(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner."*

Explanation.—For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary."

Section 79 is a code in its own self. This is so because this is the only relevant section which provides complete detailed provisions pertaining to the liability of intermediaries and other service providers which fall within the parameters of the applicability of the Information Technology Act, 2000.

It is important to point out that the Information Technology Act, 2000 had stipulated section 79. The said section has since been completely replaced by a

new language by virtue of the Information Technology (Amendment) Act, 2008. Before one examines the legal position pertaining to liability of intermediary, it is important to have a historical perspective of how the Indian Cyberlaw being the Information Technology Act, 2000 has dealt with the said subject since the year 2000. Prior to moving forward and discussing the provisions of section 79 of the Information Technology Act, 2000 as amended, it is imperative to have a look as to what was the colour and nature of the language of section 79 under the Information Technology Act, 2000, prior to the amendments.

Section 79 of the original Information Technology Act, 2000 stated as follows:—

"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 or 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."

Section 79 of the IT Act, 2000 detailed the liability of network service providers. The very tenor of the language categorically showed that the law presumed that the network service providers shall be liable in a majority of cases and only in certain specified cases would the network service providers not be liable. This interpretation found further credence from the usage of the words "for the removal of doubts" in section 79. Section 79 was thus in the nature of a clarificatory section. Also, it was in a declaratory mode as it used the words" it is hereby declared".

This section gave a definition of "network service provider". *Explanation (a)* to section 79 provided that network service provider means an intermediary.

The term "intermediary" had been defined under section 2(1)(w). A perusal of the then section 2(1)(w) demonstrated that the term "intermediary" had only been defined with reference and with respect to any particular electronic message to mean any person, who, on behalf of another person, receives, stores or transmits that message or provides any service with respect to that message. Section 79 did not talk merely about any particular electronic message. It went on to mention about third party information or data.

"Information" has been defined in section 2(1)(v) of the IT Act, 2000 to mean data, text, images, sound, voice, codes, computer programmes, software and databases or microfilm or computer generated microfiche. Further "data" had been defined under section 2(1)(o) of the IT Act, 2000 to mean a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer

network. Further, the representation of information, knowledge, facts, concepts or instructions may be in any form including computer printouts, magnetic or optical storage media, punched cards, punched tapes or the same may be stored internally in the memory of the computer.

Any intermediary concerned with the relevant business of providing network service would come within the definition of "network service provider". The liability had gone much further as the words used were "network service provider" rather than a narrower version "Internet Service Provider or ISP".

Thus, the term "network service provider" not only included Internet Service Providers but also, all other intermediaries who were in the business of network service providing. This *Explanation* further expanded the scope of "network service provider to include even those categories of providers, who, technically and practically may not be conceived to be network service providers, but who were deemed to be network service providers by means of their being intermediaries.

The then section 79 declared certain cases where a network service provider shall not be liable. Barring the specified cases in section 79, in all other cases, any person providing any service as a network service provider was liable for any third party information or data made available by him.

This section was different in its approach in the sense that it shifted the *onus* of proof from the prosecution to the network service provider. Normally speaking, a person is presumed to be innocent unless proved guilty in jurisprudence. This means that the onus of proving the guilt of the accused is on the prosecution and if the prosecution is not able to carry out its duty in a proper way, to the satisfaction of the court, the accused is liable to be acquitted.

But under the then section 79, the contrary principle was adopted which became counter-productive in the years following the year 2000. Under section 79, if you were a network service provider, you were presumed to be guilty unless proved innocent and the *onus* of proving innocence was on the network service provider. This section amounted to putting the horse before the cart and gave rise to practical difficulties under the IT Act, 2000.

Explanation (b) to section 79, explained the term "third party information" to mean any information dealt with by a network service provider in his capacity as an intermediary. This third party information must necessarily originate from an independent source and is aimed at a distinct destination. Thus, a network service provider was absolutely made liable for information providing any third party or data made available by him on his service. Only in two specified conditions was the concerned network service provider not made liable.

The first excepted condition detailed under the then section 79 was that if a network service provider was able to prove that the offence or contravention was committed without his knowledge, in that case, the network service provider shall not be liable for any third party data or information made available by him on his service. Section 79 used the word "knowledge" which meant legal knowledge.

It is important to note that network service provider had to prove his lack of knowledge of the concerned offence or contravention. The law did not give any parameters as to how and in what particular manner, the network service provider

was supposed to prove his lack of knowledge of the offence or contravention. Ordinarily, the lack of knowledge can be proved either by circumstantial or by specific direct evidence. It is also true that in a majority of cases, direct evidence about lack of knowledge is not forthcoming.

The second excepted condition under section 79 of the Information Technology Act, 2000 stated that, if a network service provider proved that he had exercised all due diligence to prevent the commission of such offence or contravention, in that case the network service provider shall not be liable for any third party data or information made available by him on his service. The second exception under section 79 also had its own set of problems inasmuch as it was not clear as to how the excepted condition could be proved by a network service provider, in legal proceedings before a court of law.

However after the coming into effect of the Information Technology Act, 2000, for couple of years, people were not even aware about the existence of section 79. However, it was some high-profile cases which brought the attention of the relevant stakeholders to the importance and significance of section 79 of the Information Technology Act, 2000.

One of the first cases pertaining to the liability of network service providers was the *Bank NSP* case. In the said case, a bank employee had used the bank's network, for the purposes of sending defamatory and derogatory e-mail. The Bank was sued in its capacity as a network service provider and intermediary. In the said case for the first time the Delhi High Court had passed orders against the bank in its capacity as the intermediary relying upon the requirements of section 79 of the Information Technology Act, 2000.

Section 79 of the Information Technology Act, 2000 came into sharp focus in the mid 2000 when the *Baazee.com* case took place.

Baazee.com case originated from the famous DPS MMS which showed a schoolgirl giving oral sex to her classmate. The said MMS was recorded on a phone and was initially meant for private circulation. However, it leaked out in the public domain. A student at IIT Kharagpur tried to monetize the said DPS MMS by posting a post on the online auction portal *Baazee.com*. The said post offered to sell the said DPS MMS for consideration. Due to the said post, a number of downloads were made by people. In that case, the CEO of *Baazee.com* was arrested on the grounds that *Baazee.com* was an intermediary and network service provider. The CEO of *Baazee.com* was subsequently released and charge-sheet filed. The charge-sheet was sought to be quashed by filing a petition before the Delhi High Court. The Delhi High Court dismissed the petition by a detailed judgment.

The Delhi High Court had held that *Baazee.com* in its capacity as the intermediary had failed to exercise diligence since its filters were faulty and allowed content that was pornographic in nature to pass through, despite the listing itself having of same content and further the said website in its capacity as the intermediary did not account for any changes in its policy to tackle with the possibility of such content being listed on its website in the future. The Delhi High Court had held as follows:—

"Investigation proves that the MD of Baazee.com[1], 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. The investigations found that the policy makers of the company were negligent in dealing with the matter and failed to exercise due diligence."

Baazee.com/Avnish Bajaj case is one of the most significant cases in the history of Indian Cyberlaw jurisprudence. In the said case, the law-enforcement initiated action against Mr. Avinish Bajaj, CEO, Baazee.com given the role of Baazee.com as a network service provider in enabling the publication and transmission of obscene DPS MMS-related content. The arrest of the CEO of Baazee.com and his subsequent release on bail after few days shocked the Indian corporate industry. The entire public sector was up in arms against section 79 of the Information Technology Act, 2000. Their argument was that there was no legal rationale or basis for arresting or initiating criminal action against a service provider company's CEO.

While summarizing its judgment, Delhi High Court highlighted that the *Baazee.com* 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 and that it may be useful to look at the legislative response in other common law jurisdictions.

Thereafter, given the huge uproar in the Indian corporate sector over the applicability and interpretation of section 79 of the Information Technology Act, 2000, various stakeholders put pressure upon the Government on the need to make appropriate changes under section 79 of the Information Technology Act, 2000. Their contention was that section 79 of the Information Technology Act, 2000 was very broad and capable of varied subjective interpretations by different stakeholders and that there was a case made out for narrowing the scope of applicability of section 79 of the Information Technology Act, 2000.

Consequently, the Government embarked upon a process of re-examining the provisions of Information Technology Act, 2000 and thereafter proposed amendments in the Parliament. The Parliament referred the said proposed amendments to be examined by the Parliamentary Standing Committee on Information Technology.

The Parliamentary Standing Committee submitted its report to the Government in late 2007. The relevant recommendations from the Parliamentary Standing Committed, headed by Sh. Nikhil Kumar, Member of Parliament, about section 79 of the Information Technology Act, 2000 recommended as follows:

"Definition and role of Intermediary and liability of network service"

8. Section 2(w) of the IT Act defines 'intermediary' with respect to any particular message as any person who on behalf of any other person receives, stores or transmits that message or provide any service with respect to that message. The Committee note that clause 4 sub-clause (F) of the Bill now seeks to define the term 'intermediary' as

1. CRL.M.C. 3066/2006 page 37 of 53 decided by Delhi High Court.

any person who on behalf of another person receives, stores or transmits electronic records or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes. It also seeks to explicitly exclude 'body corporate' as referred to in section 43(A) of the principal Act as an intermediary. The Committee also find that clause 38 of the Bill proposes to substitute the entire Chapter XII of the principal Act whereby the intermediaries are absolved of liability in certain cases. In some other situations, the culpability of the intermediaries has been fixed. To exercise further control over the intermediaries, clause 38 also stipulates that they shall observe such other guidelines as the Central Government may prescribe in the matter under sub-section 4 of section 79. After carefully going through the various proposals, the Committee are constrained to point out that the definition and role of intermediaries sought to be made through the amendments are not very clear, particularly with regard to the exclusion of body corporate referred to in section 43 (A) of the Bill. They, therefore, desire that the Department should re-examine clause 4 (F) of the Bill so that there is no scope for ambiguity while interpreting the definition and role of the intermediaries.

9. The Committee observe that under the existing provision of the IT Act, 2000 the network service providers are made liable for all third party content or data. But under the proposed amendments, the intermediaries/service providers shall not be liable for any third party information data, or communication link made available by them, except when it is proved that they have conspired or abetted in the commission of the unlawful act. The Department's reasoning for not making the intermediaries/service providers liable in certain cases is that a general consensus was arrived at, while discussions were going on the amendments to the IT Act, to the effect that the intermediaries/service providers may not be knowing what their subscribers are doing and hence they should not be penalised. The Committee do not agree with this. What is relevant here is that when their platform is abused for transmission of allegedly obscene and objectionable contents, the intermediaries/service providers should not be absolved of responsibility. The Committee, therefore, recommend that a definite obligation should be cast upon the intermediaries/service providers in view of the immense and irreparable damages caused to the victims through reckless activities that are undertaken in the cyber space by using the service providers' platform. Casting such an obligation seems imperative, more so when it is very difficult to establish conspiracy or abetment on the part of the intermediaries/service providers, as also conceded by the Department.

10. What has caused further concern to the Committee, in the above context, is that the Bill proposes to delete the words 'due diligence' as has been existing in section 79 of the principal Act. The Department's logic for the proposed removal of the words 'due diligence' is the intention to explicitly define the provisions under section 79 pertaining to exemption from liability of network service providers. The Department have further contended that the words 'due diligence' would be covered under the guidelines which the Central Government can issue under sub-section 4 of section 79 of the principal Act. The Committee do not accept the reasoning of the Department as they feel that removing an enabling provision which already exists in the principal Act and leaving it to be taken care of by the possible guidelines makes no sense. They are in agreement with the opinion of some of the investigating agencies that absence of any obligation to exercise 'due diligence' would place some of the intermediaries like online auction sites/market places in an uncalled for privileged position thereby disturbing the equilibrium with similar entities that exist in the offline world. The Committee also feel that if the intermediaries can block/eliminate the alleged objectionable and obscene contents with the help of technical mechanisms like filters and inbuilt storage intelligence, then they should invariably do it. The Committee is of the firm opinion that if explicit provisions about blocking of objectionable material/ information through various means are not codified, expecting selfregulation from the intermediaries, who basically work for commercial gains, will just remain a pipedream. The Committee, therefore, recommend that the words 'due diligence' should be reinstated and made a pre-requisite for giving immunity to intermediaries like online market places and online auction sites".

The said report was with the Government who was examining the same. Thereafter, the 26/11 Mumbai attacks took place, which propelled the Government into action. The Government introduced and got passed from the Parliament the Information Technology (Amendment) Act, 2008. The said Information Technology (Amendment) Act, 2008 replaced the old section 79 with completely new language. These amendments came into effect from 27th October, 2009.

Having examined the historical context of section 79 of the Information Technology Act, 2000 and the various developments pertaining to its jurisprudence, we now proceed forward to examine the scope, applicability and import of section 79 of the amended Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act, 2008.

The first remarkable feature about the amended section 79 of the Information Technology Act, 2000 is that it has increased the ambit of its applicability. From the mere context of the earlier section 79 of the Information Technology Act, 2000 being applicable only to network service providers, the scope and ambit of applicability of the amended section 79 of the Information Technology Act, 2000 has been dramatically increased. Now, the amended section 79 of the Information Technology Act, 2000 is applicable to intermediaries.

Section 79 of the amended Information Technology Act, 2000 is also applicable to all kinds of service providers given the specific definition of the term "intermediary". Section 2(1)(w) of the amended Information Technology Act, 2000 has defined the term "intermediary", with respect to any particular electronic records to mean 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 "intermediary" includes specifically 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. Thus, all kinds of service providers would clearly fall within the ambit of the definition of the term "intermediary". Thus, any service provider of any service of any kind whatsoever, whether direct or indirect, which is provided on a computer platform or which is available using computer network, would also

qualify to be an "intermediary" within the meaning of section 2(1)(w) of the amended Information Technology Act, 2000. Today, in the context of electronic ecosystem, a large number of value added services are being provided by various service providers as also by content service providers. The value-added services are providing various value additions for effective and more productive use of electronic/communication devices. All the said service providers will also be covered within the ambit of the term "intermediary".

Given the increased usage of electronic devices, electronic records, as are retained by intermediaries, today are extremely important in the context of not just adjudication of disputes but also in the context of investigation and prosecution of cyber crimes.

Section 79 states the liability of all intermediaries. This provision is an absolute provision and overrides anything inconsistent therewith contained in any other law for the time being in force. However, section 79(1) is subject to the provisions of section 79(2) & (3).

The term "third party information" has been defined in the *Explanation* to section 79, to mean any information dealt with by an intermediary in his capacity as an intermediary.

The term "information" has been defined under section 2(1)(v) of the amended Information Technology Act, 2000.

By and large, the intermediaries shall not be liable for any third party information, data or communication link made available or hosted by them. However, this proposition is subject to the provisions of section 79(2) & (3). The said intermediary will not be liable if the three conditions stipulated under section 79(2) of the amended Information Technology Act, 2000 are fulfilled.

The first important condition is that the intermediaries have to ensure that their function is limited to providing access to electronic ecosystems and communication system over which information made available by third parties is transmitted or temporally stored or hosted.

Thus, the only focus that the intermediary has to ensure is that its function is limited to providing access to the electronic ecosystems. The law does not stipulate that it needs to own or have any proprietary rights over the said electronic ecosystems. The law does not even talk about the various licensing requirements in this regard. How the access is provided to the electronic ecosystems by the intermediary is also not the concern of the law. The role of the intermediary must only be limited solely to providing access to electronic ecosystems over which information made available by third parties, is transmitted or temporally stored or hosted.

The second mandatory condition that the intermediary must satisfy is that 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.

This mandatory requirement under section 79(2)(b) is of greatest significance and is one of the greatest magnitude. The intermediary must ensure that it does not initiate the transmission of any third party data, which could be done by the parties. The intermediary also needs to ensure that it does not select the receiver of transmission.

Section 79(2)(b) is based on the fundamental premise that the intermediary must not exercise any "control" over the information in question for the purposes of claiming protection under section 79 of the Information Technology Act, 2000.

The third important mandatory condition under section 79(2)(b) is that the intermediary does not select or modify the information contained in the transmission. This is so because, a lot of services providers today piggy ride the information and bundle the information contained in the transmission with their advertisements or advertisement messages. This is happening in such a manner that when the receiver of the transmission receives information contained in the transmission, he not only receives the original information but also receives a lot of other information pertaining to the products and services provided by the service provider. This would qualify as a modification within the meaning of section 79(2)(b) of the amended Information Technology Act. Thus, service providers need to be extremely carefull, as to how they deal with the information contained in the transmission, when it is transmitted from the sender to the receiver using the electronic ecosystems including intermediary provided access.

The fourth important condition stipulated under section 79 by section 79(2)(c) is the mandatory requirement that the intermediary must observe due diligence while discharging his duties under the Information Technology Act, 2000 as amended and also observe such other guidelines as the Central Government may prescribe in this regard.

Section 79(2)(c) is the foundation and fulcrum on which the assumption of liability principle initiated by section 79 of the amended Information Technology Act, 2000 is based. The law mandates a duty of observing due diligence upon the service provider while discharging his duties under the Information Technology Act, 2000. Since, section 79(2)(c) mandates observance of due diligence while discharging its duties under the amended Information Technology Act, 2000, the intermediary only needs to ensure that it complies with all the parameters as stipulated by the amended Information Technology Act, 2000. Whatever parameters are applicable to the services of the intermediary, have to be duly complied with. In case, if the intermediary does not comply with any one of the stipulated conditions and terms of the amended Information Technology Act, it shall be deemed to have not done due diligence while discharging his duties under this Act.

It is important to note that section 79(2) has three distinct separate clauses being (a), (b) and (c). The law stipulates that intermediary must comply with all the three conditions stipulated under section 79(2).

Clearly one of the biggest messages that section 79 brings in the context of intermediaries is the factum that they have to observe due diligence while discharging their obligations under the Information Technology Act, 2000.

To begin with, the words "due diligence" have neither been defined under the Information Technology Act, 2000 nor under the Information Technology (Amendment) Act, 2008. Due diligence as a concept, had been engaging the attention of jurisprudence for a long period of time. However, it is pertinent to note that the law relating to due diligence has developed basically in the context of the actual world and not in relation to the electronic environment, Internet or the digital ecosystem. It goes without saying that an intermediary would be providing his services, which are connected with or somehow related to the computer network, electronic environment and all kinds of perceivable electronic networks. The standards and parameters that are accepted of due diligence in the electronic world concerning the e-format are entirely different in their nature, scope and perspective than the perspectives relating to due diligence in the real world.

At the time of writing, there are no well developed universally recognized standards of due diligence in the electronic environments. Another problem is how and in what particular way, would due diligence be judged? Would due diligence be judged in terms of money? For example, would due diligence mean spending of a specified amount of money by an intermediary, in direct proportion to the total volume of business? Or is due diligence going to be judged from standards of technology, as for example requiring a service provider to adopt and use the technological standards as specified by regulation to be an indication of it being duly diligent? Or is due diligence going to be measured in terms of the test of a reasonable man? In the actual world, the test of a reasonable man with reasonable intelligence is a good deciding factor for establishing due diligence. However, we will have difficulties in applying the concept of a reasonable man in context of online environment. Should the test of a reasonable man be made the touchstone for deciding due diligence of an intermediary?

In the actual world, established community behaviour over a number of years and universally accepted standards have refined the test of a reasonable man to mean what a reasonable man with a reasonable mind would do in a particular situation. However, with the coming of the electronic age and electronic environment, we would have difficulties in hand, given the inherent nature of the electronic environment.

For example, a reasonable man would look left and right to ensure that no vehicle is coming, before crossing a road. However, the situations raised by electronic networks are far more complex. Any one situation over the electronic network can result in a number of logical and reasonable responses. As such, it would be difficult to apply the test of a reasonable man in the context of electronic networks.

It is pertinent to point out that while the old section 79 of the Information Technology Act, 2000 had used the word "all due diligence", the said word has now been amended to only refer to "due diligence". Thus, due diligence as referred to under section 79 of the amended Information Technology Act, 2000, really refers to reasonable due diligence by an intermediary.

There is the land mark judgment on section 79 which relates to a very famous case of *Sanjay Kumar Kedia* v. *Narcotics Control Bureau*, AIR 2010 SC (Supp) 744. *In this case the Hon'ble Supreme Court has laid down a principle stating section 79 will not grant immunity to an accused who has violated the provisions of the Act as this provision gives immunity from prosecution for an offence only under Technology Act itself.*

The term "due diligence" describes a general duty to exercise care in any transaction. Due diligence sounds impressive but ultimately it translates into basic commonsense success factors such as "thinking things through" and "doing your homework"

Pavan Duggal Associates is India's niche law firm which has carried out due diligence for different stakeholders in the intermediary ecosystem. These due diligences have helped the relevant stakeholders to comply with the provisions of law, given the specific nature, ambit, scope and applicability of their respective services offerings.

One basic question that preoccupies human intellect is whether confidentiality can be maintained while doing the due diligence. It would be wrong to say that there can be no breach of confidentiality, as certain activities conducted during due diligence can breach confidentiality. For that reason, it is a must that due diligence is done meticulously and the person conducting due diligence should be bound contractually to maintain confidentiality.

It is clear that in the absence of objective parameters, which constitutes due diligence for intermediary, the interpretation of due diligence for intermediary would clearly be subjective and would depend upon the subjective thought process of the relevant judicial authorities examining the same. Further, it is interesting to note that the standard of due diligence will also vary with the nature of the contravention. Clearly, the burden of proving the fact that service provider in its capacity as the intermediary had observed due diligence while discharging its obligations under the amended Information Technology Act, 2000, lies on the service provider.

Section 79(3) further stipulates the conditions in which the exemption from liability for any third party information, data or communication link made available or hosted by an intermediary would not be applicable. Section 79(3) states that the provision of the section 79(1) shall not apply if any of the two conditions stipulated therein are met. An intermediary shall continue to be liable for third party information, data or communication link made available or hosted by him if the intermediary has conspired, abetted, aided, induced, whether by threats or promise or otherwise, in the commission of unlawful act. Thus, the moment the intermediary has participated directly or indirectly in the commission of unlawful act, whether actively or passively, the exemption from liability for third party information, data or communication link made available or hosted by the intermediary shall not be applicable.

Further, if upon receiving actual knowledge or being notified by the appropriate Government or its agencies that any information, data or communication link residing in or connected to computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to either expeditiously remove or disable access to that material on that computer resource without vitiating the evidence in any manner, the intermediary shall continue to be liable for all third party data or information made available by them.

The actual knowledge can be received by the intermediary either from any concerned user, subscriber or other person by their communication in writing or by a legal notice indicating that any information, data or communication link residing in or connected to computer resource controlled by intermediary, is being used to commit the unlawful act. Further, the intermediary can also be notified by the appropriate Governments, Central Government or State Governments or any of its agencies including law enforcement agencies of committing of any unlawful act using the information, data or communication link residing in or connected to computer resource controlled by the intermediary. Once, the intermediary has received actual knowledge or has been notified of any provision of an unlawful act using any data, information or communication link residing in or connected to computer resource controlled by the intermediary, the intermediary has been mandated to expeditiously act and remove or disable access to the said material on its computer resource. Further, the intermediary has been cast with the mandatory duty of ensuring that while it removes or disables access expeditiously to the offending material on its computer resources, it does not vitiate the evidence in any manner. In case, the intermediary is not able to carry out these mandatory duties, it shall continue to be liable for all third party information, data or communication link made available or hosted by him.

The intermediary is liable, if it fails to comply with the mandatory requirements of the section 79(2) & (3) of the amended Information Technology Act, 2000. In such a scenario, the intermediary could have exposure to legal consequences, both civil and criminal. The civil consequences could involve being sued for and paying damages by way of compensation up to rupees five crores per contravention as per the summary procedure provided under section 43 of the Information Technology Act, 2000. In addition, if the said contraventions deals with sensitive personal data and due to the breach of the security of the same, loss is caused to some person, damages by way of compensation could also be awarded against the intermediary under section 43A of the amended Information Technology Act, 2000.

The criminal liability could consist of imprisonment for the top management of the intermediary legal entity, which could extend to three years' imprisonment and five lakh rupees fine. Further, in case, the computer resources of the intermediary are being used to commit cyber terrorist acts, then the top management of the intermediary could also be exposed to criminal liability under section 66F which consists of life imprisonment and also fine. This is so by virtue of the operation of section 85 of the Information Technology Act, 2000, which stipulates the offences by companies. Generally, service providers are companies. Whenever offences are done by companies, section 85 of the amended Information Technology Act comes into play.

Section 85 of the Information Technology Act, 2000 states as follows:

> *"(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 pun.shed accordingly:*
>
> *Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves tl at 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 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 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."*

The net effect of section 85 is that where any offence is committed by a company, every person, who, at the time the contravention is 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 also be guilty of the said contravention and shall be liable to proceeded against and punished accordingly. Of course, the law further provides the exit route for the top management from such exposure to criminal liability. For exiting from liability under the Information Technology Act, 2000, every person, who, at the time the contravention is committed, was in-charge of and was responsible to the company for the conduct of the business of the company, has to prove two things:—

(a) That the contravention took place without his knowledge, or

(b) That he exercised all due diligence to prevent such contravention.

Here again, the concept of due diligence has been invoked. Under section 85 of the amended Information Technology Act, 2000, the *onus* of proof is upon the top management of the concerned intermediary company. It is important to note that the *onus* of proof under section 85 of the Information Technology Act, 2000 is much heavier as it uses the word "all due diligence" as compared to section 79, which only uses the world "due diligence"

The Indian Cyberlaw has married the requirement of due diligence alongwith the requirements of section 79(3)(b). Thus, the requirements of due diligence are also coupled with the requirement upon the service provider that upon receiving actual knowledge or 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 service provider in its capacity as an intermediary, is being used to commit the unlawful act, the service provider/ intermediary must expeditiously remove or disable access to the material on that

resource without vitiating the evidence in any manner whatsoever. Thus, the knowledge requirement in conjunction with the parameter of due diligence are clearly two most important parameters that need to be kept in mind by the service provider, while discharging its obligation under the law.

At this juncture it is important to examine the Red Flag Test that has been laid in the United States of America in the case of *Viacom* v. *YouTube*. In the said case, the said test was laid down in the following terms:—

> *"The "red flag" test has both a subjective and an objective element. In determining whether the service provider was aware of a "red flag," the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a "red flag"—in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances—an objective standard should be used."*

A service provider wishing to benefit from the limitation on liability under sub-section (c) must "take down" or disable access to infringing material residing on its system or network of which it has actual knowledge or that meets the "red flag" test, even if the copyright owner or its agent does not notify it of a claimed infringement.

Possibly the said Red Flag Test could be made applicable in India subject to the fact that it needs to be appropriately customized, keeping in mind the requirements of the electronic ecosystem in India.

Internationally speaking, there has been no unanimous approach adopted by nations at large on how to deal with intermediary liability. Different countries are coming up with their own distinctive mechanisms on how to deal with the roles of intermediaries and affixing appropriate legal liability for their roles.

Broadly speaking, two kinds of approaches have been adopted at the international level pertaining to intermediary liability. There is one set of nations that seeks to limit the civil and criminal liability of intermediaries in their capacity as technological intermediaries. In such cases, there is focus on self-regulation and on enabling the said intermediaries to take down the offending content at appropriate requests. In the event the said intermediary does not comply with such requests, does their exposure to civil and criminal liability start. In addition, we have the other school of thought across the world. In the said school of thought, Governments of different nations tend to hold intermediaries responsible for illegal content posted by users. In such cases, intermediaries are straddled with various civil and criminal liabilities for the purposes of ensuring orderly behaviour acceptable to societal norms.

While the United States is one of the prominent countries that have adopted the first school of thought, the second school of thought has been adopted by countries like India.

One of the significant parameter of section 79 is that the intermediary has to mandatorily observe due diligence while discharging his duties under the Act and also observes such other guidelines as the Central Government may prescribe in this regard.

Neither the Information Technology Act, 2000 nor the Information Technology (Amendment) Act, 2008 prescribed any specific guidelines in respect of how to observe due diligence by the intermediaries. The Information Technology (Amendment) Act, 2008 specifically states that the intermediary must observe due diligence while discharging his duties under this Act and also observe such other guidelines prescribed by the Central Government under the Information Technology Act, 2000 as to what would constitute due diligence in the context of intermediary.

It is pertinent to note that the Central Government, in exercise of powers granted to it under section 87(2)(zg) along with section 79(2) of the Information Technology Act, 2000, notified the Information Technology Rules, 2011. These are the set of four rules out of which 3 Rules are directly applied to all legal entities who qualify as intermediaries under the Information Technology Act, 2000. These Rules came into effect from 11th April, 2011.

The most significant of these Rules are the Information Technology (Intermediary Guidelines) Rules, 2011. The said Rules came into effect from 11th of April, 2011. These rules have further relied upon the definition of various terms in a manner so defined under the Information Technology Act, 2000.

These Rules further stipulate what kinds of due diligence is expected from intermediaries. Rule 3 of the Information Technology (Intermediary Guidelines) Rules, 2011 becomes an important indicator in this regard. Rule 3 of the said Rules states as follows:

> ***3. Due diligence to be observed by intermediary.***—*The intermediary shall observe following due diligence while discharging his duties, namely:*
>
> *(1) The intermediary shall publish the Rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person.*
>
> *(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that—*
>
> *(a) belongs to another person and to which the user does not have any right to;*
>
> *(b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;*
>
> *(c) harm minors in any way;*
>
> *(d) infringes any patent, trademark, copyright or other proprietary rights;*
>
> *(e) violates any law for the time being in force;*
>
> *(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;*
>
> *(g) impersonate another person;*

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.

(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2): provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in sub-rule (2).

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act."

Thus, the Information Technology (Intermediary Guidelines) Rules, 2011 actually mandate that all intermediaries should publish rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resources. Various kinds of contents have been barred under rule 3 of the Information Technology (Intermediary Guidelines) Rules, 2011. These are the kinds of content which the Rules and regulations and terms and conditions of intermediary must mandatorily inform its users, that they should not use the computer resources of intermediary to host, display, upload, modify, publish, transmit, update or share the so specified information.

When one reads rule 3 of the Information Technology (Intermediary Guidelines) Rules, 2011, it is clear that the law makers want certain content not to be dealt with in any manner, using the computer resources of the intermediaries. These contents include content or data or information that belongs to another person and to which the user does not have any right to. Rule 3(2)(b) has possibly generated the most controversy given the wide ambit and scope of the terms used therein. Rule 3(2)(b) states as follows:

> *"(2) Such Rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that—*
>
> *(b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever."*

It is pertinent to note that the Information Technology Act, 2000 as also the Information Technology Rules, 2011 do not provide legal definition of the various terms stipulated under rule 3(2)(b) of the Information Technology (Intermediary Guidelines) Rules, 2011. Given the fact that the law is silent on this, it is imperative to examine the scope of the meaning of the said terms used thereunder.

As such it will be imperative to examine the common parlance meaning of the said terms as we proceed forward.

Harmful

The word "Harmful" has been defined by the free dictionary as follows:— causing or tending to cause harm; injurious.[2]

Further, the word "Harmful" has been defined by the Oxford Learners' Dictionary, as follows: — causing or likely to cause harm.[3]

Title 76 , Chapter 10 of the Utah Criminal Code[4] deals with the terms "Harmful to minors", which mean that quality of any description or representation, in whatsoever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse when it:

(i) Taken as a whole, appeals to the prurient interest in sex of minors;

(ii) Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and

(iii) Taken as a whole, does not have serious value for minors. Serious value includes only serious literary, artistic, political or scientific value for minors.

Harass

According to Wikipedia, Harassment covers a wide range of behaviours of an offensive nature. It is commonly understood as behaviour intended to disturb or upset, and it is characteristically repetitive. In the legal sense, it is intentional behaviour which is found threatening or disturbing[5].

Further, the Oxford Learners Dictionary defines the word "harass" as:—

> *"to annoy or worry somebody by putting pressure on them or saying or doing unpleasant things to them.[6]"*

In *"Madhuri Mukund Chitnis* v. *Mukund Martand Chitnis"* on 29 September, 1988, (1990) 1 DMC 352, the Bombay High Court defined the term 'Harass' as follows:

> *8. The meaning of word "harass" in the Webster's Dictionary reads thus:— "To subject someone to continuous vexatious attacks, questions, demands or other unpleasantness."*

---

2. http://www.thefreedictionary.com/harmful
3. http://oxforddictionaries.com/definition/english/harmful
4. http://www.lectlaw.com/files/sex03.htm
5. http://en.wikipedia.org/wiki/Harassment
6. http://oald8.oxfordlearnersdictionaries.com/dictionary/harass

Blasphemous

According to Wikipedia, Blasphemy is the act of insulting or showing contempt or lack of reverence for a religious deity or the irreverence towards religious or holy persons or things. Law may discourage blasphemy as a matter of blasphemous libel, vilification of religion, religious insult or hate speech.[7]

Further, the meaning of the word "Blasphemous" in the Oxford Dictionaries reads thus:— "sacrilegious against God or sacred things; profane."[8]

Defamatory

According to Wikipedia, Defamation is the communication of a statement that makes a claim, expressly stated or implied to be factual, that may give an individual, business, product, group, government, religion, or nation a negative or inferior image. This can also be any disparaging statement made by one person about another, which is communicated or published, whether true or false, depending on legal state.[9]

In "*Bhagwan Singh* v. *Arjun Dutt*" on 29 May, 1920, 57 Ind Cas 1984 the Allahabad High Court held as follows:

In India "defamatory" means, or may include, words which "directly or indirectly lower the character or credit of a person in respect of his caste or calling."

Obscene

According to Wikipedia, an obscenity is any statement or act which strongly offends the prevalent morality of the time. It is derived from the Latin *obscaena* (offstage) a cognate of the Ancient Greek root*skene*, because some potentially offensive content, such as murder or sex, was depicted offstage in classical drama. The word can be used to indicate a strong moral repugnance, in expressions such as "obscene profits" or "the obscenity of war[10]"

The legal-dictionary.thefreedictionary defines the term "obscene" as a highly subjective reference to material or acts which display or describe sexual activity in an obviously disgusting manner, appealing only to "prurient interest," with no legitimate artistic, literary or scientific purpose[11]."

In "*Sopan S/O Vithal Shinde* v. *The State of Maharashtra*" on 27 February, 2008, the Bombay High Court held as follows:

"11. According to new Standard Dictionary, "obscene" means offensive to chastity, delicacy or decency. According to Black's Law Dictionary, "obscenity" means character or quality of being obscene, conduct, tending to corrupt the public merely by its indecency or lawness. According to Webster's New International Dictionary, "obscene" means disgusting to the senses, usually because of some filthy grotesque of unnatural quality, grossly repugnant to the generally accepted notions of what is appropriate."

7. http://en.wikipedia.org/wiki/Blasphemy
8. http://oxforddictionaries.com/definition/english/blasphemous
9. http://en.wikipedia.org/wiki/Defamation
10. http://en.wikipedia.org/wiki/Obscenity
11. http://legal-dictionary.thefreedictionary.com/obscene

In "*Abdul Rasheed* v. *State of Kerala*" on 21 May, 2008, Crl Rev Pet No. 615 of 2000, the Kerala High Court held as follows:

"The word obscene means what is offensive to modesty or decency which gives rise to emotions, nudeness filthiness and repulsiveness. The real test of obscenity is whether the pendency of the matter charged as obscene is to deprive and correct those whose minds are open to such immoral influences and to see whose hands the object of the sort may fall."

In "*Dr. Promilla Kapur* v. *Yash Pal Bhasin*," on 22 February, 1989 the Delhi High Court observed as follows:

"The word 'obscene' means what is offensive to modesty or decency which gives rise to emotions of lewdness, filthiness and repulsiveness. It was also held that there is some difference between the obscenity and pornography as the latter denotes writings, pictures etc. only intended to arouse sexual desire while the former may include writing etc. not intended to do so but which have that tendency and both, of course, offend against public decency and morals but pornography is obscenity in a more aggravated form."

Pornography/Pornographic

According to Wikipedia, Pornography is often referred to as "porn" and a pornographic work as a "porno". Pornography is the explicit portrayal of sexual subject matter. Pornography may use a variety of media, including books, magazines, postcards, photos, sculpture, drawing, painting, animation, sound recording, film, video, and video games. The term applies to the depiction of the act rather than the act itself, and so does not include live exhibitions like sex shows and striptease. A pornographic model poses for still photographs. A pornographic actor or porn star performs in pornographic films. If dramatic skills are not involved, a performer in porn films may also be called a *model*.[12] Pornographic films or sex films are films that depict sexual fantasies and seek to create in the viewer sexual arousal and erotic satisfaction. Such films usually include erotically stimulating material such as nudity and the explicit portrayal of sexual activity.[13]

Further, the meaning of word "Pornography" in the Oxford Dictionary reads as printed or visual material containing the explicit description or display of sexual organs or activity, intended to stimulate sexual excitement.[14]

The legal-dictionary.thefreedictionary defines the term "pornography" as pictures and/or writings of sexual activity intended solely to excite lascivious feelings, of a particularly blatant and aberrational kind such as acts involving children, animals, orgies, and all types of sexual intercourse. The printing, publication, sale and distribution of "hard core" pornography is either a felony or misdemeanor in most states. Since determining what is pornography and what is "soft core" and "hard core" are subjective questions to judges, juries and law

12. http://en.wikipedia.org/wiki/Pornography
13. http://en.wikipedia.org/wiki/Pornographic_film
14. http://oxforddictionaries.com/definition/english/pornography

enforcement officials it is difficult to define, since the law cases cannot print examples for the courts to follow.[15]

Pedophilia

According to Wikipedia, the word "Pedophilia" comes from the Greek: παις (*paîs*), meaning "child", and φ*λ*α (*philía*), "friendly love" or "friendship". This literal meaning has been altered toward sexual attraction in modern times, under the titles "child love" or "child lover", by pedophiles who use symbols and codes to identify their preferences. In law enforcement circles, the term "pedophile" is sometimes used in a broad manner to encompass a person who commits one or more sexually-based crimes that relate to legally underage victims. These crimes may include child sexual abuse, statutory rape, offenses involving child pornography, child grooming, stalking, and indecent exposure. Some forensic science texts, use the term to refer to a class of psychological offender typologies that target child victims, even when such children are not the primary sexual interest of the offender. The FBI, however, makes a point of acknowledging preferential sex offenders who have a true sexual preference for prepubescent children.[16]

The legal-dictionary.thefreedictionary defines the term "**Pedophilia n.**" as an obsession with children as sex objects. Overt acts, including taking sexual explicit photographs, molesting children, and exposing one's genitalia to children are all crimes. The problem with these crimes is that pedophilia is also treated as a mental illness, and the pedophile is often released only to repeat the crimes or escalate the activity to the level of murder.[17]

The meaning of word "paedophile" in the Oxford Dictionary reads as "a person who is sexually attracted to children."[18]

Libellous

The meaning of the word "Libellous" in thefreedictionary.com reads as "Involving or constituting a libel; defamatory."[19]

The term "libelous" has been defined by Merriam Webster Dictionary as Constituting or including a libel.[20] Further, the term "libel" defines as a written statement in which a plaintiff in certain courts sets forth the cause of action or the relief sought, a written or oral defamatory statement or representation that conveys an unjustly unfavourable impression, a statement or representation published without just cause and tending to expose another to public contempt (2): defamation of a person by written or representational means (3): the publication of blasphemous, treasonable, seditious, or obscene writings or pictures (4): the act, tort, or crime of publishing such a libel.[21]

15. http://legal-dictionary.thefreedictionary.com/pornography
16. http://en.wikipedia.org/wiki/Pedophilia#In_law_and_forensic_psychology
17. http://legal-dictionary.thefreedictionary.com/pedophilic
18. http://oxforddictionaries.com/definition/english/paedophile
19. http://www.thefreedictionary.com/libellous
20. http://www.merriam-webster.com/dictionary/libelous?show=0&t=1352551751
21. http://www.merriam-webster.com/dictionary/libel

The learner's dictionary defines the word "Libellous" as containing an untrue written statement that causes people to have a bad opinion of someone.[22]

Invasion of Privacy

The legal-dictionary.thefreedictionary defines the term "**Invasion of privacy**." as the intrusion into the personal life of another, without just cause, which can give the person whose privacy has been invaded, a right to bring a lawsuit for damages against the person or the entity that intruded. However, public personages are not protected in most situations, since they have placed themselves already within the public eye, and their activities (even personal and sometimes intimate) are considered newsworthy, *i.e.*, of legitimate public interest. However, an otherwise non-public individual has a right to privacy from: (1) intrusion on one's solitude or into one's private affairs; (2) public disclosure of embarrassing private information; (3) publicity which puts him/her in a false light to the public; (4) appropriation of one's name or picture for personal or commercial advantage.[23]

Invasion of privacy is the intrusion upon, or revelation of, something private. One, who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his/her private affairs or concerns, is subject to liability to the other for invasion of privacy.[24]

Hateful

The meaning of word "hateful" in thefreedictionary reads thus:— (1) Eliciting or deserving hatred, (2) Feeling or showing hatred, malevolent. Further hateful, detestable, odious, offensive, repellent: These often inter-changeable adjectives describe what elicits or deserves strong dislike, distaste, or revulsion. *Hateful* refers to what evokes hatred or deep animosity.[25]

According to Wikipedia, "**hateful**" may refer to: Someone or something full of hatred.[26]

Racially

The meaning of word "racial" in thefreedictionary reads thus:— 1. Of, relating to, or characteristic of race or races. 2. Arising from or based on differences among human racial groups. Racially refers to with respect to race; "racially integrated."[27]

The Macmillan Dictionary defines the term "racially" as in a way that is caused by someone's race or is related to someone's race. *e.g.*, a racially motivated crime, a racially mixed school.[28]

Ethnically

The meaning of word "ethnic" in thefreedictionary reads thus:— 1.a. Of, relating to, or characteristic of a sizable group of people sharing a common and

22. http://www.learnersdictionary.com/search/libelous
23. http://legal-dictionary.thefreedictionary.com/invasion+of+privacy
24. http://privacy.uslegal.com/what-constitutes-a-violation/
25. http://www.thefreedictionary.com/hateful
26. http://en.wikipedia.org/wiki/Hateful
27. http://www.thefreedictionary.com/racially
28. http://www.macmillandictionary.com/dictionary/british/racially

distinctive racial, national, religious, linguistic, or cultural heritage. b. Being a member of a particular ethnic group, especially belonging to a national group by heritage or culture but residing outside its national boundaries: ethnic Hungarians living in northern Serbia.[29]

According to Wiktionary, the terms "Ethnic" means, of or relating to a group of people having common racial, national, religious or cultural origins or Belonging to a foreign culture.[30] Ethnically refers to of, pertaining to ethnicity or ethnics.

Disparaging

The *meaning of word "Disparaging" in thefreedictionary* reads thus:— expressive of low opinion; "derogatory comments."[31] Further according to Wiktionary, the terms "*Disparaging*" means Insulting, ridiculing.[32]

Money Laundering

According to Wikipedia, "Money laundering" is the process of concealing the source of money obtained by illicit means.[33] The Business Dictionary defines the term "Money laundering", means Legitimization of illegally obtained money to hide its true nature or source (typically the drug trade or terrorist activities). Money laundering is effected by passing it surreptitiously through legitimate business channels by means of bank deposits, investments, or transfers from one place (or person) to another.[34]

Further section 3 of the Prevention of Money Laundering Act, 2002 defines offence of money laundering as under: "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering."

Gambling

Wikipedia defines the term "gambling" as, the wagering of money or something of material value (referred to as "the stakes") on an event with an uncertain outcome with the primary intent of winning additional money and/or material goods. Typically, the outcome of the wager is evident within a short period.[35] Further, the meaning of word "Gambling" in thefreedictionary reads thus:—1. A bet, wager, or other gambling venture. 2. An act or undertaking of uncertain outcome; a risk.[36]

It is pertinent to point out that the Bombay Prevention of Gambling Act, 1887 does not define the term gambling. section 3 of Bombay Prevention of Gambling Act, 1887 defines "**gaming**" as under:

29. http://www.thefreedictionary.com/ethnic
30. http://en.wiktionary.org/wiki/ethnic
31. http://www.thefreedictionary.com/disparaging
32. http://en.wiktionary.org/wiki/disparaging
33. http://en.wikipedia.org/wiki/Money_laundering
34. http://www.businessdictionary.com/definition/money-laundering.html
35. http://en.wikipedia.org/wiki/Gambling
36. http://www.thefreedictionary.com/Gambling

"In this Act" gaming" includes wagering or betting except wagering or betting upon a horse-race, or dog race when such wagering or betting takes place—

(a) on the day on which such race is to run, and

(b) in an enclosure which the licensee of the race-course, on which such race is to be run, has set apart for the purpose under the terms' of the licence issued under section 4 of the Bombay Race-Born. Courses Licensing Act, 1912 or as the case may be, of the Maharashtra Dog Race Courses Licensing Act, 1976 in respect of such race-courses or in any other place approved by the State Government on this behalf, and.

(c) between any individual in person, being present in the enclosure or approved place on the one hand, and such licensee or other person licensed by such licensee in terms of the aforesaid licence on the other hand or between any number of individuals in person in such manner and by such contrivance as may be permitted by such licence; but does not include a lottery.

Any transaction by which a person in any capacity whatever, employs another in any capacity whatever or engages for another in any capacity whatever to wager or bet whether with such licensee or with any other person shall be deemed to be "gaming":

Provided, nevertheless, that such licensee may employ servants, and persons may accept service with such licensee, or wagering or betting in such manner or by such contrivance as may be permitted in such licence. The collection or soliciting of bets; receipt or distribution of winnings or prizes in money or otherwise in respect of wagering or betting or any act which is intended to aid or facilitate wagering or betting or such collection, soliciting, receipt or distribution shall be deemed to be "gaming".

Thus, a cumulative examination of rule 3(2)(b) shows that very wide parameters have been incorporated therein with usage of words that have extremely wide connotation.

Further, the lawmakers were clear that any information that harms minors in any way must not be hosted, displayed, uploaded, modified, published, transmitted, updated or shared on the computer resources of any intermediary.

The lawmakers have further provided an additional ground under rule 3(2)(d) of content which should not be available on the intermediary's computer resource. This content relates to protection and preservation of Intellectual Property Rights of respective stakeholders. As such, any information that infringes patent, trademark, copyright or other proprietary rights of the relevant stakeholders should not be hosted, displayed, uploaded, modified, published, transmitted, updated or shared on the computer resources of the intermediary.

Rule 3(2)(e) provides that any information that violates any law for the time being in force, should not also be available on the computer resources of the intermediary nor the same should be dealt with in any manner whatsoever.

Given the cloak of anonymity that the Internet provides, large number of people today deceive or mislead the addressee of their communications or messages pertaining to origin of such communications or messages. As such, rule

3(2)(f) provides that the computer resources of the intermediary shall not be used to host, display, upload, modify, publish, transmit, update or share any information that deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or of menacing character.

Further, the law stipulates that users of computer resources of the intermediaries shall not host, display, upload, modify, publish, transmit, update or share any information that contains any software viruses. The law here seeks to distinguish difference between computer contaminant as defined under *Explanation (i)* to section 43 of the Information Technology Act, 2000 from the software viruses.

The term "computer contaminant" is far more wider in the manner as stipulated under section 43 of the Information Technology Act, 2000. However, the term "software viruses" as defined under rule 3(2)(h) is relatively very small as compared to the broad ambit of computer contaminants. The law mandates that users of computer resource of the intermediary shall not deal with information which contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource.

Rule 3(2)(e) pertains to protecting the sovereign interests of India. As such, the law mandates that the computer resources of the intermediaries shall not be used for the purposes of hosting, displaying, uploading, modifying, publishing, transmitting, updating or sharing any information which:-

(a) threatens the unity, integrity, defence, security or sovereignty of India;

(b) threatens the friendly relations with foreign States;

(c) threatens public order;

(d) causes incitement to the commission of any cognizable offence;

(e) Further prevents investigation of any offence;

(f) which is insulting to any other nation.

The terms used in the above parameters are very broad. Let us examine the scope of some of these terms:

Sovereignty:

In *"Sardar Govindrao* v. *State of Madhya Pradesh,"*, 7 May, 1982: AIR 1982 SC 1021: (1982) 3 SCR 729, the Supreme Court held as follows:

> *"According to Blacks' Legal Dictionary, 5th Edn., p. 1252 the legal conception of "**sovereignty**" is stated thus: "The supreme, absolute, and uncontrollable power by which any independent state is governed; supreme political authority, paramount control of the constitution and frame of government and its administration; the self-sufficient source of political power from which all specific political powers are derived; the international independence of a state, combined with the right and power of regulating its internal affairs without foreign dictation; also a political society, or state, which is sovereign and independent.*
>
> *"Sovereignty" means "supremacy in respect of power, dominion or rank; supreme dominion authority or rule". "Sovereignty" is the right to govern. The term "sovereignty" as applied to states implies "supreme, absolute, uncontrollable power by which any state is governed, and which resides within itself, whether residing in a single individual or a number of individuals, or in the whole body of the people." Thus, sovereignty, according to its normal legal connotation, is the supreme power which governs the body politic, or society which constitutes the state, and this power is independent of the particular form of government, whether monarchial, autocratic or democratic."*

Integrity

According to Wikipedia, Integrity is a concept of consistency of actions, values, methods, measures, principles, expectations, and outcomes. In ethics, integrity is regarded as the honesty and truthfulness or accuracy of one's actions. Integrity can be regarded as the opposite of hypocrisy. The word "integrity" stems from the Latin adjective *integer* (whole, complete). In this context, integrity is the inner sense of "wholeness" deriving from qualities such as honesty and consistency of character. As such, one may judge that others "have integrity" to the extent that they act according to the values, beliefs and principles they claim to hold.[37]

The Merriam-Webster Dictionary defines the term "Integrity"[38] as **1.** firm adherence to a code of especially moral or artistic values: incorruptibility, **2:** an unimpaired condition: soundness **3:** the quality or state of being complete or undivided: completeness

Further, as per the Oxford Dictionary, the word "**Integrity**"[39] means **1.** the quality of being honest and having strong moral principles, **2.** the state of being whole and undivided, the condition of being unified or sound in construction.

In *"Vijay Singh* v. *State of Uttar Pradesh,"* on 13 April, 2012, Civil Appeal No. 3550 of 2012, [Arising out of SLP(C) No. 27600 of 2011], the Supreme Court held as follows:

> *"14. Integrity means soundness of moral principle or character, fidelity, honesty, free from every biasing or corrupting influence or motive and a character of uncorrupted virtue. It is synonymous with probity, purity, uprightness rectitude, sinlessness and sincerity. The charge of negligence, inadvertence or unintentional acts would not culminate into the case of doubtful integrity."*

Unity

The Merriam-Webster Dictionary defines the term "**Unity**[40]" as **1 a:** the quality or state of not being multiple **2 a:** a condition of harmony; **b:** continuity without deviation or change (as in purpose or action), **3 a:** the quality or state of being made one.

The Collins Dictionary defines the term "**Unity**[41]" as the state or quality of being one; oneness; the act, state, or quality of forming a whole from separate parts; something whole or complete that is composed of separate parts; mutual

37. http://en.wikipedia.org/wiki/integrity
38. http://www.merriam-webster.com/dictionary/integrity
39. http://oxforddictionaries.com/definition/english/integrity
40. http://www.merriam-webster.com/dictionary/unity
41. http://www.collinsdictionary.com/dictionary/english/unity

agreement; harmony or concord Ò! the participants were no longer in unity; uniformity or constancy

Further as per the Oxford Dictionary, the word "**Unity**"[42] means the state of being united or joined as a whole; the state of forming a complete and harmonious whole, especially in an artistic context.

According to Wikipedia, Unity is the state of being undivided or unbroken.[43]

Public Order

In *"The Superintendent, Central ...* v. *Ram Manohar Lohia,"* AIR 1960 SC 633: (1960) 2 SCR 821, the Supreme Court of India held as follows:

> *"The expression public order" has a very wide connotation. Order is the basic need in any organised society. It implies the orderly state of society or community in which citizens can peacefully pursue their normal activities of life.*

The words "public order" were also understood in America and England as offences against public safety or public peace. The Supreme Court of America observed in Cantewell *v.* Connecticut *(1) thus:*

> *"The offence known as breach of the peace embraces a great variety of conduct destroying or menacing public order and tranquillity. It includes not only violent acts and words likely to produce violence in others. No one would have the hardihood to suggest that the principle of freedom of speech sanctions incitement to riot. When clear and present danger of riot, disorder, interference with traffic upon the public streets, or other immediate threat to public safety, peace, or order appears, the power of the State to prevent or punish is obvious. "*

The foregoing discussion yields the following results: (1) "Public order" is synonymous with public safety and tranquillity: it is the absence of disorder involving breaches of local significance in contradistinction to national upheavals, such as revolution, civil strife, war, affecting the security of the State"

In *"Municipal Council Raipur* v. *State of Madhya Pradesh"* AIR 1970 SC 1923: (1970) 1 SCR 915, the Supreme Court of India held as follows:

> *"'Public Order' is an expression of wide connotation and signifies that state of tranquillity which prevails among the members of a political society as a result of internal regulations enforced by the government which they have established."*
>
> *Later he observed:*
>
> *"'Public safety' ordinarily means security of the public or their freedom from danger. In that sense, anything which tends to prevent danger to public health may also be regarded as securing public safety."*
>
> *The learned counsel urges that "public order" includes "public safety" and the latter comprises "public health". We see no force in this contention and* Ramesh Thappar's *case does not say so. In our view "Public Order" in this context means public peace and tranquillity."*

42. http://oxforddictionaries.com/definition/english/unity
43. http://en.wikipedia.org/wiki/Unity

Security

According to Wikipedia, Security is the degree of protection to safeguard a nation, union of nations, persons or person against danger, damage, loss, and crime.[44]

Wikipedia defines the term "Security of State" as all the utterances intended to endanger the security of the State by crimes of violence intended to overthrow the government, waging of war and rebellion against the government, external aggression or war, etc., may be restrained in the interest of the security of the State. It does not refer to the ordinary breaches of public order which do not involve any danger to the State.[45]

Defence

The meaning of word "defence" in thefreedictionary reads thus:— 1. resistance against danger, attack, or harm; protection, 2. a person or thing that provides such resistance, 3. a plea, essay, speech, etc., in support of something; vindication; justification 4. a country's military measures or resources 5. *Law* a defendant's denial of the truth of the allegations or charge against him.[46]

According to Wikipedia, Defence may refer to: Tactics and strategy of defending against attack.[47]

Insult

According to Wikipedia, an insult is an expression, statement (or sometimes behaviour) which is considered degrading, offensive and impolite.[48]

The meaning of word "Insult" in thefreedictionary reads thus:— 1. a. To treat with gross insensitivity, insolence, or contemptuous rudeness.. b. To affront or demean: an absurd speech that insulted the intelligence of the audience. 2. Obsolete To make an attack on.[49]

Cognizable Offence

Section 2(c) of the Cr. P.C. defines the term "cognizable offence", means an offence for which, and "cognizable case" means a case in which, a police officer may, in accordance with the First Schedule or under any other law for the time being in force, arrest without warrant.

Incitement

According to Wikipedia, Incitement consists of persuading, encouraging, instigating, pressuring, or threatening so as to cause another to commit a crime.[50]

The meaning of word "Incitement" in thefreedictionary reads an act of urging on or spurring on or rousing to action or instigating;[51]

44. http://en.wikipedia.org/wiki/Security
45. http://en.wikipedia.org/wiki/Freedom_of_expression_in_India
46. http://www.thefreedictionary.com/defence
47. http://en.wikipedia.org/wiki/defence
48. http://en.wikipedia.org/wiki/Insult
49. http://www.thefreedictionary.com/insulting
50. http://en.wikipedia.org/wiki/incitement
51. http://www.thefreedictionary.com/incitement