AN EVALUATIVE STUDY OF LEGISLATIVE MEASURES

This chapter is devoted to focus on legislative measures adopted in order to control the cyber crimes. Some of cyber cases filed with the police or courts have been analyzed to understand the implications and the nature of punishments inflicted on the culprits. Some Case studies were also discussed at length to infer some useful findings.

Indian Cyber Laws:

According to Rohas Nagpal (2007), Indian Cyber Laws were official born on 17th October 2000 with the Information Technology Act, 2000 coming into force. This paper discusses 7 interesting case laws that I feel highlight the development of cyber legal jurisprudence in India over the last 7 years. This paper begins with a short outline of the various rules, regulations and orders that have been passed over the last 7 years. It then moves onto a brief discussion on the Indian law relating to cyber pornography and features the Avnish Bajaj (CEO of bazzee.com – now a part of the e-bay group of companies) case.

Again in his work titled, “Jurisprudence of Indian Cyber Law” Rohas Nagpal (2007) depicts that the primary source of cyber law in India is the Information Technology Act, 2000 (IT Act) which came into force on 17 October 2000. The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The IT Act also penalizes various cyber crimes and provides strict punishments (imprisonment terms up to 10 years
and compensation up to Rs 1 crore).

Minor errors in the Act were rectified by the Information Technology (Removal of Difficulties) Order, 2002, which was passed on 19 September 2002. An Executive Order dated 12 September 2002 contained instructions relating provisions of the Act in regard to protected systems and application for the issue of a Digital Signature Certificate.

The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques. Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to the Government bodies. On the same day, the Information Technology (Certifying Authorities) Rules, 2000 also came into force.

These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006.

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July 2001. Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates. These were issued on 16th December 2002. The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 also came into
force on 17th October 2000. These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers. The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT.

Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT. On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed.

These rules prescribe the qualifications and experience of Adjudicating Officers, whose chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of Service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

The appointment of adjudicating officers to decide the fate of multicrores cyber crime cases in India was the result of the public interest litigation filed by students of Asian School of Cyber Laws (ASCL). The Government had not appointed the Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the passage of the IT Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers.

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

Following this the Central Government passed an order dated 23rd March 2003 appointing the “Secretary of Department of Information Technology of each of the States or of Union Territories” of India as the adjudicating officers was passed. The Information Technology (Security Procedure) Rules, 2004 came into force on 29th October, 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. Also relevant are the Information Technology (Other Standards) Rules, 2003. An important order relating to blocking of websites was passed on 27th February, 2003. Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website. The Indian Penal Code (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.

Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act). In case of bank records, the provisions of the Bankers’ Book Evidence Act (as amended by the IT Act) are relevant. Investigation and adjudication of cyber crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act. The Reserve Bank of India Act was also amended by the IT Act.

1. Cyber Pornography

There is no settled definition of pornography or obscenity. What is considered simply sexually explicit but not obscene in USA may well be considered obscene in India. There have been many attempts to limit the availability of pornographic content on the Internet by governments and
law enforcement bodies all around the world but with little effect.

Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive.

Section 67 of the IT Act is the most serious Indian law penalizing cyber pornography. Other Indian laws that deal with pornography include the Indecent Representation of Women (Prohibition) Act and the Indian Penal Code.

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

This Section explains what is considered to be obscene and also lists the acts in relation to such obscenity that are illegal.

What constitutes obscenity in electronic form? To understand what constitutes obscenity in the electronic form, let us analyze the relevant terms: Any material in the context of this Section would include video files,
audio files, text files, images, animations etc. These may be stored on CDs, websites, computers, cell phones etc. Lascivious is something that tends to excite lust. Appeals to, in this context, means “arouses interest”. Prurient interest is characterized by lustful thoughts. Effect means to produce or cause. Tend to deprave and corrupt in the context of this Section means “to lead someone to become morally bad”. Persons here refers to natural persons (men, women, children) and not artificial persons (such as companies, societies etc). Having understood these terms, let us analyze what constitutes obscenity. To be considered obscene for the purpose of this Section, the matter must satisfy at least one of the following conditions:

1. it must tend to excite lust, or
2. it must arouse interest in lustful thoughts, or
3. it must cause a person to become morally bad.

The above conditions must be satisfied in respect of a person who is the likely target of the material. This can be understood from the following illustration:

**Illustration with examples:**

Mohan launches a website that contains information on sex education. The website is targeted at higher secondary school students. Roja is one such student who is browsing the said website. Her illiterate young maid servant happens to see some explicit photographs on the website and is filled with lustful thoughts. This website would not be considered obscene. This is because it is most likely to be seen by educated youngsters who appreciate the knowledge sought to be imparted through the photographs. It is under very rare circumstances that an illiterate person would see these explicit images.
Publishing cyber pornography (Summary)

<table>
<thead>
<tr>
<th>Actions covered</th>
<th>Publishing, causing to be published and transmitting cyber pornography.</th>
</tr>
</thead>
</table>
| Penalty               | **First offence:** Simple or rigorous imprisonment up to 5 years and fine up to Rs 1 lakh  
                        | **Subsequent offence:** Simple or rigorous imprisonment up to 10 years and fine up to Rs 2 Lakhs |
| Relevant authority    | Court of Session                                                      |
| Appeal lies to        | High Court                                                            |
| Investigation         | 1. Controller of Certifying Authorities (CCA)                        |
| Authorities           | 2. Person authorized by CCA                                           |
|                       | 3. Police Officer not below the rank of Deputy Superintendent         |
| Points to mention in complaint | 1. Complainant details                                           |
|                       | 2. Suspect details                                                    |
|                       | 3. How and when the contravention was discovered and by whom          |
|                       | 4. Other relevant information                                         |

Avnish Bajaj vs. State (N.C.T.) of Delhi:


**Summary of the case:** Avnish Bajaj, CEO of Baazee.com, an online auction website, was arrested for distributing cyber pornography. The charges stemmed from the fact that someone had sold copies of a pornographic CD through the Baazee.com website.

The court granted him bail in the case.

**The major factors considered by the court were:**

1. There was no prima facie evidence that Mr. Bajaj directly or indirectly published the pornography,
2. The actual obscene recording/clip could not be viewed on Baazee.com,
3. Mr. Bajaj was of Indian origin and had family ties in India.

**Background of the case:** Avnish Bajaj is the CEO of Baazee.com, a customer-to-customer website, which facilitates the online sale of property. Baazee.com receives commission from such sales and also generates revenue from advertisements carried on its web pages. An obscene MMS clipping was listed for sale on Baazee.com on 27th November, 2004 in the name of “DPS Girl having fun”. Some copies of the clipping were sold through Baazee.com and the seller received the money for the sale.

Avnish Bajaj was arrested under Section 67 of the Information Technology Act, 2000 and his bail application was rejected by the trial court. He then approached the Delhi High Court for bail.

**Issues raised by the Prosecution:**
1. The accused did not stop payment through banking channels after learning of the illegal nature of the transaction.
2. The item description "DPS Girl having fun" should have raised an alarm.

**Issues raised by the Defense:**
1. Section 67 of the Information Technology Act relates to publication of obscene material. It does not relate to transmission of such material.
2. On coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend.

**Findings of the court:**
1. It has not been established from the evidence that any publication took place by the accused, directly or indirectly.
2. The actual obscene recording/clip could not be viewed on the portal of
3. The sale consideration was not routed through the accused.

4. Prima facie Baazee.com had endeavored to plug the loophole.

5. The accused had actively participated in the investigations.

6. The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof.

7. Even though the accused is a foreign citizen, he is of Indian origin with family roots in India.

8. The evidence that has been collected indicates only that the obscene material may have been unwittingly offered for sale on the website.

9. The evidence that has been collected indicates that the heinous nature of the alleged crime may be attributable to some other person.

**Decision of the court:**

1. The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1 lakh each.

2. The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the Court.

3. The court also ordered Mr. Bajaj to participate and assist in the investigation.

**2. Accessing Protected System:** According to Section 70 of the IT Act

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

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-Section (1).
(3) Any person who secures access or attempts to secure access to a
protected system in contravention of the provisions of this Section
shall be punished with imprisonment of either description for a term
which may extend to ten years and shall also be liable to fine.

As per Executive order dated 12-9-2002, issued by Ministry of
Communications & Information Technology details of every protected
system should be provided to the Controller of Certifying Authorities.

There are three elements to this Section:

1. Gazette notification for declaring protected system.
2. Government order authorizing persons to access protected systems.
3. Punishment for access to protected systems by unauthorized persons.

Relevant terms and issues:

- Appropriate government is determined as per Schedule VII of the
  Constitution of India.

- Schedule VII of the Constitution of India contains 3 lists: Union, State
  and Concurrent. Parliament has the exclusive right to make laws on
  items covered in the Union List e.g. defense, Reserve Bank of India etc.

- State Governments have the exclusive right to make laws on items
  covered in the State List e.g. police, prisons etc.

- Parliament as well as the State Governments can make laws on matters
  in the Concurrent List e.g. forests, electricity etc.

Illustration 1:

If the computer network of the Indian Army is to be declared as a
protected system, the Central Government would be the appropriate
Government.

Illustration 2:
If the computer network of the Mumbai police is to be declared as a protected system, the Government of Maharashtra would be the appropriate Government.

Illustration 3:

If the computer network of the Forest Department in Maharashtra is to be declared as a protected system, the Central Government as well as the Government of Maharashtra would be the appropriate Government.

All the acts, rules, regulations etc passed by the Central and State Government are notified in the Official Gazette. The Official Gazette in the electronic form is called the Electronic Gazette. A notification becomes effective on the date of its publication in the Gazette. The Government order may specify the authorized persons by name or by designation (e.g. all officers of rank of Inspector and above deputed in a particular department).

The term “securing access” in this Section is a grammatical variation of the term “secures access” as discussed earlier. Attempt to secure access is a very wide term and can best be understood through the following illustrations.

Illustration 1:

Mohan runs a password cracking software to crack the password of a protected system. Irrespective of whether he succeeds in cracking the password, he is guilty of attempting to secure access.

3. Tampering with computer source code

According to Section 65 of the IT Act 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. Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. Computer source code need not only be in the electronic form. It can be printed on paper (e.g. printouts of flowcharts for designing a software application).

**Tampering with computer source code (Summary)**

<table>
<thead>
<tr>
<th>Actions covered</th>
<th>Knowingly or intentionally concealing, altering or destroying computer source code (or causing someone else to do so).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penalty</td>
<td>Imprisonment up to 3 years and / or fine up to Rs 2 lakh</td>
</tr>
<tr>
<td>Relevant authority</td>
<td>Judicial Magistrate First Class</td>
</tr>
<tr>
<td>Appeal lies to</td>
<td>Court of Session</td>
</tr>
</tbody>
</table>
| Investigation Authorities | 1. Controller of Certifying Authorities (CCA)  
2. Person authorized by CCA  
3. Police Officer not below the rank of Deputy Superintendent |
| Points to mention in complaint | 1. Complainant details  
2. Suspect details  
3. How and when the contravention was discovered and by whom  
4. Damage suffered  
5. Other relevant information |

Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh & Anr 2005Criminal J4314

Summary of the case:
Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm. The court held that such manipulation amounted to tampering with computer source code as envisaged by Section 65 of the Information Technology Act, 2000.

Background of the case:
Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500 as well as service bundle for 3 years with an initial payment of Rs. 3350 and monthly outflow of Rs. 600. The subscriber was also provided a 1 year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically “unlocked” so that the exclusive Reliance handsets could be used for the Tata Indicom service.

Reliance officials came to know about this “unlocking” by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Tele Services Limited officials for reprogramming the Reliance handsets. These arrested persons approached the
High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

**Issues raised by the Defense:**

1. It is always open for the subscriber to change from one service provider to the other service provider.

2. The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.

3. The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.

4. A telephone handset is neither a computer nor a computer system containing a computer programme.

5. There is no law in force which requires the maintenance of "computer source code". Hence, Section 65 of the Information Technology Act does not apply.

**Findings of the court:**

1. As per Section 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

2. The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of
computer functions. This is known as source code in computer parlance.

3. A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.

4. When the person moves from one cell to another cell in the same city, the system i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower. All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.

6. System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.

7. Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.

8. Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.

9. When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.

10. If the phone cannot find any control channels to listen to, the cell phone
displays "no service" message as it is out of range.

11. When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in database, knows which cell phone you are using and gives a ring.

12. So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

13. This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

14. When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If someone manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

**Conclusions of the court:**

1. A cell phone is a computer as envisaged under the Information Technology Act.

2. ESN and SID come within the definition of “computer source code” under Section 65 of the Information Technology Act.

3. When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.
4. Whether a cell phone operator is maintaining computer source code, is a matter of evidence.

5. In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases –
   a. "when the computer source code is required to be kept"
   b. "maintained by law for the time being in force"

Abstract of the case:

This practical is a case study of an Insurance Company’s migration to an enterprise-wide security system. It is the intent of this practical to provide a path to follow when creating or migrating to a security system. Initially, a primitive online security system was the only mechanism to control access to corporate data. The exposures were severe - there were no integrity controls outside of the online environment. Anyone with basic programming skills could add, change and/or delete production data.

A project plan was developed to identify tasks, assign resources and ensure milestones were met. The scope of the security initiative included creating an inventory of information assets, creating new objects (data within datasets), constructing new groups and granting the appropriate permissions for access to the objects. Training documentation was created to instruct the users how to access the new system, both in an interactive and batch mode.

Mini boot camps were conducted to train the trainers, who in turn, provided mentoring and tutoring for the user community. Additional staff was recruited from other departments to provide user support for the rollout. D-Day arrived and the rollout experience only minor glitches. All the exposures were mitigated to the satisfaction of internal and external auditors.

Until recently, many information technology (IT) professionals
lacked awareness and interest in the cyber crime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn’t quite fit the crimes being committed, new laws hadn’t quite caught up to the reality of what was happening, and there were few court precedents to look to for guidance. Furthermore, debates over privacy issues hampered the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust—between the two most important players in any effective fight against cyber crime: law enforcement agencies and computer professionals. However, close cooperation between the two is crucial if we are to control the cyber crime problem and make the Internet a safe “place” for its users.

Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cyber criminal.

**Implications of the IT Act in combating the cyber crimes:**

The information technology Act attempts to change outdated laws and provides ways to deal with cyber crimes. Let’s have an overview of the law where it takes a firm stand and has got successful in the reason for which it was framed.

1. The e-commerce industry carries out its business via transactions and communications done through electronic records. It thus becomes essential that such transactions be made legal. Keeping this point in the consideration, the IT Act 2000 empowers the government departments to accept filing, creating and retention of official documents in the digital format. The Act also puts forward the proposal for setting up the legal framework essential for the authentication and origin of electronic
records / communications through digital signature.

2. The Act legalizes the e-mail and gives it the status of being valid form of carrying out communication in India. This implies that e-mails can be duly produced and approved in a court of law, thus can be regarded as substantial document to carry out legal proceedings.

3. The act also talks about digital signatures and digital records. These have been also awarded the status of being legal and valid means that can form strong basis for launching litigation in a court of law. It invites the corporate companies in the business of being Certifying Authorities for issuing secure Digital Signatures Certificates.

4. The Act now allows Government to issue notification on the web thus heralding e-governance.

5. It eases the task of companies of the filing any form, application or document by laying down the guidelines to be submitted at any appropriate office, authority, body or agency owned or controlled by the government. This will help in saving costs, time and manpower for the corporate.

6. The act also provides statutory remedy to the corporate in case the crime against the accused for breaking into their computer systems or network and damaging and copying the data is proven. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore ($200,000).

7. Also the law sets up the Territorial Jurisdiction of the Adjudicating Officers for cyber crimes and the Cyber Regulations Appellate Tribunal.

8. The law has also laid guidelines for providing Internet Services on a license on a non-exclusive basis. The IT Law 2000, though appears to be self sufficient, it takes mixed stand when it comes to many practical situations. It loses its certainty at many places like:
1. The law misses out completely the issue of Intellectual Property Rights, and makes no provisions whatsoever for copyrighting, trade marking or patenting of electronic information and data. The law even doesn’t talk of the rights and liabilities of domain name holders, the first step of entering into the e-commerce.

2. The law even stays silent over the regulation of electronic payments gateway and segregates the negotiable instruments from the applicability of the IT Act, which may have major effect on the growth of e-commerce in India. It leads to make the banking and financial sectors irresolute in their stands.

3. The act empowers the Deputy Superintendent of Police to look up into the investigations and filling of charge sheet when any case related to cyber law is called. This approach is likely to result in misuse in the context of Corporate India as companies have public offices which would come within the ambit of "public place" under the Act. As a result, companies will not be able to escape potential harassment at the hands of the DSP.

4. Internet is a borderless medium; it spreads to every corner of the world where life is possible and hence is the cyber criminal. The Act initially was supposed to apply to crimes committed all over the world, but nobody knows how can this be achieved in practice, how to enforce it all over the world at the same time?

i) The IT Act is silent on filming anyone’s personal actions in public and then distributing it electronically. It holds ISPs (Internet Service Providers) responsible for third party data and information, unless contravention is committed without their knowledge or unless the ISP has undertaken due diligence to prevent the contravention.

ii) For example, many Delhi based newspapers advertise the massage
parlors; and in few cases even show the ‘therapeutic masseurs’ hidden behind the mask, who actually are prostitutes. Delhi Police has been successful in busting out a few such rackets but then it is not sure of the action it can take... should it arrest the owners and editors of newspapers or wait for some new clauses in the Act to be added up? Even the much hyped case of the arrest of Bajaj, the CEO of Bazee.com, was a consequence of this particular ambiguity of the law. One cannot expect an ISP to monitor what information their subscribers are sending out, all 24 hours a day.

Cyber law is a generic term, which denotes all aspects, issues and the legal consequences on the Internet, the World Wide Web and cyber space. India is the 12th nation in the world that has cyber legislation apart from countries like the US, Singapore, France, Malaysia and Japan. But can the cyber laws of the country be regarded as sufficient and secure enough to provide a strong platform to the country’s e-commerce industry for which they were meant? India has failed to keep in pace with the world in this respect, and the consequence is not far enough from our sight; most of the big customers of India’s outsourcing company have started to re-think of carrying out their business in India. Bajaj’s case has given the strongest blow in this respect and have broken India’s share in outsourcing market as a leader. If India doesn’t want to lose its position and wishes to stay as the world’s leader forever in outsourcing market, it needs to take fast but intelligent steps to cover the glaring loopholes of the Act, or else the day is not far when the scenario of India ruling the world’s outsourcing market will stay alive in the dreams only as it will be overtaken by its competitors.

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

The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the
Government. The IT Act also penalizes various cyber crimes and provides strict punishments (imprisonment terms up to 10 years and compensation up to Rs 1 crore).

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

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

The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques. Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to the Government bodies. On the same day, the Information Technology (Certifying Authorities) Rules, 2000 also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CAs). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006.

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9 July 2001. Next were the Guidelines for submission of certificates and certification revocation lists to the Controller.
of Certifying Authorities for publishing in the National Repository of Digital Certificates. These were issued on 16 December 2002.

The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 also came into force on 17 October 2000. These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers.

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

Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT. On 17 March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

The appointment of adjudicating officers to decide the fate of multi-crores cyber crime cases in India was the result of the public interest litigation filed by students of Asian School of Cyber Laws (ASCL).

The Government had not appointed the Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the IT Act had come into force. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for speedy appointment of Adjudicating officers.
The Bombay High Court, in its order dated 9 October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon’ble Justice A.P. Shah and Hon’ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.

Following this the Central Government passed an order dated 23 March 2003 appointing the “Secretary of Department of Information Technology of each of the States or of Union Territories” of India as the adjudicating officer for that State or Union Territory.

The Information Technology (Security Procedure) Rules, 2004 came into force on 29 October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. Also relevant are the Information Technology (Other Standards) Rules, 2003.

An important order relating to blocking of websites was passed on 27 February, 2003. Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DoT) to block a website. The Indian Penal Code (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc. Digital evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act). In case of bank records, the provisions of the Bankers’ Book Evidence Act (as amended by the IT Act) is relevant.

Investigation and adjudication of cyber crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act. The Reserve Bank of India Act was also amended by the IT Act. The Information Technology (Amendment) Act, 2008, which came into force
on 27th October, 2009 has made sweeping changes to the Information Technology Act, 2000. The following rules have also come into force on the same day:

(1) Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

(2) Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

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

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

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

Glarng loopholes in cyber law amendments

The IT Amendment Bill 2008, which seeks to make sweeping changes in the existing Indian cyberlaw, has been passed by the Lok Sabha and the Rajya Sabha. While due credit needs to be given to the government for removing the various practical difficulties of the IT Act, 2000, but given the magnitude of the amendments, it is indeed strange and amazing that this Bill was passed in an unprecedented hurry, without any discussion in the last week of December.

A careful analysis of the amendments clearly brings home the point that the new amendments are not at all sufficient in the context of emergent needs of India and have various glaring loopholes. India has neither learnt from the wisdom of the United States nor the European Union, in terms of their respective experiences in the area of data protection. As a result, the issues relating to confidential information and data of corporates and their adequate protection have not been adequately addressed. The law is not
comprehensive enough on data protection or on digital secrets. Having a couple of Sections on data protection does not serve the requirements of corporate India. The proposed provisions will not aid the victim entities, whose data and information is often misused by their employees or agents with impunity.

The IT Act Amendments are also deficient in the sense that they do not create rebuttable presumptions of confidentiality of trade-secrets and information. A large number of companies and individuals are saving their confidential data, information and trade-secrets in the electronic form. Given the apparent increase in technology adoption, it is increasingly being found that despite all precautions, employees are still going ahead and taking away confidential data from companies.

The inability of law to create enabling presumptions of confidentiality regarding corporate and individual data and information in the electronic form is likely to complicate matters further for Indian companies. Given the move to make most cyber crimes bail able offences, corporate need to forget about being able to get their errant employees, misusing their confidential data and information, behind bars.

The absence of an effective remedy for corporate by the new amendments was likely to further erode the confidence of the industry in the new cyber legal regime. The maximum damages by way of compensation stipulated by the new cyber law amendments are Rs 50 million. Calculated in US dollar terms, this is a small figure and hardly provides any effective relief to corporate, whose confidential information worth millions is stolen or misused by its employees or agents.

Another major failure of the proposed amendments is that they have not dealt with the entire issue pertaining to spam in a comprehensive manner. In any case, the word spam is not even mentioned anywhere in the IT Amendment Bill. India has yet again missed an opportunity to deal with
this contentious issue. It is pertinent to note here that the countries like the US, Australia and New Zealand have demonstrated their intentions to fight spam by coming across with dedicated anti-spam legislation. However, in India, we neither have any anti-spam legislation, nor do we have any specific provisions for effective prevention and regulation. This make India a heaven as far as spam is concerned. This is all the more serious since India already features in the top ten nations from where spam originates.

Any major failure of the IT Act Amendments is that they have not specifically detailed with the issues pertaining to electronic discovery. Today, increasingly people and entities as also corporate are relying upon electronic evidence and media as a means of communicating with each other and doing business. However, the Indian IT Act amendments are completely silent on the issues of electronic discovery. This once again shows the short sightedness of the Indian IT Amendments.

Bill to address the complicated emerging issues pertaining to electronic discovery. The IT Act amendments do not address jurisdictional issues. At a time when the internet has made geography history, it was expected that the new amendments would throw far more clarity on complicated issues pertaining to jurisdiction. This is because numerous activities on the internet take place in different jurisdictions and that there is a need for enabling the Indian authorities to assume enabling jurisdiction over data and information impacting India in a more comprehensive way than in the manner as sketchily provided under the current law.

The new amendments make it mandatory for corporates' "possessing, dealing or handling any sensitive personal data or information in a computer resource to maintain reasonable security practices and procedures". However, what are these "reasonable security practices and procedures" can be anybody’s guess. It has to be pointed out that one set of security practices will not fit the entire nation. What are reasonable security
practices for one industry may not be directly applicable to another industry. Non-maintaining such reasonable security practices will expose the said corporates to civil liability to pay damages to person/s so affected to the tune of Rs 50 million.

While the new amendments to the IT Act are likely to impact all industries that use computers, computer systems and computer networks, and which store data and information in the electronic form, they are also likely to unveil a package of unpleasant surprises for many as they come with a lot of additional compliance obligations.

The Information Technology Act 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialised field. The Act has however during its application has proved to be inadequate to a certain extent. The various loopholes in the Act are:

The hurry in which the legislation was passed, without sufficient public debate, did not really serve the desired purpose: Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for public debate.

"Cyber laws, in their very preamble and aim, state that they are targeted at aiding e-commerce, and are not meant to regulate cyber crime” Mr. Pawan Duggal holds the opinion that the main intention of the legislators has been to provide for a law to regulate the e-commerce and with that aim the I.T. Act 2000 was passed, which also is one of the reasons for its inadequacy to deal with cases of cyber crime.

The Act aims to deal with all matters connected therewith or incidental thereto. It is a cardinal rule of interpretation that “text should be read as a whole to gather the meaning”. It seems that the above statement has been made in total disregard of this rule of interpretation. The preamble, if read as a whole, makes it very clear that the Act equally aims
at legalizing e-commerce and to curb any offences arising there from.

**Cyber torts:**

The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the I.T. Act 2000 has not dealt with those offences. Further it is also contended that in future new forms of cyber crime will emerge which even need to be taken care of. Therefore India should sign the cyber crime convention. However the I.T. Act 2000 read with the Penal Code is capable of dealing with these felonies.

Cyber crime in the Act is neither comprehensive nor exhaustive- Mr. Duggal believes that we need dedicated legislation on cyber crime that can supplement the Indian Penal Code. The contemporary view is held by Mr. Prathamesh Popat who has stated- "The IT Act, 2000 is not comprehensive enough and doesn't even define the term 'cyber crime"

Mr. Duggal has further commented, “India, as a nation, has to cope with an urgent need to regulate and punish those committing cyber crimes, but with no specific provisions to do so. Supporters of the Indian Penal Code School vehemently argue that IPC has stood the test of time and that it is not necessary to incorporate any special laws on cyber crime. This is because it is debated by them that the IPC alone is sufficient for all kinds of crime. However, in practical terms, the argument does not have appropriate backing. It has to be distinctly understood that cyber crime and cyberspace are completely new whelms, where numerous new possibilities and opportunities emerge by the day in the form of new kinds of crimes.”

Mr. Duggal has stated the need to supplement IPC by a new legislation. If that is the issue then the present legislation along with the Penal Code when read harmoniously and co-jointly is sufficient to deal with the present problems of cyber crime. Further there are other
legislations to deal with the intellectual property crimes on the cyber space such as the Patents Act, Copy Right Act, Trade Marks Act.

**Ambiguity in the definitions:** The definition of hacking provided in Section 66 of the Act is very wide and capable of misapplication. There is every possibility of this Section being misapplied and in fact the Delhi court has misapplied it. Further Section 67 is also vague to certain extent. It is difficult to define the term lascivious information or obscene pornographic information. Further our inability to deal with the cases of cyber pornography has been proved by the Bal Bharati case.

**Uniform law:** Mr. Vinod Kumar holds the opinion that the need of the hour is a worldwide uniform cyber law to combat cyber crime. Cyber crime is a global phenomenon and therefore the initiative to fight it should come from the same level. E.g. the author of the love bug virus was appreciated by his countrymen.

**Lack of awareness:** One important reason that the Act of 2000 is not achieving complete success is the lack of awareness among the s about their rights. Further most of the cases are going unreported. If the people are vigilant about their rights the law definitely protects their right. E.g. the Delhi high court in October 2002 prevented a person from selling Microsoft pirated software over an auction site. Achievement was also made in the case before the court of metropolitan magistrate Delhi wherein a person was convicted for online cheating by buying Sony products using a stolen credit card.

**Jurisdiction issues:** Jurisdiction is also one of the debatable issues in the cases of cyber crime due to the very universal nature of cyber space. With the ever-growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to the conventional methods. The Act of 2000 is very silent on these issues.

**Extra territorial application:** Though S.75 provides for extra-territorial
operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

**Raising a cyber army:** By using the word ‘cyber army’ by no means I want to convey the idea of virtual army, rather I am laying emphasis on the need for a well equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting cyber crime cells in all metropolitan and other important cities. Further the establishment of the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI) is definitely a welcome step in this direction. There are many cases in which the C.B.I has achieved success. The present position of cases of cyber crime is:

**Case 1:** When a woman at an MNC started receiving obscene calls, CBI found her colleague had posted her personal details on Mumbaidating.com.

**Status:** Probe on

**Case 2:** CBI arrested a man from UP, Mohammed Feroz, who placed ads offering jobs in Germany. He talked to applicants via e-mail and asked them to deposit money in his bank account in Delhi.

**Status:** Chargesheet not filed

**Case 3:** The official web-site of the Central Board of Direct Taxes was hacked last year. As Pakistan-based hackers were responsible, authorities there were informed through Interpol.

**Status:** Pak not cooperating.

**Cyber savvy bench:** Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerela
High Court has accepted through an e-mail. The role of the judges in today's word may be gathered by the statement—judges carve 'law is' to 'law ought to be'. Member Secretary, Law Commission, has highlighted the requirements for introducing e-courts in India. In his article published in The Hindu he has stated “if there is one area of Governance where IT can make a huge difference to Indian public is in the Judicial System”.

**Dynamic form of cyber crime:** Speaking on the dynamic nature of cyber crime FBI Director Louis Freeh has said, "In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing even faster and we are falling further behind." The (de)creativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to cyber crime cases.

**Hesitation to report offences:** As stated above one of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. This was proved by the Delhi time theft case. "The police are a powerful force today which can play an instrumental role in preventing cyber crime. At the same time, it can also end up wielding the rod and harassing innocent s, preventing them from going about their normal cyber business." This attitude of the administration is also revealed by incident that took place at Meerut and Belgam. (for the facts of these incidents refer to naavi.com). For complete realization of the provisions of this Act a cooperative police force is require.

**Preventing cyber crime:** Cyber Crime is an evil having its origin in the growing dependence on computers in modern life. A simple yet sturdy definition of cyber crime would be “unlawful acts wherein the computer is either a tool or a target or both”. Defining cyber crimes, as “acts that are punishable by the information Technology Act” would be
unsuitable as the Indian Penal Code also covers many cyber crimes, such as e-mail spoofing, cyber defamation etc.,

Cyber crime 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 may be activities newly evolved with the growth of the new medium. Cyber crimes can be basically divided into 3 major categories being Cyber crimes

Against persons
Against property
Against Government

The Asian School of Cyber laws’ Computer Crime and Abuse Report (India) 2001-02 reports that Data Theft at 33per cent makes up largest category of reported incidents of Cyber crime. Of this 37per cent of data stolen is the Source/Object Code.

- Various cyber offences defined
- Cyber offences to be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police.
- Tampering with computer source documents – Section 65
- Hacking - Section 66
- Publishing of information which is obscene in electronic form - Section 67

Section 65: Tampering with computer source documents

Knowingly or intentionally concealing, destroying or altering or intentionally or knowingly causing another to conceal, destroy or alter any computer source code used for 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
Section 66: Hacking with computer system

Occurs when there is intent to cause or knowledge that one is likely to cause wrongful loss or damage to the public or any person by destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means.

Section 67: Publishing of information which is obscene in electronic form

Publishing or transmitting or causing to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

Punishment for publishing obscene information in electronic form

On first conviction there will be imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees.

Second or subsequent conviction would be imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Breach of confidentiality and privacy.

Misrepresentation: Publishing Digital Signature Certificate false in certain particulars and publication for fraudulent purposes.

IT ACT deficient: The offences defines in the IT Act are by no means exhaustive. However, the drafting of the relevant provisions of the IT Act make it appear as if the offences detailed in the said IT Act are the only Cyber offences possible and existing.

Need for ingenuity: Just as human mind is ingenious enough to devise new ways for perpetuating crime, similarly, human ingenuity needs to be
channelized into developing effective legal and regulatory mechanisms to control and prevent Cyber crimes.

**Breach of security:** Breach of security attracts consequences of civil liability. If a person without the permission of owner or any other person in charge of a computer, computer system or computer network, accesses or secures access to such computer, computer system or computer network, he is liable to pay statutory damages by way of compensation, not exceeding one crore rupees to the person so affected.

**Civil liability:** Downloading, copying or extracting any data, computer database or information from such system or introducing any computer virus into the same or damaging, destructing or causing to be damaged or disruption of the same or denying the access to any authorized person of the same, and providing any assistance to any person for doing any of the acts mentioned above, would also attract the civil liability of damages by way of compensation not exceeding rupees one crore.

Breach of security is also implicitly recognized as a penal offence in the form of hacking. This offence is declared as a penal offence punishable with three years imprisonment and two lakh rupees fine.

**Investigation:** For the purpose of investigating the offences detailed under the IT Act, 2000, police officers not below the rank of Deputy Superintendent of Police have been duly authorized and who have also been given the power of entry, search and arrest without warrant in public places.

**Section 79:** 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 there under 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.

Network Service Providers: When Not Liable

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.

Offences by companies: Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-Section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

• Clause 49, SEBI:
• For listed companies
• Certifications by CEO and the compliance officer
• Certification of data, information, computers, computer systems and computer networks
• Need for cyber legal due diligence
• Compliance with IT Act, IT Rules, notifications etc
• Compliance with Indian Evidence Act
• Information Technology Security Policy
• Legal Authentication of E-records
• Retention of E-records as per law
• Techno-Legal Risks in today’s Business Environment.
• Need to have a systematic plan for to measure risk of exposure to the same.

• Due Diligence and Compliance only mantra of survival in today’s e-world

Limiting your liability for criminal activities done on your computers, computers and computer networks by others is absolutely essential lest we face some unpleasant situations. Cyber law audit of your operations using computers, computer systems and computer networks are critical for your continued growth.

Mr. Pawan Duggal associates undertakes cyber law audits for clients for limiting their liability.

Cyber Crime refers to all activities done with criminal intent in cyberspace. These fall into three slots.

• Those against persons.
• Against Business and Non-business organizations.
• Crime targeting the government.

Let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computer. Some examples are;

Financial Claims: This would include cheating, credit card frauds, money laundering etc.

Cyber Pornography: This would include pornographic websites; pornographic magazines produced using computer and the Internet (to download and transmit pornographic pictures, photos, writings etc.)

Sale of illegal articles: This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, bulletin boards or simply by using e-mail communications.

Online gambling: There are millions of websites; all hosted on servers
abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

**Intellectual Property Crimes:** These include software piracy, copyright infringement, trademarks violations etc.

**Mail spoofing:** A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source. This can also be termed as e-Mail forging.

**Forgery:** Counterfeit currency notes, postage and revenue stamps, mark sheets etc., can be forged using sophisticated computers, printers and scanners.

**Cyber Defamation:** This occurs when defamation takes place with the help of computers and or the Internet e.g. someone published defamatory matter about someone on a websites or sends e-mail containing defamatory information to all of that person’s friends.

**Cyber Stalking:** Cyber stalking involves following a person’s movements across the Internet by posting messages on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim.

Let us examine some of the acts wherein the computer or computer Network is the target for an unlawful act. It may be noted that in these activities the computer may also be a tool. This kind of activity is usually out of the purview of conventional criminal law. Some examples are:

**Unauthorized access to computer system or network:** This activity is commonly referred to as hacking. The Indian Law has however given a different connotation to the term hacking.

**Theft of information contained in electronic from:** This includes information stored in computer hard disks, removable storage media etc.

**E-mail bombing:** E-mail bombing refers to sending a large amount of e-mails to the victim resulting in the victims’ e-mail account or mail servers.
**Data diddling:** This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

**Salami attacks:** Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A bank employee inserts a program into bank’s servers, that deducts a small amount from the account of every customer.

**Denial of Service:** This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

**Virus/worm:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses don not need the host to attach themselves to.

**Logic bombs:** These are dependent programs. This implies that these programs are created to do something only when a certain event occurs, e.g. some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date.

**Trojan Horse:** A Trojan as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

**Internet Time Theft:** This connotes the usage by unauthorized persons of the Internet hours paid for by another person.

**Physically damaging a computer system:** This crime is usually committed by physically damaging a computer or its peripherals.

**Prevention:** Preventive steps for individuals:
Children: Children should not give out identifying information such as Name, Home address, School Name or Telephone Number in a chat room. They should not give photographs to anyone on the Net without first checking or informing parents' guardians. They should not respond to messages, which are suggestive, obscene, belligerent or threatening, and not to arrange a face-to-face meeting without telling parents or guardians. They should remember that people online might not be who they seem.

Parents: Parent should use content filtering software on PC to protect children from pornography, gambling, hate speech, drugs and alcohol.

There is also software to establish time controls for use of limpets (for example blocking usage after a particulars time) and allowing parents to see which site item children have visited. This software may be used to keep track of the type of activities of children.

Preventive steps for organizations and government

Physical security: Physical security is most sensitive component, as prevention from cyber crime Computer network should be protected from the access of unauthorized persons.

Access control: Access Control system is generally implemented using firewalls, which provide a centralized point from which to permit or allow access. Firewalls allow only authorized communications between the internal and external network.

Password: Proof of identity is an essential component to identify intruder. The use of passwords is the most common security for network system including servers, routers and firewalls. Mostly all the systems are programmed to ask for username and password for access to computer system. This provides the verification of user. Password should be charged with regular interval of time and it should be alpha numeric and should be difficult to judge.
Finding the holes in network: System managers should track down the problems before the intruders perform some such crimes. Many networking product manufactures are not particularly aware with the information about security holes in their products. So organization should work hard to discover security holes, bugs and weaknesses and report their findings as they are confirmed.

Using network scanning programs: There is a security administration’s tool called UNIX, which is freely available on Internet. This utility scans and gathers information about any host on a network, regardless of which operating system or services the hosts were running. It checks the known vulnerabilities include bugs, security weakness, inadequate password protection and so on. There is another product available called COPS (Computer Oracle and Password System). It scans for poor passwords, dangerous file permissions, and dates of key files compared to dates of CERT security advisories.

Using intrusion alert programs: As we know that it is important to identify and close existing security holes, we need to put some watchdogs into service. There are some intrusion programs, which identify suspicious activity and report so that necessary action is taken. They need to be operating constantly so that all unusual behaviour on network is caught immediately.

Using encryption: Encryption is able to transform data into a form that makes it almost impossible to read it without the right key. This key is used to allow controlled access to the information to selected people. The information can be passed on to anyone but only the people with the right key are able to see the information. Encryption allows sending confidential documents by e-mail or save confidential information on laptop computers without having to fear that if someone steals it the data will become public. With the right encryption/ decryption software installed, it will hook up to
mail program and encrypt/ decrypt messages automatically without user interaction.

**Detection of Cyber:** Cyber crime is the latest and perhaps the most specialized and dynamic field in cyber laws. Some of the Cyber Crimes like network Intrusion are difficult to detect and investigation even though most of crimes against individual like cyber stalking, cyber defamation, cyber pornography can be detected and investigated through following steps:

After receiving such type of mail

1. Give command to computer to show full header of mail.
2. In full header find out the IP number and time of delivery of number and this IP number always different for every mail. From this IP number we can know who was the Internet service provider for that system and from which the mail had come.
3. To know about Internet Service Provider from IP number takes the service of search engine like nic.com, macff visual route. Com,apnic.com, arin.com.
4. After opening the website of any of above mentioned search engine, feed the IP number and after some time name of ISP can be obtained.
5. After getting the name of ISP we can get the information about the sender from the ISP by giving them the IP number, date and time of sender.
6. ISP will provide the address and phone number of the system, which was used to send the mail with bad intention.

After Knowing the address and phone number criminal can be apprehended by using conventional police methods.

**Cyber law:** India has enacted the first I.T. Act, 2000 based on the UNCIRAL model recommended by the general assembly of the United
Nations. Chapter XI of this Act deals with offences/crimes along with certain other provisions scattered in this Act. The various offences which are provided under this chapter are shown in the following table:

<table>
<thead>
<tr>
<th>Offence</th>
<th>Section under IT Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tampering with Computer source documents</td>
<td>Section 65</td>
</tr>
<tr>
<td>Hacking with Computer systems, Data alteration</td>
<td>Section 66</td>
</tr>
<tr>
<td>Publishing obscene information</td>
<td>Section 67</td>
</tr>
<tr>
<td>Un-authorized access to protected system</td>
<td>Section 70</td>
</tr>
<tr>
<td>Breach of Confidentiality and Privacy</td>
<td>Section 72</td>
</tr>
<tr>
<td>Publishing false digital signature certificates</td>
<td>Section 73</td>
</tr>
</tbody>
</table>

**NOTE:** Sec.78 of I.T.Act empowers Deputy Supdt. of Police to investigate cases falling under this Act.

**Computer Related Crimes Covered under IPC and Special Laws**

**Offence Section:** Sending threatening messages by e-mail Section 503 IPC

Sending defamatory messages by e-mail Section 499 IPC

Forgery of electronic records Section 463 IPC

Bogus websites, cyber frauds Sec 420 IPC

E-mail spoofing Section 463 IPC

Web-Jacking Section 383 IPC

Abuse Section 500 IPC

Online sale of Drugs NDPS Act

Online sale of Arms Act.

**Elementary problems associated with cyber-crimes:** One of the greatest lacunae in the field of Cyber Crime is the absence of comprehensive law anywhere in the World. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of I.T. Act and amendments made to Indian Penal Code, problems associated with cyber crimes continue to persist.

1. Jurisdiction is the highly debatable issue as to the maintainability of any suits, which has been filed. Today with the growing arms of cyber space the territorial boundaries seem to vanish.. Thus the concept of territorial jurisdiction as envisaged under Section 16 of Cr.P.C. and Section 2 of
the I.P.C. will have to give way to alternative method of dispute resolution.

2. Loss of evidence is a very common and expected problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses the system of crime investigation.

3. Cyber Army: There is also an imperative need to build a high technology crime & investigation infrastructure, with highly technical staff at the other end.

4. A law regulating the cyber-space, which India has prepared and implemented (see Annexure-1)

5. Though Section 75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provision recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

**General information:** Don’t delete harmful communications (e-mails, chats etc). They will provide vital information about system and address of the person behind these.

Try not to be panic. If you feel any immediate physical dangers contact your local police. Avoid getting into huge arguments online during chat and discussions with other users. Remember that all other Internet users are strangers; you do not know who you are chatting with. So be careful. Be extremely careful about how you share personal information about yourself online. Choose your chatting nickname carefully so as others.

Do not share personal information in public space online; do not give it to strangers. Be extremely cautious about meeting online introduced
person. If you choose to meet, do so in a public place along with a friend. If a situation online becomes hostile, log off and if a situation places you in fear, you need to contact local police. Save all communications for evidence. Do not edit it in any way. Also, keep a record of your contacts and inform Law Enforcement Officials.

Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such case, which needs appreciation, is the P.I.L. (Public Interest Litigation), which the Kerala High Court has accepted through an e-mail. 'Perfect' is a relative term. Nothing in this world is perfect. The persons who legislates the laws and by-laws also are not perfect. The laws therefore enacted by them cannot be perfect.

Concluding remarks:

The cyber law has emerged from the womb of globalization. It is at the threshold of development. In due course of exposure through varied and complicated issues it will grow to be a piece of its time legislation. Some safety measures can be forwarded are: knowing one’s human assets (staff, partners, suppliers and agents); aligning IT, Internal Audit Team and Board of Directors in case of cyber crimes; conducting regular fraud risk assessments; having a cyber-savvy CEO for cultural impact and having a cyber crisis response plan.